MAGYAR KÖZLÖNY 68. szám

MAGYARORSZÁG HIVATALOS LAPJA
2024. június 24., hétfő

Tartalomjegyzék

III. Kormányrendeletek

A Kormány 131/2024. (VI. 24.) Korm. rendelete a hallgatói hitelrendszerről szóló 1/2012. (I. 20.) Korm. rendelet módosításáról

A Kormány a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 110. § (1) bekezdés 27. pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. § A hallgatói hitelrendszerről szóló 1/2012. (I. 20.) Korm. rendelet 29/B. § (1) bekezdésében a „2024. január 1-től 2024. június 30-ig" szövegrész helyébe a „2024. július 1-jétől 2024. december 31-ig" szöveg lép.

2. § Ez a rendelet 2024. július 1-jén lép hatályba.

Orbán Viktor s. k.,
miniszterelnök

IV. A Magyar Nemzeti Bank elnökének rendeletei, valamint az önálló szabályozó szerv vezetőjének rendeletei

A Magyar Nemzeti Bank elnökének 29/2024. (VI. 24.) MNB rendelete a Magyar Nemzeti Bank által felügyelt szolgáltatók által alkalmazott auditált elektronikus hírközlő eszköz és működtetésének, belső szabályozása minimumkövetelményeinek, auditálása módjának, valamint az ilyen eszköz útján végzett elektronikus ügyfél-átvilágítás végrehajtásának részletszabályairól

A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény 77. § (3) bekezdés d) pontjában kapott felhatalmazás alapján, a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 4. § (9) bekezdésében meghatározott feladatkörömben eljárva a következőket rendelem el:

1. Általános rendelkezések

1. § E rendelet hatálya a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: Pmt.) 1. § (1) bekezdés a)–e) és m) pontja, valamint 1. § (1a) bekezdése szerinti szolgáltatóra (a továbbiakban együtt: szolgáltató) terjed ki.

2. § E rendeletet a szolgáltató által végzett vagy kiszervezett, auditált elektronikus hírközlő eszköz útján történő ügyfél-átvilágítási intézkedésre kell alkalmazni.

3. § (1) E rendelet alkalmazásában

1. *auditált elektronikus hírközlő eszköz:* az ügyfél távoli, elektronikus adatátviteli csatornán történő átvilágítására, az ügyfél nyilatkozatainak megtételére, az ügyfél által tett nyilatkozat értelmezésére, biztonságos tárolására, a tárolt adatok visszakeresésére és ellenőrzésére alkalmas auditált elektronikus rendszer;
2. *biometrikus adatok:* a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 4. cikk 14. pontja szerinti fogalom;
3. *elektronikus ügyfélazonosító és nyilatkozattételi rendszer:* olyan személyre szabott elektronikus eljárást biztosító rendszer, amely a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának egyértelmű azonosítására és a jognyilatkozat tartalmának változatlan visszaidézésére alkalmas formában teszi lehetővé a jognyilatkozat megtételét;
4. *elektronikus ügyfél-átvilágítás:* a szolgáltatótól fizikailag távol lévő ügyfél vonatkozásában auditált elektronikus hírközlő eszközzel végzett ügyfél-átvilágítási intézkedés;
5. *erős ügyfél-hitelesítés:* hitelesítés legalább két olyan
   a) ismeret, azaz csak az ügyfél által ismert információ,
   b) birtok, azaz csak az ügyfél által birtokolt dolog és
   c) biológiai tulajdonság, azaz az ügyfél jellemzője

   kategóriába sorolható elem felhasználásával, amely kategóriák egymástól függetlenek annyiban, hogy az egyik feltörése nem befolyásolja a többi megbízhatóságát, és az eljárás kialakítása révén biztosított az azonosítási adatok bizalmassága;
6. *IKT- és biztonsági kockázat:* a bizalmasság megsértéséből, a rendszerek és adatok sértetlenségének sérüléséből, a rendszerek és adatok nemmegfelelőségéből vagy elérhetetlenségéből, illetve a környezeti vagy üzleti követelmények változása esetén az információs technológia észszerű időn belül és költségekkel járó megváltoztatására való (agilitás-) képtelenségből adódó veszteség kockázata, ide tartoznak a nem megfelelő vagy rosszul működő belső folyamatokból vagy külső eseményekből eredő biztonsági kockázatok, beleértve a kibertámadásokat vagy a nem megfelelő fizikai biztonságot is;

7. *megerősített eljárás:* az ügyfélben, a termékben, a szolgáltatásban, az ügyletben, az alkalmazott eszközben vagy a földrajzi kitettségben rejlő kockázat kezelésére szolgáló kockázatalapú intézkedések együttesét magába foglaló fokozott monitoring;
8. *pénzmosási és terrorizmusfinanszírozási kockázat:* a pénzmosás vagy a terrorizmus finanszírozása felmerülésének valószínűsége és hatása;
9. *visszaéléssel érintett ügylet:* minden olyan, a pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény szerinti fizetési művelet – ide nem értve a kártyaalapú fizetési műveletet –, amely esetében észszerű okból csalás gyanúja merül fel azzal kapcsolatban, hogy a fizetési műveletet az ügyfél nem kívánta jóváhagyni, vagy tévedésben lévő ügyfél hagyta jóvá.

(2) E rendelet ügyfélre vonatkozó rendelkezéseit az ügyfél szolgáltatónál eljáró meghatalmazottjára, rendelkezésre jogosultjára és képviselőjére is alkalmazni kell.

2. Az elektronikus ügyfél-átvilágításhoz alkalmazandó auditált elektronikus hírközlő eszköz bevezetését megelőző értékelés

4. § (1) A szolgáltató – jogszabály eltérő rendelkezése hiányában – egy új auditált elektronikus hírközlő eszköz bevezetését megelőzően minden esetben mérlegeli az auditált elektronikus hírközlő eszköz bevezetésének indokoltságát, és elvégzi az auditált elektronikus hírközlő eszköz előzetes értékelését.

(2) Az előzetes értékelés legalább az alábbiakra terjed ki:

a) az auditált elektronikus hírközlő eszköz útján összegyűjtendő adatok és dokumentumok teljességére és pontosságára, valamint a felhasznált információforrások megbízhatóságára és függetlenségére;
b) az auditált elektronikus hírközlő eszköz alkalmazásának hatására a szolgáltató egészét érintő kockázatokat illetően, beleértve a pénzmosással és a terrorizmus finanszírozásával kapcsolatos technológiai, működési, reputációs és jogi kockázatokat;
c) a b) pont szerinti értékelés során azonosított valamennyi kockázatra vonatkozó érdemi kockázatmérséklő intézkedésekre és a korrekciós intézkedések, felelősök és határidők meghatározására;
d) a visszaéléssel érintett ügylet kockázatainak – többek között a személyazonosító vagy -hitelesítő adatokkal való visszaéléssel kapcsolatos és más IKT- és biztonsági kockázatok – értékelésére szolgáló tesztekre, mely
   da) teszteket olyan független tesztelők végezhetik, akik a 14. § f) pontja szerinti ismeretekkel, készségekkel és szakértelemmel rendelkeznek az információbiztonsági intézkedések tesztelésében, és akik nem vesznek részt az információbiztonsági intézkedések kidolgozásában,
   db) tesztek során az üzleti folyamatok és rendszerek azonosított kockázati szintjével arányos sérülékenységi vizsgálatok és behatolási tesztek – ideértve a fenyegetésalapú behatolásvizsgálatokat, ahol szükséges és megfelelő – elvégzésre kerülnek; továbbá
e) az elektronikus ügyfél-átvilágítási szabályzat által meghatározott ügyfelekre, termékekre és szolgáltatásokra irányuló működésének végponttól végpontig terjedő tesztelésére.

5. § A szolgáltató a Magyar Nemzeti Bank (a továbbiakban: MNB) felhívására igazolja, hogy az auditált elektronikus hírközlő eszköz bevezetése előtt előzetes értékelést végzett. Ennek keretében a szolgáltató az MNB-nek bemutatja az értékelés eredményét, valamint azt, hogy a megoldás alkalmazása megfelel-e az érintett ügyféltípus, szolgáltatás, földrajzi jellemző és termék tekintetében azonosított pénzmosási és terrorizmusfinanszírozással kapcsolatos kockázatoknak.

6. § A szolgáltató csak abban az esetben alkalmazhatja az auditált elektronikus hírközlő eszközt, ha az 5. § szerinti előzetes értékelés alapján megbizonyosodott arról, hogy az a belső kontrollrendszerébe integrálható, valamint hogy a szolgáltató képes arra, hogy megfelelően kezelje az auditált elektronikus hírközlő eszköz alkalmazásából eredő, a pénzmosással és terrorizmusfinanszírozással összefüggő kockázatokat.

3. Az elektronikus ügyfél-átvilágítással kapcsolatos szabályzat

7. § (1) A szolgáltató elektronikus ügyfél-átvilágítás esetében – az ügyfél azonosítása, személyazonosság-igazoló ellenőrzése, valamint az üzleti kapcsolat céljára és tervezett jellegére vonatkozó értékelés és információszerzés érdekében – olyan kockázatérzékenységi alapú elektronikus ügyfél-átvilágítási szabályzatot és eljárásrendet (a továbbiakban együtt: elektronikus ügyfél-átvilágítási szabályzat) készít, amely tartalmazza a szolgáltató

által alkalmazott valamennyi auditált elektronikus hírközlő eszköz útján végzett elektronikus ügyfél-átvilágítás teljesítésének szabályait. Az elektronikus ügyfél-átvilágítási szabályzat a szolgáltató döntése szerint a Pmt. 65. § (1) bekezdése szerinti belső szabályzatának részét is képezheti.

(2) Az elektronikus ügyfél-átvilágítási szabályzat tartalmazza legalább

1. az elektronikus ügyfél-átvilágítás során az információk gyűjtésére, ellenőrzésére és rögzítésére bevezetett auditált elektronikus hírközlő eszköz általános leírását, jellemzőinek és működésének ismertetését;
2. azokat a helyzeteket, amikor az adott auditált elektronikus hírközlő eszköz alkalmazható, beleértve az auditált elektronikus hírközlő eszköz útján végzett ügyfél-átvilágításra alkalmas ügyfelek, termékek és szolgáltatások kategóriájának leírását, figyelembe véve az ügyfelekkel, országokkal vagy földrajzi területekkel, termékekkel, szolgáltatásokkal, ügyletekkel és szállítási csatornákkal kapcsolatos kockázati tényezőket, valamint a szolgáltató kockázatértékelésében azonosított és értékelt kockázati tényezőket;
3. annak leírását, hogy mely lépések automatizáltak teljes mértékben, melyek és milyen terjedelemben igényelnek emberi beavatkozást, valamint a beavatkozásra vonatkozó eljárást;
4. azokat a kontrollmechanizmusokat, amelyek biztosítják, hogy az ügyféllel kötött első ügyletet csak akkor hajtsa végre a szolgáltató, ha valamennyi kötelező ügyfél-átvilágítási intézkedés elvégzésre került;
5. azoknak a bevezető és rendszeres képzési programoknak az előírását, amelyek biztosítják a szolgáltató foglalkoztatottjának naprakész ismereteit az auditált elektronikus hírközlő eszköz működésével, a kapcsolódó kockázatokkal, valamint az ilyen kockázatok mérséklését célzó intézkedésekkel kapcsolatban;
6. az auditált elektronikus hírközlő eszköz értékelésének hatókörét, gyakoriságát, lépéseit és a nyilvántartás vezetésére vonatkozó követelményeket;
7. az auditált elektronikus hírközlő eszköz útján gyűjtött adatok minőségének, teljességének, pontosságának és megfelelőségének folyamatos biztosítása érdekében tett lépéseket, amelyeknek arányban kell állniuk a szolgáltatót érintő, pénzmosással és terrorizmusfinanszírozással kapcsolatos kockázatokkal;
8. az auditált elektronikus hírközlő eszközre vonatkozó rendszeres felülvizsgálatok hatókörét és gyakoriságát;
9. az eseti felülvizsgálatokra okot adó körülményeket, figyelemmel a 9. § (2) bekezdésében foglaltakra;
10. az auditált elektronikus hírközlő eszköz útján végzett ügyfél-átvilágítás hatékonyságára és eredményességére hatással lévő kockázat vagy hiba kiküszöbölését célzó korrekciós intézkedéseket, figyelemmel a 10. §-ban foglaltakra;
11. az ügyfél azonosításához szükséges információk körét, azon dokumentumok, adatok vagy információk típusait, amelyeket a szolgáltató az ügyfél személyazonosságának ellenőrzéséhez felhasznál, valamint az említett információk ellenőrzésének módját;
12. azon információk körét, amelyekre az ügyfél azonosítása, személyazonosságának igazoló ellenőrzése, valamint az üzleti kapcsolat céljára és tervezett jellegére vonatkozó értékelés és információszerzés érdekében szükség van;
13. azon információk körét, amelyeket az ügyfél az online felületen manuálisan ad meg, beleértve annak ellenőrzését is, továbbá amit a szolgáltató automatikusan rögzít az ügyfél által rendelkezésre bocsátott dokumentumok alapján, valamint amit a szolgáltató más belső vagy külső forrásokból gyűjt össze;
14. annak szabályait, hogy mely kategóriákba tartozó jogi személyek ügyfél-átvilágítása végezhető el az auditált elektronikus hírközlő eszköz útján, figyelembe véve az egyes kategóriákhoz kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázatok szintjét, illetve az azonosító információk validálásához szükséges emberi beavatkozás mértékét;
15. azokat az üzleti-kapcsolat létesítése során alkalmazott szabályokat, amelyek előírják, hogy hogyan módosítják saját dokumentációs sablonjaikat, milyen dokumentumokat fogadnak el, és ezen dokumentumok ellenőrzésére milyen kontrollmechanizmusokat alkalmaznak; valamint
16. az ügyfél-átvilágítás kiszervezés keretében ellátott funkcióinak és tevékenységeinek felsorolását és szabályait.

(3) Az elektronikus ügyfél-átvilágítási szabályzatnak alkalmasnak kell lennie arra, hogy a szolgáltató meg tudjon felelni az e rendeletben előírt követelményeknek.

8. § (1) A szolgáltató Pmt. 63. § (5) bekezdése szerint kijelölt megfelelési vezetője – az ügyfél-átvilágítási követelményeknek való megfelelést szolgáló szabályzatok és eljárásrendek kidolgozására vonatkozó általános feladata részeként – gondoskodik arról, hogy a szolgáltató az elektronikus ügyfél-átvilágítási szabályzatot hatékonyan hajtsa végre, rendszeresen, jogszabályi, belső szabályozási vagy alkalmazási környezetben, a technológiában vagy munkafolyamatban bekövetkező lényegi változás esetén, de legalább évente, felülvizsgálja és aktualizálja.

(2) A szolgáltató irányítási funkciót betöltő testülete jóváhagyja az elektronikus ügyfél-átvilágítási szabályzatot, a kijelölt felelős vezető útján pedig felügyeli annak végrehajtását.

4. Az elektronikus ügyfél-átvilágítás folyamatos ellenőrzése

9. § (1) A szolgáltató folyamatosan – rendszeres és eseti felülvizsgálatok révén – ellenőriz minden általa alkalmazott auditált elektronikus hírközlő eszközt a belső szabályzatainak és a jogszabályok elvárásainak megfelelő működés biztosítása érdekében.

(2) A szolgáltató eseti felülvizsgálatot végez legalább a következő esetekben:

a) a szolgáltatót érintő, pénzmosással és terrorizmusfinanszírozással kapcsolatos kockázatoknak való kitettségben bekövetkezett változások,

b) az auditált elektronikus hírközlő eszköz működésében a monitoring-, audit-, külső ellenőrzési funkció által vagy felügyeleti tevékenység során feltárt hiányosságok,

c) a visszaélési kísérletek érzékelhető fokozódása, valamint

d) a jogi vagy egyéb szabályozási keretrendszer változása.

10. § (1) A szolgáltató korrekciós intézkedési tervvel rendelkezik olyan kockázat felmerülése vagy hiba feltárása esetére, amely hatással van az auditált elektronikus hírközlő eszköz útján végzett elektronikus ügyfél-átvilágítás hatékonyságára és eredményességére.

(2) A korrekciós intézkedések kiterjednek legalább az alábbiakra:

a) az összes érintett üzleti kapcsolat felülvizsgálatára annak értékelése céljából, hogy a szolgáltató megfelelő ügyfél-átvilágítási szintet alkalmazott-e a személyazonosság-igazoló ellenőrzésére, a tényleges tulajdonos azonosítására és az üzleti kapcsolat céljának és jellegének feltárására vonatkozó jogszabályi rendelkezéseknek való megfelelés érdekében, különös figyelemmel azokra, amelyek esetén a pénzmosással és terrorizmusfinanszírozással kapcsolatos kockázat a legmagasabb; és

b) figyelembe véve az a) pont szerinti felülvizsgálat során szerzett információkat, annak értékelésére, hogy az érintett üzleti kapcsolat esetében szükség van-e

ba) további ügyfél-átvilágítási intézkedésekre,

bb) a Pmt. 65. §-a szerinti belső szabályzatban meghatározott korlátozások alkalmazására,

bc) az üzleti kapcsolat felmondására,

bd) a pénzügyi információs egység felé bejelentés megtételére, továbbá

be) az ügyfél kockázati szintbe történő besorolásának módosítására.

11. § (1) A szolgáltató biztosítja, hogy az auditált elektronikus hírközlő eszköz folyamatos megfelelőségének és megbízhatóságának nyomon követésére a leghatékonyabb módszert alkalmazza.

(2) Az (1) bekezdésben foglaltak teljesítéséhez a szolgáltató az automatizált kritikus riasztások és értesítések mellett az alábbi módszerek közül legalább az egyiket alkalmazza:

a) minőségbiztosítási vizsgálat,

b) külső ellenőrzési funkció,

c) a minőségre vonatkozó rendszeres, automatizált jelentések,

d) mintavételen alapuló vizsgálat,

e) manuális felülvizsgálat.

12. § A szolgáltató a felülvizsgálati és korrekciós intézkedésekről nyilvántartást vezet, és az MNB felhívására bemutatja, hogy milyen felülvizsgálatokat és korrekciós intézkedéseket hajtott végre az általa alkalmazott auditált elektronikus hírközlő eszköz teljes alkalmazási időtartama alatt feltárt hiányosságok kezelésére.

5. Az auditált elektronikus hírközlő eszköz és működtetésének minimumkövetelményei, valamint auditálásának módja

13. § Az elektronikus hírközlő eszköz akkor auditálható és működtethető, ha legalább az alábbi informatikai biztonsági követelményeknek megfelel:

a) elemei azonosíthatók és dokumentáltak,

b) üzemeltetési folyamatai szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek,

c) változáskezelési folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverkódban bekövetkező változások csak tesztelt és dokumentált módon valósulhassanak meg,

d) adatmentési és -visszaállítási rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás az üzemeltetési szabályzat szerinti gyakorisággal és dokumentáltan tesztelt,

e) a felhasználói hozzáférés mind alkalmazási, mind infrastruktúra-szinten szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött,

f) a felállított végfelhasználói hozzáférések egységes, zárt rendszert alkotnak, biztosítják az azonosítási folyamat megvalósulását, továbbá felhasználóinak tevékenysége naplózott, a rendkívüli eseményekről automatikus figyelmeztetések generálódnak,

g) a hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek, a kiemelt jogosultságokkal elvégzett tevékenység naplózott, a naplófájlok sérthetetlensége biztosított, és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak,

h) a távoli hozzáférés szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött,

i) a vírusok és más rosszindulatú kódok és cselekmények elleni védelem biztosított,

j) adatkommunikációja és rendszerkapcsolatai dokumentáltak és ellenőrzöttek, az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosított,

k) a katasztrófa-helyreállítási terv rendszeresen tesztelt,

l) karbantartása szabályozott,

m) adathordozóinak védelme szabályozott, továbbá biztosított, hogy az adathordozókhoz csak az arra jogosult személyek és csak az adatkezelési cél teljesülése érdekében férnek hozzá, ennek felülvizsgálata és ellenőrzése rendszeresen megtörténik,

n) saját kontrolljai és az üzemeltetési szabályzat gondoskodnak a rendszerelemek és a kezelt információk sértetlenségéről és védelméről, és

o) biztosított a megfelelő szintű fizikai védelem, az elkülönített környezet és az egyes biztonsági események detektálása és kezelése.

14. § A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában gondoskodik arról, hogy

a) az ügyféllel felépített elektronikus átviteli csatornán keresztül folyó távadatátvitel megfelelően biztonságos, titkosított, bizalmas, sértetlen és hiteles legyen,

b) az ügyfél megkapja a szolgáltatás igénybevételének feltételeiről való tájékoztatást, beleértve a szolgáltatás biztonságára vonatkozó ügyféloldali felelősségről, valamint az adatkezelésről szóló tájékoztatást is,

c) a szolgáltatóoldali ügyfél-átvilágításban – amennyiben emberi beavatkozásra szükség van – csak a szükséges mértékben és csak olyan személy vegyen részt, aki – a szolgáltató által alkalmazott megoldástól függően – a közvetett vagy közvetlen elektronikus ügyfél-átvilágítás végrehajtásához szükséges jogi, technikai és biztonsági oktatásban részesült,

d) az elektronikus hírközlő eszközre és az elektronikus ügyfél-átvilágítási folyamatra vonatkozó olyan vizsgálati jelentéssel rendelkezzen, amely igazolja, hogy ezek informatikai védelme a biztonsági kockázatokkal arányos, és megfelel különösen a 13. §-ban foglalt követelményeknek,

e) a d) pont szerinti vizsgálati jelentés a jogi szabályozásban, az alkalmazott technológiában vagy az üzleti folyamatban történt releváns, a működésre kiható változás esetén, de legalább kétévente megújításra kerüljön,

f) a d) pont szerinti vizsgálati jelentést olyan, az Európai Gazdasági Térség valamely tagállamában bejegyzett szervezet állítsa ki, amely szervezetnél a vizsgálatban igazolhatóan részt vevő személy rendelkezik legalább

fa) az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Systems Auditor (CISA);

fb) az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Security Manager (CISM) vagy

fc) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP)

képesítéssel és minősítéssel,

g) az elektronikus ügyfél-átvilágítás során a szolgáltató birtokába jutott személyes adatokat és személyes adatnak nem minősülő adatokat az adatkezelés időtartama alatt az érintett részére hozzáférhetővé tegye, átadja, valamint

h) az elektronikus ügyfél-átvilágítás folyamatáról elektronikusan eltárolt adatok oly módon kerüljenek rögzítésre, hogy azok a későbbiekben alkalmasak legyenek az ügyfél-átvilágításra vonatkozó rendelkezések betartásának és az ügyfél-átvilágítási intézkedések végrehajtásának utólagos ellenőrzésére.

15. § Amennyiben a szolgáltató a dokumentumokból származó információk automatikus olvasására alkalmas funkciókat használ, gondoskodik arról, hogy ezek az eszközök pontosan és következetesen rögzítsék az információkat.

16. § A szolgáltató teljeskörűen azonosítja és kezeli az elektronikus ügyfél-átvilágítási folyamat használatához kapcsolódó IKT- és biztonsági kockázatokat, beleértve azokat az eseteket is, amikor a szolgáltató az elektronikus ügyfél-átvilágítást vagy annak egy részét kiszervezi.

17. § Amennyiben a szolgáltató az elektronikus ügyfél-átvilágítási folyamat lebonyolítására többcélú eszközt használ, a szolgáltató a kockázatokkal arányosan gondoskodik arról, hogy a többcélú eszközön az alkalmazás vagy a szoftverkód biztonságos környezetben kerüljön futtatásra. A szolgáltató további biztonsági intézkedéseket hajt végre az applikáció vagy a szoftverkód és az összegyűjtött adatok biztonságának és megbízhatóságának biztosítása érdekében.

18. § Az auditált elektronikus hírközlő eszköznek alkalmasnak kell lennie az ügyfélre vonatkozó, a Pmt. 7–10. §-a szerinti valamennyi adat, dokumentáció és információ befogadására, automatizált megoldás esetén az információ feldolgozására és ellenőrzésére is, kivéve azon dokumentumokat, amelyeket az ügyfél a szolgáltató elektronikus ügyfélazonosító és nyilatkozattételi rendszerében is benyújthat.

6. Az elektronikus ügyfél-átvilágítás közös szabályai

19. § (1) A szolgáltató az elektronikus ügyfél-átvilágítás során a Pmt. szerinti ügyfél-azonosítást és személyazonosság-igazoló ellenőrzést végez, felhívja az ügyfelet az ügyfélre irányadó, a Pmt. szerinti nyilatkozatok megtételére és okiratok bemutatására, továbbá értékeli az üzleti kapcsolat célját és tervezett jellegét, és ehhez indokolt esetben alátámasztó információkat szerez be.

(2) A szolgáltató az elektronikus ügyfél-átvilágítás rendszerét a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló törvényben foglalt, a fogyatékos személyt megillető jogokra figyelemmel alakítja ki.

(3) A szolgáltató az elektronikus ügyfél-átvilágításra vonatkozó követelmények teljesülését az elektronikus ügyfél-átvilágítási szabályzatban meghatározott foglalkoztatottja által, az elektronikus ügyfél-átvilágítási szabályzatban meghatározott módon ellenőrzi. Az ellenőrzés és az arra vonatkozó szabályozás kiterjed a munkamenet rögzítésére vonatkozó követelmények betartására is.

20. § (1) A szolgáltató az elektronikus ügyfél-átvilágítást közvetlen, illetve közvetett elektronikus módon végezheti.

(2) Auditált elektronikus hírközlő eszköz igénybevétele esetén, ha a szolgáltató a tényleges tulajdonosi és kiemelt közszereplői nyilatkozatokat, okmánymásolatokat, ügyfélismereti kérdőíveket, valamint a pénzeszköz, illetve vagyon forrásáról szóló nyilatkozatokat elektronikus ügyfélazonosító és nyilatkozattételi rendszerének használatával szerzi be, ezen nyilatkozatok és okmánymásolatok beszerzéséig, valamint az ügyfél egyedi kockázatbesorolása alapján elvégzendő valamennyi ügyfél-átvilágítási intézkedés megtételéig ügylet nem teljesíthető.

(3) A (2) bekezdés szerinti korlátozás nem alkalmazandó, ha az okmánymásolat megküldése okmánycsere vagy adatváltozás miatt korábban már teljeskörűen átvilágított ügyfél esetében szükséges.

21. § A szolgáltató ellenőrzi és biztosítja, hogy

a) az auditált elektronikus hírközlő eszközön keresztül szerzett információk naprakészek, és megfelelnek a Pmt. 12. §-ában meghatározott követelményeknek, és

b) a kép-, hang-, valamint kép- és hangfelvételek és adatok olvasható formátumban és megfelelő minőségben rögzítettek úgy, hogy az ügyfél egyértelműen felismerhető legyen.

22. § Az elektronikus ügyfél-átvilágítás során gyűjtött megőrzendő dokumentumokat és információkat a szolgáltató időbélyegzővel látja el, és biztonságosan eltárolja. A szolgáltató biztosítja, hogy a tárolt nyilvántartások tartalma olvasható formátumban álljon rendelkezésre, és lehetővé tegye az utólagos ellenőrzést.

23. § (1) A szolgáltató megfelelő mechanizmusokat vezet be az automatikusan gyűjtött információk megbízhatóságának biztosítása érdekében.

(2) A szolgáltató gondoskodik kontrollmechanizmus alkalmazásáról a kapcsolódó kockázatok kezelésére, beleértve az adatok automatikus rögzítésével kapcsolatos kockázatokat, ezen belül az ügyfél készüléke helymeghatározásának megzavarásával, illetve hamis IP-címek, virtuális magánhálózatok (VPN) vagy más hasonló szolgáltatások használatával kapcsolatos kockázatokat.

24. § (1) Amennyiben a szolgáltató biometrikus adatok használata révén ellenőrzi a természetes személy ügyfél személyazonosságát, gondoskodik arról, hogy a biometrikus adatok kellően egyediek legyenek ahhoz, hogy egyértelműen egyetlen természetes személyhez lehessen kötni őket.

(2) A szolgáltató algoritmusokat használ annak ellenőrzésére, hogy a benyújtott személyazonosító okmányon megadott biometrikus adatok ténylegesen az adott természetes személy ügyfélhez tartoznak-e. Kockázatérzékenységi megközelítéssel a benyújtott személyazonosító okmányon megadott biometrikus adatok ellenőrzéséhez további kontrollmechanizmusokat is meghatároz a szolgáltató.

25. § A szolgáltató kockázatérzékenységi megközelítés alapján az alábbiak közül legalább egy kontrollmechanizmust vagy más hasonló intézkedést alkalmaz az ellenőrzési folyamat megbízhatóságának fokozása érdekében:

a) az első kifizetésnek az ügyfél nevére szóló (kizárólagos vagy közös tulajdonú), az Európai Unió területén belül vagy olyan harmadik országban működő szabályozott hitel- vagy pénzintézetnél vezetett számlára történő teljesítése, amely ország a pénzmosás és a terrorizmusfinanszírozás elleni küzdelem tekintetében legalább a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről, a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról, valamint a 2005/60/EK európai parlamenti és tanácsi irányelv és a 2006/70/EK bizottsági irányelv hatályon kívül helyezéséről szóló, 2015. május 20-i 2015/849/EU európai parlamenti és tanácsi irányelvben előírtaknak megfelelő vagy azoknál szigorúbb követelményeket alkalmaz;

b) egyszer használatos és korlátozott időre szóló, véletlenszerűen generált azonosító kód küldése az ügyfélnek a távoli ellenőrzési folyamat során való jelenlét megerősítésére, és a kód ügyfél általi visszaküldése a szolgáltató által választott kommunikációs formában;

c) biometrikus adatok gyűjtése más, független és megbízható közhiteles forrásokból gyűjtött adatokkal történő összehasonlítás céljából;

d) telefonos kapcsolattartás az ügyféllel;

e) közvetlen – elektronikus és postai – küldemények küldése az ügyfélnek.

7. Az elektronikus ügyfél-átvilágítás kiszervezésének szabályai

26. § (1) A szolgáltató az elektronikus ügyfél-átvilágítás vagy annak egy részének kiszervezése előtt megbizonyosodik arról, hogy

a) a kiszervezett tevékenységet végző fél auditált elektronikus hírközlő eszközzel összefüggő elektronikus ügyfél-átvilágítási folyamatai és eljárásai, valamint az ezzel összefüggésben gyűjtött információk és adatok elégségesek, és összhangban vannak a jogszabályokban meghatározott követelményekkel,

b) a kiszervezett tevékenységet végző fél biztosítani tudja az ügyfél, illetve a szolgáltatók közötti üzleti kapcsolatok folytonosságát az olyan eseményekkel szembeni védelem érdekében, amelyek során hiányosságokra derülhet fény a kiszervezett tevékenységet végző fél által auditált elektronikus hírközlő eszköz igénybevételével végzett elektronikus ügyfél-átvilágítási folyamattal kapcsolatban, valamint

c) a kiszervezett tevékenységet végző fél által működtetett auditált elektronikus hírközlő eszköz megfelel az e rendeletben meghatározott követelményeknek, és mindenkor az e rendelet szerinti érvényes vizsgálati jelentéssel rendelkezik.

(2) A szolgáltató biztosítja, hogy a kiszervezés nem eredményezi az üzleti kapcsolat létesítésével kapcsolatos döntési jogkör átadását.

27. § (1) A szolgáltató az elektronikus ügyfél-átvilágítási folyamat vagy annak egy részének kiszervezése előtt és a kiszervezés során kockázatérzékenységi megközelítés alapján

a) rendszeres jelentéstételi kötelezettség előírásával, folyamatos nyomon követéssel, helyszíni szemlével, illetve mintavételes vizsgálat útján történő ellenőrzéssel biztosítja, hogy a kiszervezett tevékenységet

végző fél a kiszervezési megállapodással összhangban ténylegesen végrehajtsa a szolgáltató elektronikus ügyfél-átvilágításra vonatkozó belső szabályait, és azoknak megfelelően járjon el,

b) a személyzet képzésével, a technológiai alkalmasságával és az adatirányítással összefüggő értékeléseket végez annak biztosítása érdekében, hogy a kiszervezett tevékenységet végző fél megfelelő személyi és tárgyi feltételekkel rendelkezzen az elektronikus ügyfél-átvilágítási folyamat, részfolyamat elvégzésére, valamint

c) biztosítja, hogy a kiszervezett tevékenységet végző fél előzetesen tájékoztassa a szolgáltatót az elektronikus ügyfél-átvilágítási folyamattal kapcsolatban felmerült bármely módosítási javaslatról.

(2) A szolgáltató gondoskodik arról, hogy a kiszervezési megállapodás tartalmazza az érintetti joggyakorlással kapcsolatos adatvédelmi kérelmek teljesítésének rendjét.

28. § Amennyiben a kiszervezett tevékenységet végző fél az elektronikus ügyfél-átvilágítási folyamat során az ügyfélre vonatkozó adatokat – többek között kép- és hangfelvételeket, továbbá dokumentumokat – tárol, a szolgáltató biztosítja, hogy

a) a kiszervezett tevékenységet végző fél kizárólag a szükséges ügyfél adatokat gyűjtse és tárolja, a Pmt. 56–58. §-ában meghatározott adatmegőrzési időtartamnak megfelelően,

b) az adatokhoz való hozzáférés szigorúan korlátozott és nyilvántartott legyen, valamint

c) a kiszervezett tevékenységet végző fél megfelelő biztonsági intézkedéseket hajtson végre a tárolt adatok védelmének biztosítása érdekében.

8. A közvetett elektronikus ügyfél-átvilágítás formái és szabályai

29. § (1) A szolgáltató a közvetett elektronikus ügyfél-átvilágítást olyan eszköz útján végzi, amely képes

a) megállapítani, hogy az átvilágítás alanyaként a távoli helyszínen megjelenő ügyfél valós, élő személy, az auditált elektronikus hírközlő eszközt valós időben személyesen használja, és az élő kép nem manipulált, valamint

b) az ügyfélről az ügyfél-átvilágítás során készített fényképet és az átvilágításhoz felhasznált okiratban szereplő képmást összehasonlítani olyan módon, hogy az alapján kétséget kizáróan megállapítható, hogy a személyazonosság igazolására alkalmas hatósági igazolványban szereplő személy azonos a fényképfelvételen szereplő személlyel.

(2) A szolgáltató közvetett elektronikus ügyfél-átvilágítás alkalmazása esetében az auditált elektronikus hírközlő eszköz vonatkozásában biztosítja az ügyfél-átvilágításra vonatkozó feltételeket, ha

a) az ügyfél a közvetett elektronikus ügyfél-átvilágítás feltételeit részletesen megismerte, és ahhoz kifejezetten hozzájárult,

b) erős ügyfél-hitelesítést alkalmaz,

c) a képátvitelt lehetővé tévő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas az ügyfél nemének, korának, arcjellemzőinek felismerésére és az ügyfél által bemutatott fényképes azonosító okmánnyal való összevetésre, a bemutatott személyazonosság igazolására alkalmas hatósági igazolvány biztonsági elemeinek azonosítására, valamint

d) az ügyfél-átvilágítási folyamat szabályozott és a szolgáltató belső szabályzatában meghatározott módon folyamatosan ellenőrzött.

30. § (1) A szolgáltató a közvetett elektronikus ügyfél-átvilágítás során a szolgáltató és az ügyfél között létrejött teljes munkamenetet, az ügyfél közvetett elektronikus ügyfél-átvilágítással kapcsolatos részletes tájékoztatását és az ügyfélnek a közvetett elektronikus ügyfél-átvilágításhoz történő kifejezett hozzájárulását visszakereshető módon rögzíti.

(2) A közvetett elektronikus ügyfél-átvilágítás érdekében a szolgáltató

a) gondoskodik arról, hogy olyan felvétel készüljön az ügyfélről, amelyen arcképe felismerhető és rögzíthető,

b) meggyőződik arról, hogy az ügyfél valós, élő személy, az auditált elektronikus hírközlő eszközt valós időben személyesen használja, és az élő kép nem manipulált, valamint

c) olyan módon rögzíti az ügyfél-átvilágításhoz használt okiratokat, hogy az azokon található biztonsági elemek és adatsorok felismerhetők és tárolhatók legyenek.

(3) A közvetett elektronikus ügyfél-átvilágítást végző szolgáltató megbizonyosodik arról, hogy a felhasznált személyazonosság igazolására alkalmas hatósági igazolvány alkalmas a közvetett elektronikus ügyfél-átvilágítás elvégzésére, így

a) a személyazonosság igazolására alkalmas hatósági igazolvány egyes elemei és azok elhelyezkedése megfelel a személyazonosság igazolására alkalmas hatósági igazolványt kiállító hatóság előírásainak, valamint

b) az egyes biztonsági elemek – így különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetők és sérülésmentesek.

(4) A szolgáltató megbizonyosodik arról, hogy

a) az ügyfél arcképe felismerhető és azonosítható az általa bemutatott személyazonosság igazolására alkalmas hatósági igazolványon látható arcképpel, valamint

b) a Pmt. által előírt azonosítási adatok teljeskörűen beszerzésre kerültek, és a személyazonosság igazolására alkalmas hatósági igazolványokon megtalálható adatok logikailag megfeleltethetők az ügyfélről a szolgáltatónál rendelkezésre álló adatokkal.

31. § (1) A szolgáltató a közvetett elektronikus ügyfél-átvilágítási eljárás során az ügyfélről rögzített fényképet és a személyazonosság igazolására alkalmas hatósági igazolványban szereplő képmást az auditált elektronikus hírközlő eszköz segítségével összehasonlítja.

(2) A Pmt. által előírt, az ügyfél egyedi kockázatbesorolása alapján elvégzett valamennyi ügyfél-átvilágítási intézkedés eredményének ismeretében a szolgáltató a rögzítést követő 2 banki napon belül értesítést küld az ügyfélnek az ügyfél-átvilágítás eredményéről.

32. § (1) A szolgáltató nem hajtja végre a közvetett elektronikus ügyfél-átvilágítást, ha

a) az ügyfél az ügyfél-átvilágítás során visszavonja az adatrögzítéshez vagy a közvetett elektronikus ügyfél-átvilágítás elvégzéséhez adott hozzájárulását,

b) az ügyfél által bemutatott személyazonosság igazolására alkalmas hatósági igazolvány fizikai és adattartalmi követelményei nem felelnek meg a 30. § (3) bekezdésében foglalt feltételeknek,

c) az ügyfél által bemutatott személyazonosság igazolására alkalmas hatósági igazolvány vizuális azonosításának feltételei nem adottak,

d) a szolgáltató nem tudja elkészíteni a képfelvételt, vagy nem tudja rögzíteni a 30. § (1) bekezdésében meghatározott munkamenetet,

e) az ügyfél-átvilágítás során ellentmondás vagy bizonytalanság lép fel, vagy

f) az azonosítási folyamat nem folytatható, mert műszaki hiányosságokat vagy váratlan csatlakozási fennakadásokat észlelnek.

(2) A szolgáltató az ügyfelet haladéktalanul személyes megjelenés mellett világítja át, vagy közvetlen elektronikus ügyfél-átvilágítást végez, ha az ügyfél tevékenysége vonatkozásában felmerül a pénzmosás vagy terrorizmusfinanszírozás kockázata és az ügyfél együttműködik a megváltozott módon történő ügyfél-átvilágítás végrehajtásában, és ezáltal a szolgáltató a felfedés tilalmát nem sérti meg.

33. § (1) A szolgáltató a közvetett elektronikus ügyfél-átvilágítást

a) Központi Azonosítási Ügynök (a továbbiakban: KAÜ szolgáltatás) igénybevételével,

b) elektronikus tárolóelemet tartalmazó, személyazonosság igazolására alkalmas hatósági igazolványból az ügyfél azonosításra alkalmas, hiteles természetes azonosító adatok kiolvasásával,

c) a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (a továbbiakban: Dáptv.) 46. § (1) bekezdés a) pontja szerinti eAzonosítás igénybevételével vagy

d) egyéb módon, a 38. § szerinti korlátozásra figyelemmel

végzi el.

(2) A szolgáltató az (1) bekezdés c) pontja szerinti eAzonosítással végzi a közvetett elektronikus ügyfél-átvilágítást, ha az ügyfél a Dáptv. szerinti elektronikus azonosítási szolgáltatással azonosítja magát.

34. § A 33. § (1) bekezdés a) pontjában foglalt elektronikus azonosítási szolgáltatás megvalósítása érdekében a szolgáltató

a) az auditált elektronikus hírközlő eszköz útján csatlakozik a KAÜ szolgáltatáshoz, és annak segítségével biztosítja, hogy az ügyfél-átvilágítás során az ügyfél azonosítsa magát, és

b) az általa biztosított auditált elektronikus hírközlő eszköz útján a KAÜ-től visszakapott információk alapján ellenőrzi az ügyfél személyazonosságát.

35. § (1) A szolgáltató a 33. § (1) bekezdés b) pontja szerint végzi a közvetett elektronikus ügyfél-átvilágítást, ha

a) az ügyfél által bemutatott, elektronikus tárolóelemet tartalmazó, személyazonosság igazolására alkalmas hatósági igazolványból a szolgáltató az ügyfél személyes azonosításra alkalmas, hiteles természetes személyazonosító adatait és a személyazonosság igazolására alkalmas hatósági igazolványt kiállító hatóság által az ügyfélről készített fényképfelvételt az auditált elektronikus hírközlő eszköz útján elektronikus úton kiolvassa, és összeveti az ügyfél által megadott, illetve az azonosítás során felvett adatokkal és készített fényképfelvétellel, és

b) az adatok és fényképfelvételek auditált elektronikus hírközlő eszközzel történő összehasonlítása során kétséget kizáróan megállapítható, hogy a személyazonosság igazolására alkalmas hatósági igazolványban szereplő személy azonos az auditált elektronikus hírközlő eszközzel az átvilágítás során készített fényképfelvételen szereplő személlyel, valamint hogy a személyazonosság igazolására alkalmas hatósági igazolványt arra hatáskörrel rendelkező hatóság állította ki, és az elektronikusan tárolt és kiolvasott adatok változatlanok és hitelesek.

(2) A szolgáltató a 32. §-ban meghatározott eseteken túlmenően nem hajtja végre az ügyfél-átvilágítást akkor sem, ha az átvilágítás során nem sikerül az elektronikus személyazonosító igazolvány elektronikus tároló eleméből minden vonatkozó adatot kiolvasni, kétség merül fel a személyazonosság igazolására alkalmas hatósági igazolvány vagy a személyazonosság igazolására alkalmas hatósági igazolványból kiolvasott adatok hitelessége vonatkozásában, vagy a kiolvasott adatok alapján a szolgáltató nem képes az ügyfelet kétséget kizáró módon azonosítani.

36. § A 33. § (1) bekezdés c) pontjában meghatározott közvetett elektronikus ügyfél-átvilágítás alkalmazása esetében a Dáptv. és a Dáptv.-ben foglalt felhatalmazás alapján kiadott jogszabályban meghatározott követelmények az irányadók.

37. § A szolgáltató a 34. és 35. §-ban meghatározott esetben az ügyfél által az auditált elektronikus hírközlő eszköz használatával bemutatott személyazonosság igazolására alkalmas hatósági igazolvány érvényességét ellenőrzi, ideértve különösen, hogy a személyazonosság igazolására alkalmas hatósági igazolvány nem érvénytelen-e, nem került-e visszavonásra vagy érvénytelenítésre, valamint nem jelentették-e elvesztését, eltulajdonítását, megsemmisülését, megrongálódását, megtalálását, illetve nem adták-e le az illetékes hatóság számára.

38. § A szolgáltató a 33. § (1) bekezdés d) pontja alapján közvetett elektronikus ügyfél-átvilágítást akkor végezhet, ha az ügyfél tevékenységét az üzleti kapcsolat létrehozásának időpontjától számítva egy évig megerősített eljárásban nyomon követi.

9. A közvetlen elektronikus ügyfél-átvilágítás szabályai

39. § (1) A közvetlen elektronikus ügyfél-átvilágítás során a szolgáltató a 29. § (1) bekezdésében meghatározottaknak megfelelő eszköz útján összeveti az ügyfélről készített fényképet és az átvilágításhoz felhasznált személyazonosság igazolására alkalmas hatósági igazolványban szereplő képmást. Az ügyfél-átvilágítás megfelelő, ha kétséget kizáróan megállapítható, hogy a személyazonosság igazolására alkalmas hatósági igazolványban szereplő személy azonos a fénykép- vagy videófelvételen szereplő személlyel.

(2) A szolgáltató a közvetlen elektronikus ügyfél-átvilágítást egy, a célnak megfelelő helyiségben végzi.

(3) A közvetlen elektronikus ügyfél-átvilágítást csak a szolgáltató olyan vezetője és foglalkoztatottja végezheti, aki a szolgáltató által előzőleg e tevékenység ellátására szervezett képzésen részt vett, a képzés során megfelelő ismereteket szerzett az auditált elektronikus hírközlő eszköz útján végzett ügyfél-átvilágításhoz kapcsolódó megtévesztési technikák alkalmazásának felismerésére és megelőzésére, és aki a képzést követően eredményes vizsgát tett.

(4) Az ügyfél és a szolgáltató foglalkoztatottja közötti összejátszás elkerülése érdekében a szolgáltató biztosítja a közvetlen elektronikus ügyfél-átvilágítások vonatkozásában a részt vevő foglalkoztatott véletlenszerű beosztását.

40. § (1) A szolgáltató kérdés-felelet formájú útmutatót készít, amely meghatározza a közvetlen elektronikus ügyfél-átvilágítás egymást követő lépéseit, valamint a foglalkoztatottól elvárt intézkedéseket. Az útmutató iránymutatást tartalmaz a közvetlen elektronikus ügyfél-átvilágítás során gyanús viselkedést jelző pszichológiai tényezők és egyéb jellemzők megfigyelésére és azonosítására vonatkozóan.

(2) A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában biztosítja az ügyfél átvilágítására vonatkozó feltételeket, amennyiben

a) az ügyfél a közvetlen elektronikus ügyfél-átvilágítás feltételeit részletesen megismerte, és ahhoz kifejezetten hozzájárult, az adatkezelésről tájékoztatást kapott, és azt tudomásul vette,

b) a valós idejű kép- és hangátvitelt lehetővé tévő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas az ügyfél nemének, korának, arcjellemzőinek felismerésére, és

c) az ügyfél-átvilágítási folyamat szabályozott és folyamatosan ellenőrzött.

41. § (1) A szolgáltató a közvetlen elektronikus ügyfél-átvilágítás során a szolgáltató és az ügyfél között létrejött teljes kommunikációt, az ügyfél közvetlen elektronikus ügyfél-átvilágítással kapcsolatos részletes tájékoztatását és az ügyfél ehhez történő kifejezett hozzájárulását visszakereshető módon kép- és hangfelvételen rögzíti.

(2) A közvetlen elektronikus ügyfél-átvilágítás során a szolgáltató biztosítja, hogy az ügyfél

a) úgy nézzen bele a kamerába, hogy arcképe felismerhető és rögzíthető legyen,

b) érthető módon közölje a közvetlen elektronikus ügyfél-átvilágításhoz használt személyazonosság igazolására alkalmas hatósági igazolvány azonosítóját, és

c) úgy mozgassa a közvetlen elektronikus ügyfél-átvilágításhoz használt személyazonosság igazolására alkalmas hatósági igazolványát, hogy az azon található biztonsági elemek és adatsorok felismerhetők és rögzíthetők legyenek.

(3) A közvetlen elektronikus ügyfél-átvilágítást végző szolgáltató köteles megbizonyosodni arról, hogy a közvetlen elektronikus ügyfél-átvilágításhoz használt személyazonosság igazolására alkalmas hatósági igazolvány alkalmas a közvetlen elektronikus ügyfél-átvilágítás elvégzésére, így

a) a személyazonosság igazolására alkalmas hatósági igazolvány egyes elemei és azok elhelyezkedése megfelel a személyazonosság igazolására alkalmas hatósági igazolványt kiállító hatóság előírásainak, illetve a vonatkozó jogszabályi előírásoknak,

b) az egyes biztonsági elemek – így különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetők és sérülésmentesek, és

c) a személyazonosság igazolására alkalmas hatósági igazolvány okmányazonosítója megegyezik az ügyfél által közölt okmányazonosítóval, felismerhető és sérülésmentes.

(4) A közvetlen elektronikus ügyfél-átvilágítást végző szolgáltató megbizonyosodik arról, hogy

a) az ügyfél arcképe felismerhető és azonosítható az általa bemutatott személyazonosság igazolására alkalmas hatósági igazolványon látható arckép alapján, és

b) a személyazonosság igazolására alkalmas hatósági igazolványban megtalálható adatok logikailag megfeleltethetők az ügyfélről a szolgáltatónál rendelkezésre álló adatokkal.

(5) A szolgáltató az ügyfél által bemutatott személyazonosság igazolására alkalmas hatósági igazolvány érvényességét ellenőrzi, ideértve különösen, hogy a személyazonosság igazolására alkalmas hatósági igazolvány nem érvénytelen-e, nem került-e visszavonásra vagy érvénytelenítésre, valamint nem jelentették-e elvesztését, eltulajdonítását, megsemmisülését, megrongálódását, megtalálását, illetve nem adták-e le az illetékes hatóság számára.

(6) A szolgáltató egy alfanumerikus kódból álló, központilag, véletlenszerűen generált azonosítási kódot küld az ügyfélnek a szolgáltató választása szerint az ügyfél azonosítására alkalmas e-mail-címre vagy SMS-ben mobiltelefonszámra, amely kódot az ügyfél a közvetlen elektronikus ügyfél-átvilágítás befejezéséig a szolgáltató által választott kommunikációs formában küldi vissza a szolgáltatónak.

42. § A szolgáltató megszakítja a közvetlen elektronikus ügyfél-átvilágítást, ha

a) az ügyfél a közvetlen elektronikus ügyfél-átvilágítás során visszavonja az adatrögzítéshez adott hozzájárulását,

b) az ügyfél által bemutatott személyazonosság igazolására alkalmas hatósági igazolvány fizikai és adattartalmi követelményei nem felelnek meg a 41. § (3) bekezdésében előírt feltételeknek,

c) az ügyfél által bemutatott személyazonosság igazolására alkalmas hatósági igazolvány vizuális azonosításának feltételei nem adottak,

d) a szolgáltató nem tudja elkészíteni a hang- és képfelvételt,

e) az ügyfél nem, nem teljes egészében vagy hibásan küldi vissza az azonosítási kódot,

f) az ügyfél nem tesz nyilatkozatot, vagy a szolgáltató számára észlelhetően befolyás alatt tesz nyilatkozatot, vagy
g) az ügyfél-átvilágítás során ellentmondás vagy bizonytalanság lép fel.

10. Záró rendelkezések

43. § (1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – 2024. július 1-jén lép hatályba.
(2) A 3. alcím 2025. január 1-jén lép hatályba.

44. § (1) A szolgáltató felméri, hogy e rendelet hatálybalépésekor már alkalmazott auditált elektronikus hírközlő eszköze milyen mértékben felel meg az e rendeletben foglaltaknak, és a teljes körű megfelelésig intézkedéseket alkalmaz az auditált elektronikus hírközlő eszköz igénybevételéből eredő releváns kockázatok csökkentése érdekében.
(2) A szolgáltató az (1) bekezdés szerinti értékelés során figyelembe veszi különösen azt, hogy az általa alkalmazott auditált elektronikus hírközlő eszköz kiterjed-e az alábbi kockázatok kezelésére:
a) a hitelesítéssel járó kockázatok és elektronikus ügyfél-átvilágítási szabályzatban meghatározott egyedi kockázatcsökkentő intézkedések, különös tekintettel a személyazonossággal való visszaéléssel kapcsolatos kockázatokra,
b) annak a kockázata, hogy az ügyfél nem azonos azzal a személlyel, akinek kiadja magát, valamint
c) az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt személyazonosító okmányok használatának kockázata, beleértve adott esetben a személyazonossággal való visszaélés felderítésére és megelőzésére szolgáló eszközöket is.
(3) Az e rendelet hatálybalépésének napján már alkalmazott auditált elektronikus hírközlő eszköz tekintetében a szolgáltató 2024. október 31-ig köteles az (1) bekezdés szerinti felmérést elvégezni, és legkésőbb 2025. május 1-jéig megfelelni e rendelet előírásainak.

Virág Barnabás s. k.,
a Magyar Nemzeti Bank alelnöke

A Magyar Nemzeti Bank elnökének 30/2024. (VI. 24.) MNB rendelete a Magyar Nemzeti Bank által felügyelt szolgáltatóknak a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvényben foglalt egyes kötelezettségei végrehajtásának részletszabályairól, valamint e szolgáltatóknak az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszere kidolgozásának és működtetésének minimumkövetelményeiről

A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény 77. § (3) bekezdés a)–c) és e)–k) pontjában kapott felhatalmazás alapján,
a 9. alcím tekintetében az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló 2017. évi LII. törvény 17. § (3) bekezdésében kapott felhatalmazás alapján,
a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 4. § (9) bekezdésében meghatározott feladatkörömben eljárva a következőket rendelem el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. § (1) E rendelet hatálya – a (2) bekezdésben meghatározott kivétellel – a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (a továbbiakban: Pmt.) 1. § (1) bekezdés a)–e) és m) pontja, valamint (1a) bekezdése szerinti szolgáltatóra (a továbbiakban együtt: szolgáltató) terjed ki.

(2) E rendelet 8. alcíme nem terjed ki a kizárólag a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény szerinti számlainformációs szolgáltatást nyújtó szolgáltatóra.

2. § E rendelet alkalmazásában

1. *áru:* a fogyasztóvédelemről szóló 1997. évi CLV. törvény 2. § 2. pontjában meghatározott fogalom,
2. *csatorna:* elektronikus technikai eszköz – különösen mobiltelefon, számítógép, táblagép – vagy közvetítő, amelynek igénybevételével az ügyintézés nem abban a helyiségben történik, ahol a szolgáltató a tevékenységét állandó jelleggel folytatja,
3. *készpénzes ügylet:* az ügyfél részére történő készpénzkifizetés és az ügyfél általi készpénzbefizetés pénznemtől függetlenül,
4. *kockázati profil:* a beazonosított pénzmosási és terrorizmusfinanszírozási kockázatok csökkentését követően megmaradó kockázat általános jellege, beleértve a kockázat típusát és szintjét is,
5. *küszöbérték:* az üzleti kapcsolat során teljesített ügyletek révén elérhető olyan kumulált összeghatár, amelyet a szolgáltató kockázatérzékenységi alapon határoz meg,
6. *megerősített eljárás:* az ügyfélben, az áruban, az ügyletben, az alkalmazott eszközben vagy a földrajzi kitettségben rejlő kockázat kezelésére szolgáló kockázatalapú intézkedések együttesét magába foglaló fokozott monitoring,
7. *monitoring:* az üzleti kapcsolat és az ügyleti megbízásokat rendszeresen adó ügyfél folyamatos figyelemmel kísérése,
8. *pénzmosási és terrorizmusfinanszírozási kockázat:* a pénzmosás vagy a terrorizmusfinanszírozás felmerülésének valószínűsége és hatása,
9. *szokatlan ügylet:* olyan ügylet,
   a) amely nincs összhangban az áruval kapcsolatban általánosan követett eljárásokkal,
   b) amelynek nincs világosan érthető gazdasági célja vagy jogi alapja, vagy
   c) amely esetében az ügyfél korábbi tevékenységéhez képest indokolatlanul megváltozik az ügyletek gyakorisága, illetve nagysága,
10. *vezető testület:* valamely szolgáltató irányítási funkciót betöltő testülete, illetve a felvigyázási funkciót betöltő testülete.

II. FEJEZET
AZ ÜGYFÉL-ÁTVILÁGÍTÁSRA ÉS A TÉNYLEGES TULAJDONOS SZEMÉLYAZONOSSÁGÁNAK ELLENŐRZÉSÉRE VONATKOZÓ EGYES SZABÁLYOK

1. A tényleges tulajdonos kilétének, valamint az ügyfél tulajdonosi és irányítási szerkezetének megértése és megállapítása érdekében megteendő intézkedések

3. § A szolgáltató a Pmt. 8. § (4) bekezdésében és 9. § (3) bekezdésében előírt kötelezettség végrehajtása érdekében az ügyfél tulajdonosi és irányítási szerkezetének megértése céljából olyan észszerű intézkedéseket végez, amelyek elegendők ahhoz, hogy a szolgáltató meggyőződhessen arról, hogy átlátja és megérti az ügyfél vonatkozásában a tulajdonlás, irányítás és az ellenőrzés különböző szintjeihez kapcsolódó kockázatot, és meg tudja határozni a tényleges tulajdonosok kilétét.

4. § (1) A tényleges tulajdonos meghatározása érdekében a szolgáltató a Pmt. 3. § 38. pontjában foglaltaknak megfelelően – figyelembe véve a Magyar Nemzeti Bank (a továbbiakban: MNB) által nyilvánosságra hozott információkat is – megvizsgálja, hogy vannak-e olyan személyek, akik a jogi személynek vagy jogi személyiséggel nem rendelkező szervezetnek minősülő ügyfél tekintetében egyéb módon tényleges irányítást, ellenőrzést gyakorolnak. A szolgáltató ennek érdekében figyelembe veszi különösen:

a) az ügyfelet érintő, közvetlen tulajdonlás nélküli irányítást hozzátartozói viszony vagy szerződéses kapcsolatok révén,
b) az ügyfél tulajdonában lévő eszközök igénybevételét, használatát vagy azokból való haszonszerzést, továbbá
c) az ügyfél üzleti gyakorlatait vagy működését befolyásoló stratégiai döntésekért való felelősséget.

(2) A szolgáltató a tényleges tulajdonos kilétének megállapítása érdekében alkalmazott módszert belső szabályzatában rögzíti.

(3) A szolgáltató az ügyfél tulajdonosi és irányítási szerkezetének megállapítását akkor alapozhatja kizárólag az ügyfél nyilatkozatára, ha az ügyfél alacsony kockázatú, és a nyilatkozat valóságtartalmával összefüggésben az összes körülmény figyelembevételével a szolgáltatóban nem merül fel kétség. A szolgáltató minden más esetben kockázatérzékenységi megközelítés alapján a felmerült kockázati szinthez mérten arányos intézkedéseket alkalmaz az ügyfél tulajdonosi és irányítási szerkezetének feltárása érdekében.

5. § A szolgáltató a jogi személy ügyfél vonatkozásában kockázatérzékenységi alapon ellenőrzi a létesítési joghatósága szerinti tényleges tulajdonosi nyilvántartást, amennyiben a nyilvántartásban szereplő adatok a szolgáltató számára hozzáférhetőek. A jogi személy ügyfél vonatkozásában a tényleges tulajdonosok nyilvántartásában szereplő adatok kockázatérzékenységi alapon történő értékelésén túl a szolgáltató további adatokat szerez be, ha az üzleti kapcsolathoz magasabb kockázat társul, vagy ha a szolgáltatónak kétségei vannak afelől, hogy a nyilvántartásban szereplő személy a tényleges tulajdonos.

6. § (1) A szolgáltató az ügyfél által megnevezett vezető tisztségviselőt kizárólag abban az esetben rögzítheti az ügyfél tényleges tulajdonosaként, ha minden lehetséges eszközt kimerített azon természetes személy azonosítása céljából, aki az ügyfél tekintetében a Pmt. 3. § 38. pont a) vagy b) alpontja szerinti tulajdoni hányaddal, szavazati joggal vagy meghatározó befolyással rendelkezik, vagy aki egyéb módon tényleges irányítást, ellenőrzést gyakorol felette.

(2) A szolgáltató az (1) bekezdésben foglalt esetben a nyilvántartásában visszakereshető módon rögzíti annak okát, hogy az ügyfél tényleges tulajdonosaként miért az ügyfél által megnevezett vezető tisztségviselőt rögzítette.

7. § Ha kétség merül fel a tényleges tulajdonos kilétével kapcsolatban, a szolgáltató az ügyfél által megnevezett tényleges tulajdonos vonatkozásában a következő intézkedéseket alkalmazza:

a) a tényleges tulajdonos személyazonosságának igazoló ellenőrzése és

b) az üzleti kapcsolat céljának és jellegének, valamint a tényleges tulajdonos valós gazdasági kapcsolódásának ellenőrzése érdekében visszakereshető módon dokumentált és a Pmt. 56–58. §-ában foglaltaknak megfelelően megőrzendő ügyfélismereti beszélgetés lefolytatása

ba) az ügyféllel,

bb) – amennyiben a tényleges tulajdonos ebben együttműködik – kockázatérzékenységi alapon a tényleges tulajdonossal is.

8. § Ha a szolgáltató az ügyfél-átvilágítás keretében elvégzett intézkedések eredményeképpen nem tudja megismerni az ügyfél tulajdonosi és irányítási szerkezetét, és ekképpen a tényleges tulajdonos kilétét sem, az érintett ügyfélre vonatkozóan a Pmt. 13. § (8) bekezdésében foglaltak szerint jár el.

9. § A szolgáltató az ügyfél vonatkozásában felmerült kockázatokat és az azokra tekintettel elvégzett intézkedések eredményét visszakereshető módon dokumentálja és a Pmt. 56–58. §-ában foglaltaknak megfelelően megőrzi. Ennek érdekében a szolgáltató olyan nyilvántartást vezet, amelyből kétséget kizáróan megállapítható, hogy milyen forrásból származnak az ügyfélre vonatkozó adatok, és hogy a szolgáltató ezeket milyen módon ellenőrizte.

2. Az egyszerűsített ügyfél-átvilágítás és a fokozott ügyfél-átvilágítás esetkörei

10. § A szolgáltató egyszerűsített ügyfél-átvilágítást alkalmazhat, ha ügyfele a Pmt. 6/A. §-a szerinti besorolás alapján alacsony kockázatú.

11. § (1) A szolgáltató a Pmt.-ben meghatározottakon kívül fokozott ügyfél-átvilágítást alkalmaz, ha ügyfele

a) a szolgáltató belső kockázatértékelésében meghatározott kritériumoknak megfelelő nonprofit szervezet,

b) olyan jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amelynek tényleges tulajdonosa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országból származik,

c) olyan részvénytársaság, amelynek bemutatóra szóló részvénye van, vagy amelynek részvényesét részvényesi meghatalmazott képviseli, vagy

d) olyan jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amelynek tulajdonosi szerkezete a jogi személy vagy jogi személyiséggel nem rendelkező szervezet üzleti tevékenységének jellegéhez képest szokatlannak vagy túlzottan összetettnek tűnik.

(2) Az (1) bekezdés d) pontjában foglaltak nem alkalmazandók, ha a szolgáltató megítélése szerint a jogi személy vagy jogi személyiséggel nem rendelkező szervezet túlzottan összetett tulajdonosi szerkezete megindokolható, és azt a szolgáltató belső kockázatértékelésében részletesen, a kockázatcsökkentő és -növelő tényezők együttes értékelésével alátámasztja, vagy az ügyfél a Pmt. 6/A. §-a szerinti besorolás alapján alacsony kockázatú.

III. FEJEZET
AZ ÜGYFÉL EGYEDI KOCKÁZATBESOROLÁSA ALAPJÁN ELVÉGZENDŐ SZOLGÁLTATÓI INTÉZKEDÉSEK

3. A szolgáltató által az üzleti kapcsolat jellegének és céljának megállapítása érdekében megteendő intézkedések

12. § (1) A Pmt. 1. § (1) bekezdés a) pontja szerinti szolgáltató a Pmt. 6. § (1) bekezdés a) pontjában meghatározott esetben az ügyféllel az üzleti kapcsolat céljának és jellegének megértése, az ügyfél megfelelő kockázati szintbe történő besorolása, valamint a későbbi monitoringtevékenység támogatása érdekében ügyfélismereti kérdőívet töltet ki. Az ügyfélismereti kérdőív az üzleti kapcsolat céljáról és tervezett jellegéről legalább a következőket tartalmazza:

a) a jövedelemszerző tevékenységének jellegét,
b) a szerződéskötést követő 365 napban végrehajtani tervezett ügyletek maximális értékét,
c) a tervezett átlagos havi számlaforgalom összegét,
d) külföldi ügyletek tervezett végrehajtását, ennek keretében az ügyfélnek külön szükséges nyilatkoznia arról, hogy az Európai Unión kívüli ügyleteket tervez-e, amennyiben igen, úgy várhatóan mely országok irányába, milyen nagyságrendben és milyen gyakorisággal,
e) a havi és éves szintű készpénzes ügyletek várható nagyságát pénznemtől függetlenül,
f) a harmincmillió forintot meghaladó ügyletek várható előfordulását és tervezett gyakoriságát,
g) annak ismertetését, hogy az ügyfél tervezi-e csatornák igénybevételét – ennek keretében az ügyfélnek külön szükséges nyilatkoznia az így végrehajtani tervezett ügyleteinek maximális napi kumulált értékéről –, továbbá
h) az igénybe venni tervezett hitel vagy kölcsön összegét, továbbá hogy ezek igénybevétele során az ügyfél tervezi-e csatorna igénybevételét.

(2) A jogi személynek, valamint jogi személyiséggel nem rendelkező szervezetnek minősülő ügyfél esetében az ügyfélismereti kérdőív az (1) bekezdésben foglaltakon túlmenően az ügyfél vonatkozásában tartalmazza

a) leggyakoribb üzleti partnereit,
b) üzletszerű vagy nem üzletszerű bizalmi vagyonkezelői minőségét,
c) a tervezett átlagos havi számlaforgalom összegéhez viszonyított készpénzes ügyletek arányát,
d) az ügyfél nevében várhatóan készpénzbefizetést teljesítő személy ügyfélhez való viszonyát,
e) annak ismertetését, hogy milyen indok alapján döntött az ügyfél a szolgáltató, annak árui igénybevételéről, valamint
f) külföldi székhelyű ügyfél esetén
   fa) a Magyarországon folytatott adóköteles gazdasági tevékenységét,
   fb) a magyarországi számlanyitás indokát, azzal, hogy amennyiben a szolgáltató álláspontja szerint az ügyfél általi számlanyitás más országban racionálisabb lenne, az ügyfél nyilatkozatának arra is ki kell terjednie, hogy miért Magyarországon és miért a szolgáltatóval kíván üzleti kapcsolatot létesíteni,
   fc) a leggyakoribb magyar üzleti partnereit,
   fd) az alkalmazottai számát és
   fe) az utolsó lezárt üzleti év szerinti árbevételét.

(3) A szolgáltató az ügyfelet az (1) bekezdés c)–h) pontjában, valamint a (2) bekezdés c) pontjában foglaltakról a szolgáltató által kockázati alapon, sávosan meghatározott érték megjelölésével nyilatkoztatja.

(4) A szolgáltató az ügyfélismereti kérdőíven az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 16. §-a szerint tájékoztatást nyújt az adatkezelésről az ügyfél részére.

13. § (1) Amennyiben a Pmt. 1. § (1) bekezdés a) pontja szerinti szolgáltató rendelkezésére álló ügyfélismereti adatok az ügyfél kockázati besorolásának megállapításához vagy az ügyfél esetében szükséges kockázatkezelési intézkedések meghatározásához nem elégségesek, a szolgáltató az ügyfelet az üzleti kapcsolat célja és tervezett jellege vonatkozásában a 12. §-ban foglaltakról, továbbá az alábbiakról is nyilatkoztatja:

a) a szolgáltató árui felhasználásának tervezett módja,

b) annak alátámasztása, hogy az ügyfél által végrehajtott ügyletek gazdasági szempontból racionálisak-e,

c) olyan ágazatokkal való kapcsolata, amelyekhez magasabb pénzmosási vagy terrorizmusfinanszírozási kockázat kapcsolódik, különösen amelyekre

ca) magasabb korrupciós kockázat vagy

cb) nagy mennyiségű készpénzhasználat

jellemző,

d) a szolgáltatónál igénybe vett szolgáltatások más szolgáltatónál történő párhuzamos igénybevétele, a versenytárs megjelölése nélkül, továbbá

e) a belföldi vagy külföldi politikai kapcsolatai, így különösen kiemelt közszereplővel vagy olyan jogi személlyel vagy jogi személyiséggel nem rendelkező szervezettel fennálló vagy az elmúlt egy naptári évben fennállt kapcsolatai, amelynek tényleges tulajdonosa kiemelt közszereplő, valamint az ügyfélnek vagy tényleges tulajdonosának kiemelt közszereplővel fennálló vagy az elmúlt egy naptári évben fennállt más releváns kapcsolata.

(2) A természetes személynek minősülő ügyfelet az ügyfélismereti kérdőívben – ha az (1) bekezdésben meghatározott kockázatkezelési intézkedésekhez szükséges – az (1) bekezdésben foglaltakon túlmenően a szolgáltató az alábbiakról is nyilatkoztatja:

a) milyen indok alapján döntött a szolgáltató, valamint annak árui igénybevételéről,

b) az esetleges nem üzletszerű bizalmi vagyonkezelői minőségéről, továbbá

c) az általa tervezett ügyletekben eseti jellegű meghatalmazottak igénybevételéről.

(3) A jogi személynek, valamint jogi személyiséggel nem rendelkező szervezetnek minősülő ügyfelet az ügyfélismereti kérdőívben – ha az (1) bekezdésben meghatározott kockázatkezelési intézkedésekhez szükséges – az (1) bekezdésben foglaltakon túlmenően a szolgáltató az alábbiakról is nyilatkoztatja:

a) annak alátámasztása, hogy az ügyfél által forgalmazott áru árképzése kereskedelmi szempontból racionális-e, és

b) valamely cégcsoporthoz tartozás esetén a cégcsoport és a tagok gazdasági tevékenységének, valamint földrajzi elhelyezkedésének bemutatása.

14. § (1) Ha a szolgáltatónak az üzleti kapcsolat – a Pmt. 11. § (1) bekezdésében meghatározott – folyamatos figyelemmel kísérése során a 12. és 13. § szerint rögzített adatokhoz, információkhoz, tényekhez képest ellentétes adat, információ jut a tudomására, az ellentmondások tisztázása érdekében felveszi a kapcsolatot az ügyféllel. A szolgáltató az ügyféllel történő kapcsolatfelvételt követően kockázatérzékenységi alapon, de legfeljebb hatvan munkanapon belül tisztázza az ellentmondás okát. Amennyiben ez nem vezet eredményre, a szolgáltató ismételten elvégzi a Pmt. 7–10. §-ában meghatározott, az ellentmondás feloldásához szükséges ügyfél-átvilágítási intézkedéseket, amelynek tartama alatt a Pmt. 13. § (8) bekezdésében foglaltakat alkalmazza.

(2) A szolgáltató mellőzheti az ügyfélismereti kérdőív azon pontjainak kitöltését, amelyek a szolgáltató jellegéből, tevékenységéből adódó okból nem értelmezhetőek, vagy amelyek vonatkozásában az információ más hiteles forrásból már a rendelkezésére áll. Ilyen esetben a szolgáltató az adott kérdés ügyfél általi kitöltésének mellőzését alátámasztó okot visszakereshető módon rögzíti.

4. A kockázatérzékenységi megközelítés alapján üzleti kapcsolat létesítéséhez vagy ügyleti megbízás teljesítéséhez a kijelölt felelős vezető döntését igénylő esetek és e döntések meghozatalának részletes szabályai

15. § (1) A Pmt.-ben meghatározottakon felül a szolgáltató kijelölt felelős vezetője dönt legalább az alábbi esetekben:

a) az üzleti kapcsolat létesítéséről, ha arra utaló adat, tény, illetve körülmény merül fel, hogy a szolgáltatást ténylegesen nem az a személy veszi igénybe, aki a szerződéskötési kérelemben ügyfélként feltüntetésre került,

b) privátbanki üzleti kapcsolat létesítéséről,

c) a szolgáltató által nyújtott árura vonatkozó vagy új üzleti gyakorlattal, többek között új teljesítési megoldással, valamint új vagy fejlődő technológiák alkalmazásának bevezetésével kapcsolatban,

d) az üzleti kapcsolat létesítéséről az ügyfélismereti kérdőív kiértékeléséből származó jelentős pénzmosási és terrorizmusfinanszírozási kockázat esetén, különösen, ha a kérdőíven évi százmillió forintot elérő vagy meghaladó készpénzforgalom lebonyolítását jelzi az ügyfél,

e) bizalmi vagyonkezelővel vagy ahhoz hasonló tevékenységet végző ügyféllel történő üzleti kapcsolat létesítéséről, valamint

f) üzleti kapcsolat létesítéséről, amennyiben az ügyfél székhelyéül székhelyszolgáltató címét jelöli meg.

(2) A szolgáltató kijelölt felelős vezetője az (1) bekezdésben meghatározott esetekben olyan dokumentált formában dönt, amely biztosítja a következetességet, a folyamatos figyelemmel kísérhetőséget és az ellenőrizhetőséget is.

16. § (1) A szolgáltató kockázatérzékenységi megközelítés alapján a Pmt. 65. §-a szerinti szabályzatában rendelkezhet a Pmt. 10. § (3) bekezdésében, 14/A. § (4) bekezdésében, 16. § (2) bekezdés a) pontjában és 16/A. § (1) bekezdés b) pontjában, valamint e rendelet 15. §-ában foglalt, az üzleti kapcsolat létesítéséhez vagy ügyleti megbízás teljesítéséhez a kijelölt felelős vezető döntését igénylő esetek teljes körű vagy részleges, állandó vagy a kijelölt felelős vezető eseti helyettesítését biztosító delegálásának szabályairól.

(2) A szolgáltató a Pmt. 65. §-a szerinti szabályzatában az (1) bekezdés szerinti döntési jogköröket kizárólag olyan vezetőre delegálhatja, aki rendelkezik a döntéshez szükséges szakmai ismeretekkel. A delegálásra vonatkozó szabályok kialakítása során a szolgáltató meghatározza az egyes döntési jogkörök delegálásnak mérlegelése során figyelembe veendő szempontokat is.

5. A megerősített eljárás esetkörei és feltételrendszere

17. § (1) A szolgáltató a Pmt.-ben meghatározottakon túl legalább a következő esetekben alkalmaz megerősített eljárást:

a) a takarékbetétről szóló törvényerejű rendelet szerinti nem névre szóló takarékbetét névre szólóvá alakításával érintett ügyfél tekintetében, ha a névre szólóvá alakítani kívánt takarékbetétek összértéke eléri a négymillió-ötszázezer forintot, az átalakítástól számított egy évig,

b) ha az ügyfelet a szolgáltató tízmillió forintot elérő vagy meghaladó pénzváltás miatt világítja át, a tízmillió forintot elérő vagy meghaladó utolsó pénzváltástól számított egy évig,

c) ha az ügyleti megbízásokat rendszeresen adó ügyfelet a szolgáltató ötvenmillió forintot elérő vagy meghaladó összegű ügyleti megbízás miatt világítja át, az ötvenmillió forintot elérő vagy meghaladó utolsó ügylettől számított egy évig,

d) ha az ügyfél készpénzforgalma – azaz befizetéseinek és pénzfelvételeinek összege – a havi százmillió forintot eléri vagy meghaladja, az utolsó százmillió forintot elérő vagy meghaladó készpénzforgalmú hónapot követően számított egy évig,

e) ha a szolgáltató ügyfelével kapcsolatban a szolgáltató által vagy a csoporton belül, amelyhez a szolgáltató tartozik, a Pmt. 30. § (1) bekezdése szerinti bejelentés történt, az utolsó bejelentéstől számított egy évig, valamint

f) nem magyar állampolgárságú és kilencven napot meghaladó magyarországi tartózkodásra jogosító engedéllyel vagy tartózkodási regisztrációval, lakóhellyel vagy tartózkodási hellyel nem rendelkező, az Európai Unió területén kívüli lakóhellyel vagy tartózkodási hellyel rendelkező természetes személynél.

(2) A szolgáltató a megerősített eljárásnak az (1) bekezdésben meghatározottakon kívüli egyéb eseteit a belső kockázatértékelésében rögzíti.

(3) A szolgáltató az általa meghatározott ügyfelek egy csoportja tekintetében mellőzheti a megerősített eljárást, ha az (1) bekezdés szerinti esetekre vonatkozóan belső kockázatértékelésében azt részletesen, a kockázatcsökkentő és -növelő tényezők együttes értékelésével alátámasztja.

18. § (1) A szolgáltató a megerősített eljárás alá tartozó ügyfeleknél a 28–31. § rendelkezéseinek megfelelően szűri és pénzmosás és terrorizmusfinanszírozás szempontjából elemzi és értékeli a belső kockázatértékelésben meghatározott ügyleteket.

(2) Az (1) bekezdésben meghatározott kockázatértékelés során a szolgáltató ügyletenkénti értékhatárt alkalmaz.

(3) A belső kockázatértékelésben meghatározott értékhatárt a szolgáltató a kockázatcsökkentő és -növelő tényezők együttes értékelésével, kockázatalapon, ügyletenként határozza meg.

(4) Ha a megerősített eljárás alá tartozó ügyfelek tízmillió forintot elérő vagy meghaladó összegű készpénzbefizetést vagy pénzváltást teljesítenek, a szolgáltató beszerzi a pénzeszköz forrására vonatkozó információt, valamint ezen információk igazoló ellenőrzése érdekében a pénzeszközök forrására vonatkozó dokumentumok bemutatását is megköveteli.

IV. FEJEZET
A PÉNZMOSÁS ÉS A TERRORIZMUS FINANSZÍROZÁSA MEGELŐZÉSÉRE, MEGAKADÁLYOZÁSÁRA, VALAMINT AZ EURÓPAI UNIÓ ÉS AZ EGYESÜLT NEMZETEK SZERVEZETÉNEK BIZTONSÁGI TANÁCSA ÁLTAL ELRENDELT PÉNZÜGYI ÉS VAGYONI KORLÁTOZÓ INTÉZKEDÉSEK VÉGREHAJTÁSÁRA VONATKOZÓ EGYES SZABÁLYOK

6. A belső kockázatértékelés elkészítésének szabályrendszere

19. § (1) A belső kockázatértékelés alkalmazása során a szolgáltató beazonosítja a már ismert kockázatai közül azokat, amelyek hatással vannak a pénzmosási és terrorizmusfinanszírozási kockázataira.

(2) A szolgáltató az (1) bekezdésben meghatározott beazonosítás során figyelembe veszi a már rendelkezésre álló kockázati profilt.

20. § (1) A szolgáltató a kockázati tényezők beazonosítása során a Pmt.-ben meghatározottakon túl az alábbiakat veszi figyelembe:

a) az Európai Bizottság nemzetek feletti kockázatértékelését,

b) az európai felügyeleti hatóságok véleményét a pénzügyi ágazatot érintő európai uniós pénzmosási és terrorizmusfinanszírozási kockázatokról,

c) az MNB által kiadott ajánlást,

d) az MNB által nyilvánosságra hozott információkat és

e) az MNB által folytatott eljárás során keletkezett és nyilvánosságra hozott határozatokat.

(2) A szolgáltató a kockázati tényezők beazonosítása során különösen

a) a civil társadalomtól,

b) a 21. § (1) bekezdése szerinti állam pénzmosás és a terrorizmus finanszírozása elleni rendszere megfelelőségével és hatékonyságával, korrupcióellenes és adózási rendszerével kapcsolatos értékeléséből,

c) nyilvános forrásból és

d) tudományos intézményektől

származó információkat vehet figyelembe.

21. § (1) Ha a szolgáltató ki van téve az Európai Unió egy másik tagállama vagy harmadik ország pénzmosási és terrorizmusfinanszírozási kockázatainak, a szolgáltató ezeket a kockázatokat is beazonosítja.

(2) A szolgáltató az (1) bekezdés szerinti kockázatokat különösen abban az esetben azonosítja be, ha a szolgáltató

a) az Európai Unió egy másik tagállamában vagy harmadik országban létrehozott pénzügyi csoport tagja,

b) tulajdonosa az Európai Unió egy másik tagállamában vagy harmadik országban bejegyzett szolgáltatónak,

c) tényleges tulajdonosa az Európai Unió egy másik tagállamából vagy harmadik országból származik, vagy

d) olyan kapcsolatot tart fenn az Európai Unió egy másik tagállamában vagy harmadik országban lévő szervvel vagy szervezettel, amely arra utal, hogy a szolgáltató ki van téve az adott ország pénzmosási és terrorizmusfinanszírozási kockázatainak.

(3) A szolgáltató beszerzi az (1) bekezdés szerinti tagállamhoz vagy harmadik országhoz köthető pénzmosási és terrorizmusfinanszírozási kockázatokkal kapcsolatos azon információkat, amelyek hatással lehetnek az általa végzett tevékenységre.

(4) A szolgáltató a tudomásszerzéstől számított három munkanapon belül bejelentést tesz az MNB-hez, ha az (1) bekezdés szerinti kockázatok beazonosítását és a (3) bekezdés szerinti információk beszerzését követően olyan hiányosság jut a tudomására, amely veszélyt jelent az Európai Unió pénzügyi rendszerére.

22. § A szolgáltató az alábbi szempontokat veszi figyelembe belső kockázatértékelésének elkészítésekor:

a) tulajdonosi és vállalati szerkezete, figyelemmel arra, hogy a szolgáltató nemzetközi, külföldi vagy belföldi intézmény, anyavállalat, leányvállalat, fióktelep vagy egyéb szervezet,

b) szervezetének és szerkezetének összetettsége és átláthatósága,

c) a kínált áru, az elvégzett tevékenység és ügylet természete és összetettsége,
d) az alkalmazott eszköz, beleértve az ingyenes szolgáltatásnyújtást, az ügynök vagy a közvetítő használatát,
e) a kiszolgált ügyfelek típusai,
f) az üzleti tevékenység földrajzi területe, különösen, ha azt stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban végzi, vagy az ügyfelei jelentős részének származási országa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik ország,
g) a belső irányítási megoldás és szerkezet minősége, beleértve a belső ellenőrzési és megfelelési funkció hatékonyságát, a pénzmosás és a terrorizmusfinanszírozás megelőzésével és megakadályozásával összefüggő jogi követelménynek való megfelelést és a megelőző belső kockázatértékeléseinek hatékonyságát, és
h) az uralkodó vállalati kultúra, különösen a megfelelési és átláthatósági kultúra.

23. § (1) A 20–22. § szerinti tényezők együttesen képezik a szolgáltató kockázatértékelésének alapját.
(2) A szolgáltató értékeli a 20–22. § szerinti tényezők szolgáltatóra gyakorolt hatását és a szolgáltatónál működő kockázatalapú ellenőrzési rendszer és folyamat megfelelőségét a pénzmosási és terrorizmusfinanszírozási kockázat enyhítése érdekében.
(3) A szolgáltató a kockázati tényező relatív jelentősége alapján eltérően súlyozhatja a kockázatot és az azt mérséklő tényezőket.
(4) A szolgáltató a kockázatokat legalább alacsony, átlagos és magas kockázati kategóriába sorolja.
(5) A szolgáltató a kockázatokat legalább ügyfél, áru, alkalmazott eszköz, földrajzi kockázati csoportokba sorolja.

24. § (1) A szolgáltató a Pmt. 65. § (1) bekezdése szerinti belső szabályzatában a beazonosított kockázat értékelése alapján meghatározza, hogy milyen intézkedésre van szükség a feltárt kockázat kezelése érdekében.
(2) A szolgáltató vezető tisztségviselője vagy irányítási funkciót betöltő testülete a belső kockázatértékelésről szóló jelentést jóváhagyja.

25. § (1) A szolgáltató a belső kockázatértékelését az alapjául szolgáló információ időszakos és eseti felülvizsgálatával aktualizálja.
(2) A szolgáltató az (1) bekezdés alapján elvégzett felülvizsgálatot úgy ütemezi, hogy az arányban álljon a szolgáltatóhoz kapcsolódó pénzmosási és terrorizmusfinanszírozási kockázattal.
(3) A szolgáltató a belső kockázatértékelését soron kívül felülvizsgálja, ha
a) külső hatás megváltoztatja a kockázat természetét,
b) új típusú pénzmosási és terrorizmusfinanszírozási kockázat merül fel,
c) az MNB hatósági döntése ilyen intézkedést tartalmaz,
d) a szolgáltató saját maga által tett, kockázatot csökkentő intézkedéséből ez következik,
e) a szolgáltató tulajdonosaival, a vezető testület tagjaival, a fő funkciókat ellátó személyekkel vagy a szervezetével kapcsolatban új információk merülnek fel, továbbá
f) minden egyéb esetben, amikor a szolgáltatónak alapos oka van azt feltételezni, hogy a kockázatértékelés alapjául szolgáló információ már nem vagy nem teljesen helytálló.

7. Az ügylet felfüggesztése

26. § (1) A szolgáltató meghatározza az ügyfélnek adandó tájékoztatást, valamint belső szabályzatában rögzíti szervezeti egységeinek kötelezettségét és felelősségét az ügylet felfüggesztése során.
(2) Az (1) bekezdés szerinti tájékoztatás nem utalhat az ügylet felfüggesztésének tényére és a felfüggesztés indokára.
(3) A szolgáltató biztosítja, hogy
a) a felfüggesztés tényéről a szolgáltató tudomással bíró, Pmt. 31. § (1) bekezdésében meghatározott vezetője és foglalkoztatottja az (1) bekezdés szerinti tájékoztatás szerint járjon el,
b) a felfüggesztés teljesítéséhez csak a szükséges szervezeti egységet vonja be,
c) a felfüggesztési kötelezettség teljesítésére utaló adat, tény, illetve körülmény felmerülésekor telefonon értesíthesse a pénzügyi információs egységként működő hatóságot, és ebben az esetben a tőle kapott instrukciók szerint járjon el, valamint
d) a felfüggesztés ideje alatt a telefonos kapcsolattartás a pénzügyi információs egységként működő hatósággal a kijelölt személy akadályoztatása esetén is folyamatos legyen.

(4) A szolgáltató az általa vezetett nyilvántartáson belül az ügylet felfüggesztését igazoló iratot vagy annak másolatát elkülönítetten kezeli.

8. A belső ellenőrző és információs rendszer működtetése

27. § Ezen alcím alkalmazásában

1. *automatikus szűrőrendszer:* az ügyfél és az ügylet pénzmosás és terrorizmusfinanszírozás szempontjából előzetes paraméterezés alapján történő, emberi beavatkozást nem igénylő leválogatására alkalmas informatikai rendszer;
2. *manuális szűrés:* az ügyfél és az ügylet pénzmosás és terrorizmusfinanszírozás szempontjából történő, emberi beavatkozást igénylő leválogatása.

28. § (1) A szolgáltató a belső ellenőrző és információs rendszer részeként olyan, a bejelentés teljesítését támogató szűrőrendszerrel rendelkezik, amely biztosítja a pénzmosás és a terrorizmusfinanszírozás szempontjából kockázatos ügyfél és szokatlan ügylet kiszűrését és a bejelentés megtételéhez szükséges adatok rendelkezésre bocsátását (a továbbiakban: szűrőrendszer).

(2) A szolgáltató – a (3) bekezdésben foglalt kivétellel – manuális szűréseken alapuló szűrőrendszert alkalmazhat.

(3) A szolgáltató automatikus szűrőrendszert működtet, ha

a) pénzforgalmi szolgáltatási tevékenységet végez, vagy

b) ügyfeleinek száma a tárgyévet megelőző év végén meghaladta az ötvenezret.

29. § (1) A szolgáltató a szűrőrendszer működéséről, a kiszűrt ügyfél, valamint az ügylet elemzésének és értékelésének menetéről belső eljárásrendet készít.

(2) Az (1) bekezdés szerinti belső eljárásrendet a szolgáltató írásban rögzíti, naprakészen tartja, és az illetékes felügyeleti hatóságok rendelkezésére bocsátja.

(3) A szűrőrendszer belső eljárásrendjének legalább az alábbi feltételeknek kell megfelelnie:

a) a szolgáltató belső kockázatértékelésén alapul,

b) megfelel a szolgáltató kapcsolódó belső szabályzatainak,

c) dokumentálja a szolgáltató által használt szcenáriókat, az azok alapjául szolgáló logikákkal, paraméterekkel és küszöbértékekkel, és biztosítja a változások nyomon követhetőségét,

d) biztosítja az adatok integritását és minőségét annak érdekében, hogy a szűrőrendszeren pontos és teljes adatok menjenek keresztül,

e) rögzíti a releváns adatokat tartalmazó összes adatforrást,

f) biztosítja a szűrőrendszer megtervezéséért, működtetéséért, teszteléséért, beüzemeléséért és folyamatos felügyeletéért, valamint az esetkezelésért, felülvizsgálatért és a találatok és lehetséges bejelentések tekintetében hozott döntésekért felelős szakképzett alkalmazottak vagy külső tanácsadók rendelkezésre állását,

g) rögzíti az elemző- és értékelőfolyamat során alkalmazott határidőket,

h) olyan vizsgálati protokollokat tartalmaz, amelyek részletesen bemutatják, hogy a szűrőrendszer által generált figyelmeztetéseket milyen módon kell megvizsgálni, milyen módon kell dönteni afelől, hogy mely találatok kerüljenek bejelentésre, ki a felelős az ilyen döntés meghozataláért, valamint azt, hogy milyen módon kell a döntéshozatali eljárást dokumentálni,

i) biztosítja a szcenáriók és az azok alapjául szolgáló logikák, paraméterek és küszöbértékek kockázataival összhangban történő felülvizsgálatát, illetve tartalmazza, hogy ki a felelős a felülvizsgálatért, valamint

j) automatikus szűrőrendszer esetén előírja a szűrőrendszer teljes folyamatát nyomon követő, valamint a bevezetését megelőző és azt követő tesztelését, csakúgy, mint az időszakos tesztelések elvégzését az irányítás, az adatok leképezése, az ügyletek azonosítása, a keresési szcenáriók és logikák, a szűrési modellezés, valamint a bevitt adatok és az eredmények vizsgálatával kapcsolatosan.

30. § (1) A szolgáltató legalább a következő ügyfél-, illetve ügylettípusokra végzett szűréseket hajtja végre, és azt biztosítja a belső kockázatértékelésében:

a) huszonötmillió forintot elérő vagy meghaladó összegű készpénzbefizetés természetes személy ügyfél részére,

b) ötvenmillió forintot elérő vagy meghaladó összegű készpénzbefizetés jogi személy és jogi személyiséggel nem rendelkező ügyfél részére,
c) huszonötmillió forintot elérő vagy meghaladó összegű készpénzkifizetés természetes személy ügyfél részére,
d) ötvenmillió forintot elérő vagy meghaladó összegű készpénzkifizetés jogi személy és jogi személyiséggel nem rendelkező ügyfél részére,
e) stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országból kezdeményezett vagy oda továbbított, huszonötmillió forintot elérő vagy meghaladó összegű ügylet,
f) huszonötmillió forintot elérő vagy meghaladó összegű pénzátutalás adószámmal nem rendelkező jogi személy és jogi személyiséggel nem rendelkező ügyfél részére, vagy általa kezdeményezve, valamint
g) ötvenmillió forintot elérő vagy meghaladó összegű pénzátutalás nem magyar adószámmal rendelkező jogi személy és jogi személyiséggel nem rendelkező ügyfél részére, vagy általa kezdeményezve.

(2) A szolgáltató a szűrési feltételeit az (1) bekezdésben meghatározottakon túl a belső kockázatértékelése alapján határozza meg.

(3) A szolgáltató belső kockázatértékelése alapján az (1) bekezdésben szereplő kötelező szűrési feltételeket más szűrésekkel is helyettesítheti, ha az MNB részére bizonyítani tudja, hogy bevezetett szűrései teljeskörűen alkalmasak az (1) bekezdésben szereplő szűrések mögötti kockázatok kezelésére.

31. § (1) A szolgáltató a szűrést folyamatosan végzi. A szűrés folyamatosságát huszonnégy órát meghaladóan akadályozó körülmény szolgáltató tudomására jutásáról és az ennek kiküszöbölésére foganatosított, illetve foganatosítani tervezett intézkedésekről a szolgáltató haladéktalanul, elektronikus formában, az MNB Elektronikus Rendszer Hitelesített Adatok Fogadásához megnevezésű rendszerén (a továbbiakban: ERA rendszer) keresztül tájékoztatja az MNB-t.

(2) A kiszűrt ügyfél, illetve ügylet pénzmosás és terrorizmusfinanszírozás szempontjából történő elemzését és értékelését a szolgáltató a 18. § (1) bekezdésében és a 30. § (1) bekezdésében foglalt esetben a szűrést követő hatvan munkanapon belül végzi el. A szűrés elvégzésének napja a határidőbe nem számít bele.

(3) A szolgáltató a szűrései során figyelembe veszi a belső kockázatértékelése alapján kialakított szokatlan tranzakciókra figyelmeztető jelzéseket.

(4) A kiszűrt ügyfél, illetve ügylet elemzésének és értékelésének folyamatát a szolgáltató úgy dokumentálja, hogy a szolgáltató által végrehajtott intézkedés eredménye és az az alapján hozott döntés utólag rekonstruálható legyen.

32. § (1) A szolgáltató a belső ellenőrző és információs rendszer részeként névtelenséget biztosító visszaélésbejelentési rendszert működtet.

(2) Visszaélés-bejelentést az (1) bekezdésben foglaltak szerinti visszaélésbejelentési rendszeren keresztül az tehet, aki tudomással bír arról, hogy a szolgáltatónál a Pmt. rendelkezése megsértésre kerül vagy került.

(3) A visszaélés-bejelentést a szolgáltató harminc napon belül kivizsgálja. A határidőbe a bejelentés megtételének napja nem számít bele.

(4) A visszaélés-bejelentés kivizsgálásában nem vehet részt a bejelentéssel érintett személy.

(5) Ha a szolgáltató azt állapítja meg, hogy pénzmosásra, terrorizmusfinanszírozásra vagy dolog büntetendő cselekményből való származására utaló adat, tény, illetve körülmény merül fel, a kijelölt személy haladéktalanul bejelentést tesz a pénzügyi információs egységnek.

(6) Ha a szolgáltató azt állapítja meg, hogy bűncselekmény gyanúja áll fenn, haladéktalanul feljelentést tesz a hatáskörrel és illetékességgel rendelkező nyomozó hatóságnál.

(7) Ha a szolgáltató az (5) és (6) bekezdésben foglalt eseteken kívül a Pmt., az Európai Unió és az Egyesült Nemzetek Szervezetének Biztonsági Tanácsa (a továbbiakban: ENSZ BT) által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény vagy e rendelet megsértését állapítja meg, e tényt a kijelölt személy haladéktalanul bejelenti az MNB-nek.

(8) A szolgáltató a bejelentés megtételét követően biztosítja, hogy a bejelentéshez a bejelentést tevőn vagy a szolgáltató foglalkoztatottján, mint a bejelentés kivizsgálásában érintett személyen kívül más személy ne férhessen hozzá.

33. § A szolgáltató biztosítja, hogy a belső ellenőrző és információs rendszer képes legyen az üzleti kapcsolat leválogatására

a) a Pmt. által előírt személyes adat,
b) a fizetési számla pénzforgalmi jelzőszáma vagy IBAN-ja,

c) ügyfélszám,
d) ügylettípus vagy
e) összeghatár
alapján.

34. § A szolgáltató biztosítja, hogy a belső ellenőrző és információs rendszer képes legyen a benne rögzített adatoknak a Pmt.-ben meghatározott időtartam alatt visszakereshetőséget lehetővé tevő nyilvántartására.

9. Az Európai Unió és az ENSZ BT által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtása érdekében működtetett szűrőrendszer kidolgozása és működtetésének minimumkövetelményei

35. § Ezen alcím alkalmazásában
1. *automatikus szűrőrendszer:* az ügyfél, a tényleges tulajdonos, a rendelkezésre jogosult, a meghatalmazott és a képviselő személyes adatainak uniós jogi aktusban és az Egyesült Nemzetek Szervezete Biztonsági Tanácsának határozatában (a továbbiakban: ENSZ BT határozat) szereplő személyek adataival való folyamatos, emberi beavatkozást nem igénylő összehasonlítására alkalmas informatikai rendszer,
2. *manuális szűrés:* az ügyfél, a tényleges tulajdonos, a rendelkezésre jogosult, a meghatalmazott és a képviselő személyes adatainak uniós jogi aktusban és ENSZ BT határozatban szereplő személyek adataival való összehasonlítására alkalmas, emberi beavatkozást igénylő eljárás,
3. *szankciós szűrőrendszer:* olyan szűrőrendszer, amely biztosítja a pénzügyi és vagyoni korlátozó intézkedéseket elrendelő uniós jogi aktusok és ENSZ BT határozatok haladéktalan és teljes körű végrehajtását.

36. § A szolgáltató szankciós szűrőrendszerrel rendelkezik.

37. § A szolgáltató a szankciós szűrőrendszer keretében automatikus szűrést alkalmaz, ha a szolgáltató ügyfeleinek száma a tárgyévet megelőző év végén meghaladta az ezret, egyéb esetben a szolgáltató manuális szűréssel is biztosíthatja a pénzügyi és vagyoni korlátozásokat elrendelő uniós jogi aktusok és ENSZ BT határozatok haladéktalan végrehajtását.

38. § (1) A szolgáltató belső eljárásrendet készít a szankciós szűrőrendszer működése, illetve kiszűrt ügyfél, tényleges tulajdonos, rendelkezésre jogosult, meghatalmazott és képviselő, valamint ügylet elemzése és értékelése vonatkozásában.

(2) Az (1) bekezdésben meghatározott belső eljárásrendet a szolgáltató írásban rögzíti, naprakészen tartja, és azt a felügyeleti jogkörében eljáró MNB rendelkezésére bocsátja.

(3) A szankciós szűrőrendszer belső eljárásrendje legalább az alábbi feltételeknek felel meg:
a) dokumentálja a szolgáltató által használt keresési logikákat, az azok alapjául szolgáló feltételezésekkel, paraméterekkel,
b) biztosítja az adatok integritását, pontosságát és minőségét annak érdekében, hogy a szankciós szűrőrendszeren pontos és teljes adatok menjenek keresztül,
c) rögzíti a releváns adatokat tartalmazó összes adatforrást,
d) biztosítja a szankciós szűrőrendszer megtervezéséért, működtetéséért, teszteléséért, beüzemeléséért és folyamatos felügyeletéért, valamint az esetkezelésért, felülvizsgálatért és a találatok és lehetséges bejelentések tekintetében hozott döntésekért felelős szakképzett alkalmazottak vagy külső tanácsadók rendelkezésre állását,
e) rögzíti az elemző- és értékelőfolyamat során alkalmazott határidőket,
f) olyan vizsgálati protokollokat tartalmaz, amelyek részletesen bemutatják, hogy a szankciós szűrőrendszer által generált figyelmeztetéseket milyen módon kell megvizsgálni, milyen módon kell dönteni afelől, hogy mely találatok kerüljenek bejelentésre, ki a felelős az ilyen döntés meghozataláért, valamint hogy milyen módon kell a döntéshozatali eljárást dokumentálni,
g) biztosítja a szűrési logikák és az azok alapjául szolgáló szabályok, paraméterek folyamatos vizsgálatát, és
h) automatikus szűrőrendszer esetén lehetővé teszi a szankciós szűrőrendszer teljes folyamatát nyomon követő, valamint a bevezetését megelőző és azt követő tesztelését, csakúgy, mint az időszakos tesztelések elvégzését

az irányítás, adatok leképezése, ügyletek azonosítása, keresési logikák, szűrési modellezés, valamint bevitt adatok és az eredmények vizsgálatával.

39. § (1) A szolgáltató az Európai Unió és az ENSZ BT által elrendelt pénzügyi és vagyoni korlátozó intézkedésekre vonatkozó szűrést folyamatosan végzi. A szűrés folyamatosságát huszonnégy órát meghaladóan akadályozó körülmény szolgáltató tudomására jutásáról és az ennek kiküszöbölésére foganatosított, illetve foganatosítani tervezett intézkedésekről a szolgáltató haladéktalanul, elektronikus formában, az ERA rendszeren keresztül tájékoztatja az MNB-t.

(2) A szolgáltató a kiszűrt találatokat elemzi és értékeli.

(3) A szolgáltató a (2) bekezdés alapján végzett értékelő-elemző munka eredményességét és a szűrőrendszerének hatékony működését kockázati alapon, a működési modellje figyelembevételével a szolgáltató valamennyi védelmi vonalának bevonásával, rendszeresen ellenőrzi.

(4) A kiszűrt találatok elemzésének és értékelésének folyamatát, valamint ezek ellenőrzését a szolgáltató úgy dokumentálja, hogy a szolgáltató által végrehajtott intézkedés eredménye és az az alapján hozott döntés utólag rekonstruálható legyen.

10. A képzési program

40. § (1) A szolgáltató a pénzmosás és a terrorizmusfinanszírozás megelőzésével és megakadályozásával, valamint az Európai Unió és az ENSZ BT által elrendelt pénzügyi és vagyoni korlátozó intézkedésekkel összefüggő tevékenység ellátásában részt vevő megfelelési vezetőjét és foglalkoztatottját (a továbbiakban együtt: foglalkoztatott) ebben a munkakörben történő alkalmazását megelőzően vagy a belépést követő harminc napon belül képzésben részesíti (a továbbiakban: megelőzési képzés), és részére a belépés évét követően évente legalább egy alkalommal továbbképzést szervez (a továbbiakban együtt: képzés). A képzés része a szolgáltató által szervezett írásbeli vizsga, ideértve a szolgáltató elektronikus rendszereiben lebonyolított vizsgát is.

(2) A foglalkoztatott pénzmosás és a terrorizmusfinanszírozás megelőzésével és megakadályozásával, valamint az Európai Unió és az ENSZ BT által elrendelt pénzügyi és vagyoni korlátozó intézkedésekkel összefüggő tevékenység ellátásában csak az (1) bekezdésben meghatározott képzéssel összefüggő sikeres vizsgát tett munkatárs felügyelete mellett vehet részt mindaddig, amíg a megelőzési képzésen megszerzett ismeretekről a szolgáltató által szervezett vizsgát sikeresen nem teljesíti.

(3) A szolgáltató a képzések tartására csak olyan személyt vehet igénybe, aki

a) szakirányú felsőfokú – így különösen jogi, közgazdasági, pénzügyi vagy informatikai – végzettséggel, valamint

b) legalább hároméves,

ba) a Pmt. hatálya alá tartozó szolgáltatónál belső ellenőrzési vagy megfelelőségi (compliance) feladatokat ellátó területen szerzett szakmai gyakorlattal vagy

bb) a Pmt. 5. §-ában meghatározott felügyeletet ellátó szervnél a Pmt. hatálya alá tartozó felügyeleti tevékenység ellátása területén szerzett szakmai gyakorlattal

rendelkezik.

(4) A szolgáltató az egyes munkakörök betöltéséhez szükséges mélységű képzési programot állít össze, a képzési program az egyes munkakörök betöltéséhez szükséges témaköröket tartalmazza.

(5) A szolgáltató a képzések, valamint az ezekhez kapcsolódó vizsgák anyagát, a képzések időpontját és a résztvevők névsorát, a vizsga javítókulcsát, a vizsgázók névsorát és vizsgázónként a vizsgaeredményeket visszakereshető módon nyilvántartja, és a vizsga napjától számított öt évig őrzi.

(6) A szolgáltató megfelelési vezetője felelős a szolgáltató képzési programjának kidolgozásáért, a megelőzési képzés határidőben történő megszervezéséért, a foglalkoztatottak képzésen történő részvételi lehetőségének biztosításáért, az (5) bekezdésben meghatározott adatok visszakereshető módon történő nyilvántartásáért, valamint a (2) bekezdésben foglaltak betartásának ellenőrzéséért.

(7) A csoportszintű politikák és eljárások kidolgozása során a szolgáltató figyelembe veszi az (1)–(6) bekezdésben foglaltakat.

V. FEJEZET
A KÜLSŐ ELLENŐRZÉSI FUNKCIÓT ELLÁTÓ SZEMÉLY SZAKMAI KÖVETELMÉNYEI ÉS IGÉNYBEVÉTELÉNEK KÖTELEZŐ ESETEI

11. A külső ellenőrzési funkciót ellátó személy kijelölésére és igénybevételére vonatkozó szabályok

41. § (1) A Pmt. 3. § 21a. pontjában meghatározottak szerinti külső ellenőrzési funkciót az a személy láthatja el, aki legalább 5 éves igazolt szakmai tapasztalattal rendelkezik a szolgáltató által nyújtott szolgáltatások ellenőrzése vagy az azokkal kapcsolatos tanácsadás tekintetében.

(2) A szolgáltató az MNB felhívására bizonyítja, hogy az általa kijelölt külső ellenőrzési funkciót ellátó fél és annak a külső ellenőrzési funkciót ténylegesen ellátó alkalmazottja (a továbbiakban együtt: külső ellenőr) megfelelő ismeretekkel rendelkezik az alábbiak tekintetében:

a) a szolgáltató szektorára irányadó jogszabályi követelmények,

b) a szolgáltató által alkalmazott rendszerek,

c) a szolgáltató által bevezetett szabályzatok és eljárásrendek, valamint

d) a szolgáltató által nyújtott áruk.

(3) A külső ellenőr kijelölése során a szolgáltató figyelembe veszi, hogy a külső ellenőr nem lehet azonos

a) a szolgáltató jogszabályi kötelezettségen alapuló könyvvizsgálatát a külső ellenőrzési vizsgálat időpontját megelőző három évben ellátó könyvvizsgálóval vagy könyvvizsgáló céggel, sem a szolgáltató által a külső ellenőrzési vizsgálat időpontját megelőző három évben a pénzmosás és terrorizmusfinanszírozás megelőzésével kapcsolatos normatív elvárásokat tartalmazó rendelkezéseknek való megfelelés érdekében igénybe vett jogi tanácsadóval vagy jogi képviselővel,

b) a szolgáltató által alkalmazott rendszereket szállító vagy azokat működtető szolgáltatóval, a szolgáltató hatályos belső eljárásrendjét kidolgozó külső szolgáltatóval, illetve az ilyen rendszerek beszerzése vagy az eljárásrendek kidolgozása során tanácsadói feladatkört betöltő szolgáltatóval, valamint

c) a szolgáltató, a szolgáltató leányvállalata vagy a (4) bekezdésben felsorolt személyek tulajdonában álló vállalkozással.

(4) Nem tölthet be külső ellenőrzési funkciót az, aki a megbízást megelőző három évben a szolgáltatónál az alábbi funkciókat töltötte be:

a) a vizsgált szolgáltató alkalmazottja,

b) a vizsgált szolgáltató vezető tisztséget betöltő alkalmazottja,

c) a vizsgált szolgáltató audit bizottságának tagja, vagy ilyen bizottság hiányában az audit bizottság feladatainak megfelelő feladatokat ellátó testület tagja vagy

d) a vizsgált szolgáltató vezető testületének tagja.

(5) A külső ellenőr megbízatása eseti jellegű vagy határozott idejű lehet. A külső ellenőrzési funkció ellátására szóló határozott idejű megbízás legfeljebb két évre szólhat. A megbízás lejártát követően az eredeti megbízás időtartamának kétszereséig terjedő időszakban a külső ellenőr számára a szolgáltató újabb külső ellenőrzési megbízást nem adhat. A rendszeresen ismétlődő eseti jellegű megbízásokat e bekezdés alkalmazásában egy összefüggő, határozott idejű megbízásnak kell tekinteni.

(6) A Pmt. 60. § (2) bekezdés e) pontjában írtakat is figyelembe véve a külső ellenőr kiválasztására vonatkozó eljárásrendet a szolgáltató belső szabályzatban rögzíti.

(7) Külső ellenőrzési funkció igénybevétele esetén a szolgáltató a Pmt. 27. § (1) bekezdésében meghatározott belső kockázatértékelése alapján a Pmt. 65. §-ában meghatározott belső szabályzatban naprakészen meghatározza mindazon vizsgálandó témaköröket, amelyekre a külső ellenőr által készített ellenőrzési jelentésnek ki kell terjednie a szolgáltató kockázatainak csökkentése és kezelése érdekében. Határozott idejű megbízás esetén a belső szabályzatban rögzített, vizsgálandó területek kiterjednek legalább a szolgáltató által a pénzmosás és terrorizmusfinanszírozás megelőzése és megakadályozása érdekében használt szűrő-, bejelentési és az ügyfelek kockázati besorolását támogató rendszerek megfelelésének vizsgálatára.

42. § (1) A szolgáltató legalább a következő esetekben alkalmaz külső ellenőrzési funkciót:

a) amennyiben a szolgáltató a belső kockázatértékelésében beazonosítottak alapján külső ellenőrzési funkció igénybevételéről dönt,

b) amennyiben az MNB a szolgáltatót annak belső kockázatértékelésében foglaltak figyelembevételével külső ellenőr igénybevételére kötelezi, valamint

c) amennyiben a szolgáltató éves átlagban legalább százezer, a szolgáltatóval üzleti kapcsolatot létesítő ügyféllel rendelkezik, és a szolgáltató szűrőrendszere által generált kockázati intézkedést igénylő jelzések éves száma eléri a tízezer darabot, vagy szűréseihez mesterséges intelligenciára épített megoldást alkalmaz; továbbá a szolgáltató által igénybe vett vagy alkalmazott, a pénzmosás és terrorizmusfinanszírozás megelőzése és megakadályozása érdekében használt szűrő-, bejelentési és az ügyfelek kockázati besorolását támogató rendszerek külső ellenőrzési funkció által történő vizsgálatára 5 éven belül nem került sor.

(2) A szolgáltató az MNB felhívására a felhívásban szereplő szempontok értékelése érdekében külső ellenőrzési vizsgálatot rendel el.

12. A külső ellenőr működésére vonatkozó szabályok

43. § (1) A külső ellenőr a feladata ellátása során nem utasítható és senki által nem befolyásolható.

(2) A külső ellenőr a szolgáltatónál végzett vizsgálatról az eseti megbízás lejáratakor, határozott idejű megbízás esetén pedig legalább naptári évenként ellenőrzési jelentést készít, amelyben gyakorlati példákkal alátámasztott megállapításokat és észrevételeket tesz annak értékelése érdekében, hogy a szolgáltató képes-e a Pmt.-ben, valamint az annak felhatalmazásán alapuló jogszabályban foglalt kötelezettségek teljesítésére, és hogy az ehhez szükséges eljárásrendjei, az általa alkalmazott rendszerek, valamint a belső és külső erőforrásai megfelelők és elégségesek-e. A külső ellenőr szükség szerint soron kívüli jelentést is készíthet.

(3) A külső ellenőr által készített ellenőrzési jelentés tartalmazza a szolgáltató jogszabályi megfelelése érdekében megtenni szükséges, valamint a (2) bekezdésében meghatározott szempontok vizsgálata alapján szükségesnek ítélt intézkedésekre vonatkozó javaslatokat is.

(4) A külső ellenőr az ellenőrzési jelentését közvetlenül a szolgáltató vezető testületének küldi meg. A szolgáltató vezető testülete a külső ellenőr ellenőrzési jelentését testületi ülésén megvitatja, amely során a külső ellenőr meghívottként jelen lehet.

(5) A szolgáltató a külső ellenőr ellenőrzési jelentését haladéktalanul az MNB és a szolgáltató megfelelési vezetője rendelkezésére bocsátja.

44. § A külső ellenőr az általa a szolgáltatónak okozott kár megtérítése érdekében felelősségbiztosítással rendelkezik, amely garantálja a tevékenységével kapcsolatos esetleges helytállási kötelezettség teljesítését.

45. § (1) A szolgáltató és a külső ellenőr között létrejött megbízási szerződés tartalmazza legalább

a) a 11. alcímben foglaltak szerint a külső ellenőr alkalmasságának szakmai ismertetését és az alkalmassági követelményeknek való megfelelésre vonatkozó nyilatkozatát, beleértve valamennyi közreműködője alkalmasságát is,

b) a külső ellenőr feladatának ellátáshoz szükséges tárgyi feltételek és rendszerhozzáférési jogosultságok meghatározását,

c) a külső ellenőr felelősségbiztosításával kapcsolatos, 44. § szerinti feltételek meghatározását,

d) a kötelezettséget arra vonatkozóan, hogy a külső ellenőr vagy az általa igénybe vett közreműködő részt vesz az MNB által szervezett vagy az MNB által megfelelőként elismert és a honlapján közzétett szakmai képzésen,

e) a megbízási szerződés azonnali felmondásával kapcsolatos feltételek között annak rögzítését, ha a külső ellenőr teljesítése során az alkalmatlanságát bizonyító tények merülnek fel, és

f) a külső ellenőr alkalmazását – a 42. §-ban foglaltak szerint – megalapozó tények ismertetését.

(2) A szolgáltató az MNB felhívására bemutatja, hogy milyen intézkedéseket tett a megbízási szerződésben foglalt, a külső ellenőrt terhelő kötelezettségek szerződésszerű teljesítésének betartatása érdekében.

VI. FEJEZET
ZÁRÓ RENDELKEZÉSEK

13. Hatályba léptető rendelkezések

46. § (1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – 2024. július 1-jén lép hatályba.

(2) A 12–14. §, a 41–45. § és a 47–51. § 2025. március 1-jén lép hatályba.

14. Módosító rendelkezések

47. § A rendelet 2. §-a a következő 2a. ponttal egészül ki:
(E rendelet alkalmazásában)
„2a. *eredendő kockázat:* a kockázatcsökkentés előtt fennálló kockázatszint,"

48. § A rendelet 2. alcíme helyébe a következő alcím lép:
„2. A fokozott ügyfél-átvilágítás esetkörei, valamint az egyszerűsített ügyfél-átvilágítás során alkalmazandó küszöbérték és határidő
10. § (1) A szolgáltató a Pmt.-ben meghatározottakon túl fokozott ügyfél-átvilágítást alkalmaz legalább azokban az esetekben, ha ügyfele
a) a szolgáltató belső kockázatértékelése alapján
aa) magas terrorizmusfinanszírozási kockázatot hordozó nonprofit szervezet,
ab) magas proliferáció-finanszírozási kockázatot hordozó szervezet,
ac) működéséhez különösen jelentős készpénzforgalmazást lebonyolító szervezet,
ad) magas földrajzi kockázatú területhez szorosan kapcsolódó szervezet,
b) olyan jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amelynek tényleges tulajdonosa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országból származik,
c) olyan részvénytársaság, amelynek bemutatóra szóló részvénye van, vagy amelynek részvényesét részvényesi meghatalmazott képviseli,
d) olyan jogi személy vagy jogi személyiséggel nem rendelkező szervezet, amelynek tulajdonosi és irányítási szerkezete a jogi személy vagy jogi személyiséggel nem rendelkező szervezet üzleti tevékenységének jellegéhez képest szokatlannak vagy túlzottan összetettnek tűnik, vagy
e) olyan tényleges tulajdonossal rendelkezik, aki nem működik együtt a 7. § b) pont bb) alpontja szerinti ügyfélismereti beszélgetésben.
(2) Az (1) bekezdés d) pontjában foglaltak nem alkalmazandók, ha a szolgáltató megítélése szerint a jogi személy vagy jogi személyiséggel nem rendelkező szervezet túlzottan összetett tulajdonosi szerkezete megindokolható, és azt a szolgáltató belső kockázatértékelésében részletesen a kockázatcsökkentő és -növelő tényezők együttes értékelésével alátámasztja, vagy az ügyfél a Pmt. 6/A. §-a szerinti besorolás alapján alacsony kockázatú.
11. § (1) A szolgáltató egyszerűsített ügyfél-átvilágítást alkalmazhat, ha ügyfele a Pmt. 6/A. §-a szerinti besorolás alapján alacsony kockázatú.
(2) Egyszerűsített ügyfél-átvilágítás alkalmazása esetén a szolgáltató belső kockázatértékelésében rögzíti azt az észszerű küszöbértéket és határidőt, amely elérésekor sor kerül a Pmt. 15. § (1b) bekezdésében meghatározott intézkedések végrehajtására.
(3) Az intézkedés küszöbértékének és határidejének meghatározása akkor tekinthető észszerűnek, ha a Pmt. 15. § (1b) bekezdésében meghatározott intézkedéseknek az ügyfélkapcsolat létesítéstől eltérő időpontban való végrehajtása nem növeli a pénzmosás vagy a terrorizmusfinanszírozás kockázatát, és pénzmosásra vagy terrorizmusfinanszírozásra utaló adat, tény vagy körülmény nem merül fel.
(4) Nem szükséges a belső kockázatértékelésben küszöbértéket meghatározni azon esetekre, amelyeknél a folyamatosan csekély pénzmosási kockázat miatt az intézkedésekre kizárólag a Pmt. 12. § (1) és (2) bekezdésében meghatározott ellenőrzési kötelezettség teljesítése során kerül sor."

49. § A rendelet 17. és 18. §-a helyébe a következő rendelkezések lépnek:
„17. § (1) A szolgáltató a Pmt.-ben meghatározottakon túl legalább a következő esetekben alkalmaz megerősített eljárást:
a) a takarékbetétről szóló törvényerejű rendelet szerinti nem névre szóló takarékbetét névre szólóvá alakításával érintett ügyfél tekintetében, ha a névre szólóvá alakítani kívánt takarékbetétek összértéke eléri a négymillió-ötszázezer forintot, az átalakítástól számított egy évig,
b) ha az ügyfelet a szolgáltató húszmillió forintot elérő vagy meghaladó pénzváltás miatt világítja át, az utolsó húszmillió forintot elérő vagy meghaladó pénzváltástól számított egy évig,
c) ha az ügyleti megbízásokat rendszeresen adó ügyfelet a szolgáltató ötvenmillió forintot elérő vagy meghaladó összegű ügyleti megbízás miatt világítja át, az utolsó ötvenmillió forintot elérő vagy meghaladó ügylettől számított egy évig,

d) ha az ügyfél készpénzforgalma – azaz befizetéseinek és pénzfelvételeinek összege – a havi százmillió forintot eléri vagy meghaladja, az utolsó százmillió forintot elérő vagy meghaladó készpénzforgalmú hónapot követően egy évig,
e) ha a szolgáltató ügyfelével kapcsolatban szolgáltató által vagy a csoporton belül, amelyhez a szolgáltató tartozik, a Pmt. 30. § (1) bekezdése szerinti bejelentés történt, az utolsó bejelentéstől számított egy évig,
f) nem magyar állampolgárságú és kilencven napot meghaladó magyarországi tartózkodásra jogosító engedéllyel vagy tartózkodási regisztrációval, lakóhellyel vagy tartózkodási hellyel nem rendelkező, az Európai Unió területén kívüli lakóhellyel vagy tartózkodási hellyel rendelkező természetes személynél,
g) ha a szolgáltató ügyfelével kapcsolatban olyan levelezőbanki vagy hatósági megkeresést kap, amely alapján a szolgáltató értékelése szerint megnőtt az ügyfélhez kapcsolható pénzmosás kockázata, a jelzés érkezésétől számított egy évig, továbbá
h) ha a szolgáltató ügyfele székhelyéül székhelyszolgáltatót jelölt meg, és az ügyfélkapcsolat létesítését követő 3 hónapon belül Magyarország területén kívülre pénzátutalást teljesített, a pénzátutalástól számított egy évig.
(2) A szolgáltató a megerősített eljárásnak az (1) bekezdésben meghatározottakon kívüli egyéb eseteit a belső kockázatértékelésében rögzíti.
(3) A szolgáltató az általa meghatározott ügyfelek egy csoportja tekintetében mellőzheti a megerősített eljárást, ha az (1) bekezdés szerinti esetekre vonatkozóan a belső kockázatértékelésében részletesen, a kockázatcsökkentő és -növelő tényezők együttes értékelésével azt alátámasztja.
18. § (1) A szolgáltató a megerősített eljárás alá tartozó ügyfeleknél a 28–33. § rendelkezéseinek megfelelően kockázatalapon, de minden esetben 30 munkanapon belül szűri, és pénzmosás és terrorizmus finanszírozása szempontjából elemzi és értékeli a belső kockázatértékelésben meghatározott ügyleteket.
(2) Az (1) bekezdésben meghatározott kockázatértékelés során a szolgáltató a megerősített eljárás alá tartozó ügyfelekre ügyletenként és egy adott időszakra vonatkozó több ügyletre összesített értékhatárt is alkalmaz.
(3) A belső kockázatértékelésben meghatározott értékhatárt a szolgáltató a kockázatcsökkentő és -növelő tényezők együttes értékelésével, kockázatalapon, ügyletenként határozza meg.
(4) A szolgáltató a megerősített eljárás alá tartozó ügyfelek esetében – a megerősített eljárást megalapozó feltétel teljesülését követően – az ügyfele pénzmosás szempontjából kockázatos ügyletei vonatkozásában
a) haladéktalanul beszerzi a pénzeszköz forrására vonatkozó információkat, valamint ezen információk igazoló ellenőrzése érdekében a pénzeszközök forrására vonatkozó dokumentumok bemutatását is megköveteli,
b) ellenőrzi, hogy az ügyféllel vagy annak jelentős ügyleti partnereivel kapcsolatban nem merült-e fel negatív jellegű, hiteles és megbízható nyilvános forrásból származó információ, továbbá
c) megvizsgálja, hogy ügyfele üzleti tevékenysége gazdasági szempontból racionális-e.”

50. § A rendelet 6. alcíme helyébe a következő alcím lép:

„6. A belső kockázatértékelés elkészítésének szabályrendszere

19. § (1) A belső kockázatértékelés keretében a szolgáltató beazonosítja a már ismert kockázatai közül azokat, amelyek hatással vannak a pénzmosási és terrorizmusfinanszírozási kockázataira.
(2) A szolgáltató a belső kockázatértékelés keretében az egyedi ügyfélszintre vonatkozó és az egyes üzletági tevékenységeire kiterjedő kockázatok értékelését is elvégezi. A szolgáltató az üzleti tevékenységekre vonatkozó kockázatértékelést beépíti az egyedi ügyfélszintű kockázatértékelések módszertanába is.
(3) A szolgáltató az (1) bekezdésben foglalt kötelezettsége teljesítése során kockázatérzékenységi alapon határozza meg az információforrások típusát és számát, valamint a bevezetendő rendszerek és kontrollmechanizmusok körét, figyelembe véve üzleti tevékenysége jellegét és összetettségét is.
(4) Amennyiben a szolgáltató egy olyan csoport tagja, amely csoportszintű kockázatértékelést dolgoz ki, mérlegeli, hogy a csoportszintű kockázatértékelés kellően részletes és specifikus-e ahhoz, hogy tükrözze a szolgáltató üzleti tevékenységét és azokat a kockázatokat, amelyeknek a szolgáltató ki van téve, és szükség esetén a belső kockázatértékelése alapján kiegészíti a csoportszintű kockázatértékelést. Ha a csoport anyavállalatának székhelye stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban található, a szolgáltató ezt akkor is figyelembe veszi kockázatértékelésében, ha a csoportszintű kockázatértékelés nem tesz említést róla.
20. § (1) A pénzmosási és terrorizmusfinanszírozási kockázat feltárásához a szolgáltató különféle forrásokból származó információkat használ fel, amelyekhez egyedileg, illetve a rendelkezésre álló, több forrásból származó információkat összesítő eszközök vagy adatbázisok útján férhet hozzá.
(2) Az adatbázisokban foglaltakon túlmenően a szolgáltató a pénzmosási és terrorizmusfinanszírozási kockázati tényezők beazonosítása során

a) a civil társadalomtól,
b) harmadik ország pénzmosás és terrorizmusfinanszírozás elleni rendszere megfelelőségével és hatékonyságával, korrupcióellenes és adózási rendszerével kapcsolatos értékeléséből,
c) hiteles és megbízható nyilvános forrásból,
d) tudományos és felsőoktatási intézményektől,
e) szakmai érdekképviseleti szervezetektől, valamint
f) hiteles és megbízható kereskedelmi szervezetektől
származó információkat is figyelembe vehet.

21. § (1) A szolgáltató biztosítja, hogy rendelkezzen az újonnan felmerülő pénzmosási és terrorizmusfinanszírozási kockázatok feltárására szolgáló rendszerekkel és kontrollmechanizmusokkal, valamint, hogy értékelni tudja, és adott esetben időben be tudja építeni e kockázatokat az üzleti tevékenysége egészére kiterjedő és az egyedi kockázatértékelésébe.

(2) A szolgáltató által a felmerülő kockázatok feltárása érdekében bevezetendő rendszerek és kontrollmechanizmusok közé tartoznak legalább a következők:
a) olyan eljárások, amelyek biztosítják a szolgáltató belső üzleti működése során szerzett információk rendszeres felülvizsgálatát a tendenciák és a felmerülő kockázatok azonosítása érdekében, mind az egyedi üzleti kapcsolatok, mind a szolgáltató üzletági tevékenységével kapcsolatban,
b) olyan eljárások, amelyek biztosítják, hogy a szolgáltató mind az ügyfélszintű egyedi, mind az üzletági tevékenysége egészére kiterjedő kockázatértékelések tekintetében rendszeresen ellenőrizze a releváns információforrásokat, köztük a 20. §-ban meghatározott információforrásokat, beleértve az azok alapján szükséges intézkedések megtételét is,
ba) az ügyfélszintű egyedi kockázatértékelések tekintetében:
1. a terrorizmussal kapcsolatos riasztásokat, valamint a pénzügyi szankciórendszereket és ezek változásait azok közzétételét követően haladéktalanul, és
2. a szolgáltatás működése szerinti ágazatok vagy joghatóságok szempontjából releváns médiabeszámolókat,
bb) az üzletági tevékenységekre kiterjedő kockázatértékelések tekintetében:
1. a bűnüldözési riasztásokat és jelentéseket,
2. az illetékes hatóságok által kiadott tematikus értékeléseket és
3. a kockázatokra, különösen az ügyfelek, országok vagy földrajzi területek új kategóriáival, az új árukkal, új alkalmazott eszközzel, valamint az új megfelelési rendszerekkel és kontrollmechanizmusokkal kapcsolatos kockázatokra vonatkozó információk gyűjtésére és felülvizsgálatára szolgáló eljárásokat, valamint
c) a szolgáltató ágazatának más képviselőivel és az illetékes hatóságokkal folytatott együttműködés során szerzett információk, továbbá olyan eljárások, amelyek arra szolgálnak, hogy a szolgáltató munkavállalói visszajelzést kapjanak valamely megállapításról.

22. § A szolgáltató az üzletági tevékenységei kockázati tényezőinek beazonosítása során a Pmt. 27. §-ában foglaltakon túl az alábbiakat is figyelembe veszi:
a) az Európai Bizottság nemzetek feletti kockázatértékelését,
b) az európai felügyeleti hatóságok véleményét az európai uniós pénzügyi ágazatot érintő pénzmosási és terrorizmusfinanszírozási kockázatokról,
c) az MNB által kiadott ajánlást,
d) az MNB által nyilvánosságra hozott információkat,
e) az MNB által folytatott eljárás során keletkezett és nyilvánosságra hozott határozatokat,
f) az Európai Bizottság jegyzékét a kiemelt kockázatot jelentő harmadik országokról,
g) a Magyarország Kormánya által elfogadott nemzeti kockázatértékelést,
h) a pénzmosási és terrorizmusfinanszírozási tárgyú jogszabályok indokolását,
i) a pénzügyi információs egységektől és bűnüldöző hatóságoktól származó információkat,
j) az első ügyfél-átvilágítási folyamat és a folyamatos ügyfélmonitoring keretében szerzett információkat,
k) az általa kínált áru, az elvégzett tevékenység és ügylet természetét és összetettségét,
l) az általa alkalmazott megoldást, beleértve az ingyenes szolgáltatásnyújtást, az ügynök vagy a közvetítő használatát,
m) a kiszolgált ügyfelek típusait és
n) az üzleti tevékenység földrajzi területeit, különösen, ha azt stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik országban végzi, vagy az ügyfelei jelentős részének származási országa stratégiai hiányosságokkal rendelkező, kiemelt kockázatot jelentő harmadik ország.

23. § (1) A szolgáltató átfogó képet alakít ki az általa feltárt pénzmosási és terrorizmusfinanszírozási kockázati tényezőkről, amelyek együttes figyelembevételével határozza meg az üzletági és ügyfélszintű pénzmosási és terrorizmusfinanszírozási kockázat szintjét.

(2) A szolgáltató a kockázatértékelés során figyelembe veszi az eredendő kockázatokat és az általa meghatározott kockázatcsökkentő intézkedéseket, majd az így megállapított pénzmosási és terrorizmusfinanszírozási kockázati szint alapján a belső kockázatértékelésében kategorizálja az üzletágait, valamint üzleti kapcsolatait és ügyleti megbízásait.

(3) A szolgáltató a kockázatokat legalább alacsony, átlagos és magas kockázati kategóriába sorolja.

(4) A szolgáltató a (3) bekezdésben meghatározottaknak megfelelően definiált kockázatokat üzletági és ügyfél szinten is legalább ügyfél, áru, alkalmazott eszköz, földrajzi kockázati csoportba sorolja. A szolgáltató üzletági tevékenységeinek kockázatértékelései együttesen képezik a szolgáltató egyedi ügyfélszintű kockázatértékelésének alapját. Ügyfélszinten az üzletági szinten elvégzett kockázatértékelést nem kell megismételni, elégséges az ügyfélhez kapcsolódó üzleti kockázatra utalni, ha további egyedi ügyfél tényezőket ehhez a szolgáltató ügyfélszinten nem vesz figyelembe.

(5) A szolgáltató a kockázati tényező relatív jelentősége alapján üzletáganként eltérően súlyozhatja a kockázatot és az azokat mérséklő tényezőket.

(6) A kockázati tényezők súlyozásakor a szolgáltató biztosítja a következőket:

a) a súlyozást indokolatlanul ne befolyásolja kizárólag egyetlen tényező,

b) üzleti szempontokon alapuló megfontolások ne befolyásolják a kockázatminősítést,

c) a súlyozás ne vezessen olyan helyzethez, amelyben egyetlen üzleti kapcsolat sem sorolható magas kockázati kategóriába,

d) az ügyfelek kockázati besorolása kerüljön az informatikai rendszerben rögzítésre, és azok naprakészségét kockázatértékeléstől és a szolgáltató méretétől függően a rendszerbe épített automatizált informatikai megoldások támogassák,

e) a jogszabályban meghatározott magas pénzmosási kockázatot jelentő helyzetekre vonatkozó rendelkezéseket ne írhassa felül a szolgáltató súlyozása,

f) a szolgáltató kockázatértékelése ne kizárólagosan automatizmusokon alapuljon, szükség esetén a szolgáltató felülírhassa az automatikusan megállapított kockázati értékeket, továbbá

g) a kockázatértékelés során megállapított kockázati értékek felülírására vonatkozó döntés és annak indokolása visszakereshetően rögzítve legyen.

(7) A szolgáltató kockázatérzékenységi alapon meghatározza a belső kockázatértékeléséhez alkalmazott módszertan átfogó felülvizsgálatának gyakoriságát.

24. § (1) A szolgáltató Pmt. 65. § (1) bekezdése szerinti belső szabályzatában a beazonosított kockázat értékelését követően az ügyfélszintű kockázat mértékével arányosan meghatározza, hogy milyen intézkedésre van szükség a feltárt kockázatok kezelése érdekében. A szolgáltató az egyedi ügyfélszintű kockázatértékelések elvégzésekor mérlegeli az MNB kapcsolódó ajánlásában foglaltakat is.

(2) Az üzletági és az ügyfélszintű kockázatértékelést is tartalmazó, a belső kockázatértékelésről szóló jelentést a szolgáltató irányítási funkciót betöltő testülete vagy annak hiányában a vezető tisztségviselője hagyja jóvá.

25. § A szolgáltató a belső kockázatértékelését naprakészen tartja, minden naptári évre vonatkozóan egy időpontot meghatározva, amikor az üzleti tevékenység egészére kiterjedő kockázatértékelés aktualizálását el kell végezni.

25/A. § A szolgáltató a belső kockázatértékelését soron kívül felülvizsgálja, legalább azokban az esetekben, ha

a) külső hatás megváltoztatja a kockázat természetét,

b) a szolgáltató tulajdonosaival, a vezető testület tagjaival, a fő funkciókat ellátó személyekkel vagy a szervezetével kapcsolatban új információk merülnek fel, továbbá

c) minden egyéb esetben, amikor a szolgáltatónak alapos oka van azt feltételezni, hogy a kockázatértékelés alapjául szolgáló információ már nem alkalmazható."

51. § A rendelet 8. alcíme helyébe a következő alcím lép:

„8. A belső ellenőrző és információs rendszer működtetése

27. § Ezen alcím alkalmazásában

1. *automatikus szűrőrendszer:* az ügyfél és az ügylet pénzmosás és terrorizmusfinanszírozás szempontjából, előzetes paraméterezés alapján történő, emberi beavatkozást nem igénylő leválogatására alkalmas informatikai rendszer,

2. *manuális szűrés:* az ügyfél és az ügylet pénzmosás és terrorizmusfinanszírozás szempontjából történő, emberi beavatkozást igénylő leválogatása,

3. *szűrőrendszer:* a bejelentés teljesítését támogató rendszer, amely biztosítja a pénzmosás és terrorizmusfinanszírozás szempontjából kockázatos ügyfél és szokatlan ügylet kiszűrését, valamint a bejelentés megtételéhez szükséges adatok rendelkezésre bocsátását.

28. § (1) A szolgáltató a belső ellenőrző és információs rendszer részeként olyan szűrőrendszerrel rendelkezik, amely az ügyletek valós idejű monitoringját is biztosítja.

(2) A szolgáltató – a (3) bekezdésben meghatározott kivétellel – manuális szűréseken alapuló szűrőrendszert alkalmazhat.

(3) A szolgáltató automatikus szűrőrendszert működtet, ha

a) pénzforgalmi szolgáltatási tevékenységet végez, vagy

b) ügyfeleinek száma a tárgyévet megelőző év végén meghaladta az ötvenezret.

29. § A szolgáltató által alkalmazott szűrőrendszer legalább a következőket biztosítja:

a) a szokatlan vagy gyanús ügyletek feltárását,

b) a pénzmosás és terrorizmusfinanszírozás gyanúja szempontjából releváns ügyletek nyomon követését,

c) a b) pont szerinti ügyletekhez kapcsolódó ügyfelek kockázati profiljának összhangját a szolgáltató ügyfélre vonatkozó szélesebb körű ismereteivel,

d) a szűrőrendszer által tárolt jelzések összhangját a szolgáltató birtokában lévő dokumentumokkal, adatokkal vagy információkkal annak megértése céljából, hogy változott-e az üzleti kapcsolathoz társuló kockázat, és az arról való meggyőződés érdekében, hogy a folyamatos nyomon követés alapját képező információk pontosak-e és

e) amennyiben a szűrés eredményének lezárásához szükséges, további adatok – különösen a pénzeszközök vagy vagyon forrására vonatkozó dokumentumok – beszerzését.

30. § A szolgáltató az MNB felhívására bizonyítja, hogy az ügylet monitoringját szolgáló szűrőrendszere hatékony és megfelelő.

31. § (1) A szolgáltató a szűrések feltételeit, intenzitását és az ügylet monitoringjának gyakoriságát a belső kockázatértékelése alapján határozza meg, figyelembe véve az üzleti tevékenységének jellege, nagyságrendje és összetettsége, valamint a kockázati kitettségének szintje alapján kialakított szokatlan ügyletekre figyelmeztető jelzéseket és az MNB jelzéseit is.

(2) A szolgáltató a kiszűrt ügyfél, illetve ügylet pénzmosás és terrorizmusfinanszírozás szempontjából történő elemzését és értékelését kockázatalapon, de legfeljebb a szűrés elvégzésének napját követő hatvan munkanapon belül végzi el.

(3) A szolgáltató belső kockázatértékelésébe haladéktalanul beépíti az MNB által – a bűnügyi érdekek biztosítása céljából a nyilvánosság korlátozása mellett – adott tájékoztatást azokról a szűrési feltételekről, amelyek valós idejű ügyletmonitoringot tesznek szükségessé, vagy a (2) bekezdésben meghatározott hatvan munkanapnál gyorsabb értékelést követelnek meg.

(4) A szolgáltató a (2) bekezdés alapján végzett értékelő-elemző munka eredményességét és a szűrőrendszerének hatékony működését kockázati alapon, a működési modellje figyelembevételével, külső ellenőrzési funkció vagy annak hiányában további védelmi vonalak bevonásával rendszeresen ellenőrzi.

(5) A kiszűrt ügyfél, illetve ügylet elemzésének és értékelésének folyamatát, valamint ezek ellenőrzését a szolgáltató úgy dokumentálja, hogy a szolgáltató által végrehajtott intézkedés eredménye és az az alapján hozott döntés utólag rekonstruálható legyen.

32. § (1) A szolgáltató a szűrőrendszer működéséről, a kiszűrt ügyfél, valamint az ügylet elemzésének és értékelésének menetéről belső eljárásrendet készít.

(2) Az (1) bekezdés szerinti belső eljárásrendet a szolgáltató írásban rögzíti, naprakészen tartja, és felhívásra az MNB rendelkezésére bocsátja.

(3) A szűrőrendszerre vonatkozó belső eljárásrend megfelel legalább az alábbi feltételeknek:

a) a szolgáltató belső kockázatértékelésén alapul,

b) megfelel a szolgáltató kapcsolódó belső szabályzatainak,

c) dokumentálja a szolgáltató által használt szcenáriókat, az azok alapjául szolgáló logikákkal, paraméterekkel és küszöbértékekkel, és biztosítja a változások nyomonkövethetőségét,

d) biztosítja az adatok integritását és minőségét annak érdekében, hogy a szűrőrendszeren pontos és teljes adatok menjenek keresztül,

e) rögzíti a releváns adatokat tartalmazó összes adatforrást,

f) biztosítja a szűrőrendszer megtervezéséért, működtetéséért, teszteléséért, beüzemeléséért és folyamatos felügyeletéért, valamint az esetkezelésért, felülvizsgálatért és a találatok és lehetséges bejelentések tekintetében hozott döntésekért felelős szakképzett alkalmazottak vagy külső tanácsadók rendelkezésre állását,

g) rögzíti az elemző- és értékelőfolyamat során alkalmazott határidőket,
h) olyan vizsgálati protokollokat tartalmaz, amelyek részletesen bemutatják, hogy a szűrőrendszer által generált figyelmeztetéseket milyen módon kell megvizsgálni, milyen módon kell dönteni afelől, hogy mely találatok kerüljenek bejelentésre, ki a felelős az ilyen döntés meghozataláért, valamint azt, hogy milyen módon kell a döntéshozatali eljárást dokumentálni,
i) biztosítja a szcenáriók és az azok alapjául szolgáló logikák, paraméterek és küszöbértékek kockázataival összhangban történő felülvizsgálatát, és tartalmazza, hogy ki a felelős azok felülvizsgálatáért,
j) meghatározza, hogy mely ügyleteket követi nyomon valós időben, és mely ügyleteket követi nyomon utólag, ennek részeként legalább a következőkről rendelkezik:
ja) melyek azok a magas kockázatot jelző tényezők vagy a magas kockázatot jelző tényezők azon kombinációi, amelyek minden esetben valós idejű ügyletmonitoringot tesznek szükségessé, és
jb) a valós időben nyomon követett ügyletek esetében melyek a magasabb pénzmosási és terrorizmusfinanszírozási kockázatok, különös tekintettel azon ügyletekre, amelyek esetében az üzleti kapcsolathoz fokozott kockázat társul, valamint
k) automatikus szűrőrendszer esetén előírja a szűrőrendszer teljes folyamatát nyomon követő, valamint a bevezetését megelőző és azt követő tesztelését, csakúgy, mint az időszakos tesztelések elvégzését az irányítás, az adatok leképezése, az ügyletek azonosítása, a keresési szcenáriók és logikák, a szűrési modellezés, valamint a bevitt adatok és az eredmények vizsgálatával kapcsolatosan.
33. § A szolgáltató a szűrést folyamatosan végzi. A szűrés folyamatosságát huszonnégy órát meghaladóan akadályozó körülménynek a szolgáltató tudomására jutásáról és az ennek kiküszöbölésére foganatosított, illetve foganatosítani tervezett intézkedésekről a szolgáltató haladéktalanul, elektronikus formában, az MNB Elektronikus Rendszer Hitelesített Adatok Fogadásához megnevezésű rendszerén (a továbbiakban: ERA rendszer) keresztül tájékoztatja az MNB-t.
34. § (1) A szolgáltató a belső ellenőrző és információs rendszer részeként névtelenséget biztosító visszaélésbejelentési rendszert működtet.
(2) Visszaélés-bejelentést az (1) bekezdésben foglaltak szerinti visszaélésbejelentési rendszeren keresztül az tehet, aki tudomással bír arról, hogy a szolgáltatónál a Pmt. rendelkezése megsértésre kerül vagy került.
(3) A visszaélés-bejelentést a szolgáltató a beérkezését követő harminc napon belül kivizsgálja.
(4) A visszaélés-bejelentés kivizsgálásában nem vehet részt a bejelentéssel érintett személy.
(5) Ha a szolgáltató azt állapítja meg, hogy pénzmosásra, terrorizmus finanszírozására vagy dolog büntetendő cselekményből való származására utaló adat, tény, illetve körülmény merül fel, a kijelölt személy haladéktalanul bejelentést tesz a pénzügyi információs egységnek.
(6) Ha a szolgáltató azt állapítja meg, hogy bűncselekmény gyanúja áll fenn, haladéktalanul feljelentést tesz a hatáskörrel és illetékességgel rendelkező nyomozó hatóságnál.
(7) Ha a szolgáltató az (5) és (6) bekezdésben foglalt eseteken kívül a Pmt., az Európai Unió és az Egyesült Nemzetek Szervezetének ENSZ Biztonsági Tanácsa (a továbbiakban: ENSZ BT) által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény vagy e rendelet megsértését állapítja meg, e tényt a kijelölt személy haladéktalanul bejelenti az MNB-nek.
(8) A szolgáltató a bejelentés megtételét követően biztosítja, hogy a bejelentéshez a bejelentést tevőn vagy a szolgáltató foglalkoztatottján mint a bejelentés kivizsgálásával foglalkozó személyen kívül más személy ne férhessen hozzá.
34/A. § A szolgáltató biztosítja, hogy a belső ellenőrző és információs rendszer képes legyen az üzleti kapcsolatnak
a) a Pmt. által előírt személyes adat;
b) fizetési számla pénzforgalmi jelzőszáma vagy IBAN-ja;
c) az ügyfélszám;
d) az ügylettípus vagy
e) az összeghatár
alapján történő leválogatására.
34/B. § A szolgáltató biztosítja, hogy a belső ellenőrző és információs rendszer képes legyen a benne rögzített adatoknak a Pmt.-ben meghatározott időtartam alatt visszakereshetőséget lehetővé tevő nyilvántartására."

15. Hatályon kívül helyező rendelkezés

52. § Hatályát veszti a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól szóló 26/2020. (VIII. 25.) MNB rendelet.

Virág Barnabás s. k.,
a Magyar Nemzeti Bank alelnöke

A Magyar Nemzeti Bank elnökének 31/2024. (VI. 24.) MNB rendelete az anticiklikus tőkepuffer képzésének feltételeiről és az anticiklikus tőkepufferráta mértékéről szóló 27/2022. (VII. 8.) MNB rendelet módosításáról

A Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 171. § (1) bekezdés k) pont kb) alpontjában kapott felhatalmazás alapján, a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény 4. § (7) bekezdésében meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § Az anticiklikus tőkepuffer képzésének feltételeiről és az anticiklikus tőkepufferráta mértékéről szóló 27/2022. (VII. 8.) MNB rendelet 3. §-a a következő c) ponttal egészül ki:
(A Magyarországon lévő féllel szembeni kitettségekre vonatkozó anticiklikus tőkepufferráta mértéke)
„c) 2025. július 1-jétől 1 százalék."

2. § Ez a rendelet a kihirdetését követő napon lép hatályba.

Virág Barnabás s. k.,
a Magyar Nemzeti Bank alelnöke

A Szabályozott Tevékenységek Felügyeleti Hatósága elnökének 7/2024. (VI. 24.) SZTFH rendelete a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 28. § (3) bekezdés h) pontjában, valamint a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 29. § f) pontjában kapott felhatalmazás alapján,
a 7. §, a 8. § és az 1. melléklet tekintetében a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 29. § b) pontjában kapott felhatalmazás alapján,
a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § n) és q) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § (1) A Szabályozott Tevékenységek Felügyeleti Hatósága mint a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan.tv.) 22. § (1) bekezdése szerinti kiberbiztonsági felügyeletet ellátó hatóság (a továbbiakban: felügyeleti hatóság) kiberbiztonsági felügyeleti tevékenysége keretében végzi a kiberbiztonsági audit végrehajtására jogosult gazdálkodó szervezet (a továbbiakban: auditor) vonatkozásában a Kibertan.tv. 23. § (6) bekezdése szerinti nyilvántartás (a továbbiakban: nyilvántartás) vezetését.

(2) A felügyeleti hatóság eljárása a felügyeleti hatóság által e célra rendszeresített elektronikus űrlapon kezdeményezhető.

2. § (1) Az auditornak a nyilvántartásba történő felvételére irányuló eljárás kérelemre indul, amelyet az auditor nyújt be a felügyeleti hatósághoz.

(2) Az (1) bekezdés szerinti kérelem tartalmazza

a) az auditor

aa) megnevezését,

ab) adószámát,

ac) cégjegyzékszámát,

ad) székhelyének címét,

ae) – felügyeleti hatóság honlapján közzétételre kerülő – elektronikus levelezési címét és telefonszámát és

af) – felügyeleti hatóság által tájékoztatási célra felhasználható – elektronikus levelezési címét az auditor kérelemben rögzített kérése alapján,

b) azt, hogy az auditor a kiberbiztonsági audit tevékenységet milyen biztonsági osztályba sorolt elektronikus információs rendszerekre kívánja végezni,

c) az auditor kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát, elektronikus levelezési címét, valamint

d) az auditor által a kiberbiztonsági audit során igénybe vett közreműködő adatait, valamint kijelölt kapcsolattartója azonosításához szükséges természetes személyazonosító adatait, telefonszámát és elektronikus levelezési címét.

(3) Az auditor az (1) bekezdés szerinti kérelemhez mellékeli

a) a (6) bekezdésben meghatározott dokumentumokat, valamint

b) a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének a Szabályozott Tevékenységek Felügyeleti Hatósága kiberbiztonsági feladataival összefüggő eljárásainak igazgatási szolgáltatási díjairól szóló rendeletében meghatározott igazgatási szolgáltatási díj megfizetésének igazolását.

(4) Az auditornak – az (1) bekezdés szerinti kérelemben feltüntetett bármely biztonsági osztály esetében – a következő feltételeknek kell megfelelnie:

a) legalább két olyan szakértőt foglalkoztat, aki a felsőoktatásban szerezhető képesítések jegyzékéről és az új képzések létesítéséről szóló miniszteri rendelet szerinti műszaki vagy informatika képzési területen felsőfokú végzettséggel rendelkezik,

b) rendelkezik információbiztonsági szabályzattal, valamint tanúsított információbiztonsági irányítási rendszerrel,

c) rendelkezik olyan biztonságos kommunikációs eszközökkel, szoftverekkel, amelyek garantálják a vizsgálathoz felhasznált adatok bizalmasságát, sértetlenségét és hitelességét a vizsgált szervezetekkel való kapcsolattartás során,

d) rendelkezik az auditálás lefolytatásához szükséges adatok törlésére vonatkozó jogszabályi előírások teljesítése érdekében olyan törlési eljárásrenddel és megoldásokkal, amelyek biztosítják az adatok visszaállíthatatlan módon történő törlését a rendszereikből és az archív mentéseikből, és

e) rendelkezik a Kibertan.tv. 23. § (11) bekezdése szerinti szabályzattal.

(5) Az auditornak a nyilvántartásba vételi eljárás során igazolnia kell – a (2) bekezdés b) pontjában megjelölt biztonsági osztályhoz tartozóan – a következő feltételek teljesítését:

a) foglalkoztat

aa) „alap" biztonsági osztály esetén legalább kettő,

ab) „jelentős" biztonsági osztály esetén legalább tíz,

a munka törvénykönyvéről szóló törvény szerinti munkavégzésre irányuló jogviszonyban álló személyt a Kibertan.tv. 23. § (11) bekezdése szerinti szabályzatban rögzített munkakörben;

b) rendelkezik

ba) „alap" biztonsági osztály esetén minimum 15 000 000 forint,

bb) „jelentős" biztonsági osztály esetén minimum 50 000 000 forint

éves összeghatárig kiterjedő tevékenységi felelősségbiztosítással;

c) rendelkezik informatikai biztonsági funkciókat megvalósító szoftvertermékek vagy elektronikus információs rendszerek biztonságának hazai vagy nemzetközi informatikai biztonsági módszertanon alapuló auditálás szolgáltatásra vonatkozóan
   ca) „alap" biztonsági osztály esetén legalább 5,
   cb) „jelentős" biztonsági osztály esetén legalább 15
   referenciával;
d) „jelentős" biztonsági osztály esetén rendelkezik a nyilvántartásba vételi kérelem benyújtását megelőző 7 évben legalább 5 éven keresztül a minősített adat védelméről szóló 2009. évi CLV. törvény 16. §-a alapján kiállított telephelybiztonsági tanúsítvánnyal;
e) „jelentős" biztonsági osztály esetén az auditjelentés kiállításához a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelete szerinti „jelentős" vagy „magas" megbízhatósági szint követelményeinek megfelelő vizsgálólaboratóriumot vesz igénybe;
f) „magas" biztonsági osztály esetén szerepel a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelete szerinti megfelelőségértékelő szervezetek jegyzékén „magas" megbízhatósági szinten.

(6) Az auditor a Kibertan.tv. 23. § (4) bekezdésében meghatározott és a (4) és (5) bekezdés szerinti feltételek meglétét a következő módon igazolja:
a) a Kibertan.tv. 23. § (4) bekezdésének teljesülését az Alkotmányvédelmi Hivatal által kiállított nyilvántartásba vételi határozattal;
b) a (4) bekezdés a) pontja esetében az érintett munkavállalók felsőfokú végzettséget igazoló okirat másolatával és szakmai önéletrajzzal;
c) a (4) bekezdés b) pontja esetében az információbiztonsági szabályzattal, valamint az információbiztonsági irányítási rendszerre kiállított tanúsítvánnyal;
d) a (4) bekezdés c) pontja esetében a biztonságos kommunikációs eszközök és szoftverek műszaki dokumentációjával;
e) a (4) bekezdés d) pontja esetében törlési eljárásrenddel és műszaki leírásokkal;
f) a (4) bekezdés e) pontja esetében a Kibertan.tv. 23. § (11) bekezdése szerinti szabályzattal;
g) az (5) bekezdés a) pontja esetében anonimizált munkaszerződésekkel;
h) az (5) bekezdés b) pontja esetében biztosítási kötvénnyel;
i) az (5) bekezdés c) pontja esetében referencianyilatkozattal;
j) az (5) bekezdés d) pontja esetében telephelybiztonsági tanúsítvánnyal;
k) az (5) bekezdés e) pontja esetében a közreműködő vizsgálólaboratórium nyilatkozatával;
l) az (5) bekezdés f) pontja esetében a nyilvántartásba vételi határozat számának megjelölésével.

(7) Ha a kérelmező auditort a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelete alapján megfelelőségértékelő szervezetként nyilvántartásba vették, és a (2) bekezdés b) pontjában megjelölt biztonsági osztály nem magasabb a megfelelőségértékelő szervezetként nyilvántartásba vett megbízhatósági szintnél, a (4) bekezdés a)–d) pontjában és az (5) bekezdés a), b) és d) pontjában foglaltak igazolására nem köteles.

(8) A felügyeleti hatóság a benyújtott dokumentumok hitelességét a kiállító szerv bevonásával ellenőrizheti.

(9) Ha az auditor a Kibertan.tv. 23. § (4) bekezdésében meghatározott és a (4) és (5) bekezdésben szereplő feltételeket nem teljesíti, a felügyeleti hatóság a nyilvántartásba vételre irányuló kérelmet elutasítja. A kérelmező auditor a hatósági döntés véglegessé válását követő 90 napon belül új nyilvántartásba vételi kérelmet nem nyújthat be.

(10) A felügyeleti hatóság nyilvántartja a (2) bekezdés a) pont af) alpontja, a (2) bekezdés b) pontja és a (6) bekezdés szerinti adatokat.

3. § (1) A nyilvántartásba vett auditornak folyamatosan meg kell felelnie a Kibertan.tv. 23. § (4) bekezdésében meghatározott és a 2. § (4) és (5) bekezdése szerinti feltételeknek.

(2) A nyilvántartásba vett auditornak minden év január 31-ig az előző évben megkezdett, folyamatban lévő, illetve lezárult kiberbiztonsági audit lefolytatására irányuló szerződései kapcsán adatot kell szolgáltatnia a felügyeleti hatóság részére.

(3) A (2) bekezdés szerinti adatszolgáltatás a következő adatokat tartalmazza a kiberbiztonsági audit lefolytatására irányuló szerződések tekintetében:

a) sorszám,
b) szerződéskötés dátuma,
c) teljesítési határidő,
d) teljesítés dátuma,
e) a kiberbiztonsági audit díja.

(4) Az auditor a Kibertan.tv. 23. § (7) bekezdése és a 2. § (2) bekezdés a) pontja szerinti adatokban bekövetkező változást annak bekövetkezésétől számított 15 napon belül bejelenti a nyilvántartásba vétel érdekében a felügyeleti hatóság részére a felügyeleti hatóság által rendszeresített elektronikus űrlap alkalmazásával.

(5) Az auditor a változás beálltát követő 8 napon belül bejelenti a felügyeleti hatóságnak, ha
a) a 2. § (4) bekezdése szerinti általános, valamint a 2. § (5) bekezdése szerinti, nyilvántartásba vett biztonsági osztályra vonatkozó követelmények nem teljesülnek, vagy
b) a legfőbb szerve a végelszámolásáról döntött, vagy csődeljárás, felszámolási eljárás vagy kényszertörlési eljárás indult ellene.

(6) A felügyeleti hatóság törli a nyilvántartásból az auditort, ha
a) a Kibertan.tv. 23. § (4) bekezdésében meghatározott feltételeknek nem felel meg,
b) a 2. § (4) és (5) bekezdése szerinti feltételeknek nem felel meg,
c) jogutód nélkül megszűnik, vagy
d) jogutódlásra került sor, és a jogutód a tevékenységet nem folytatja.

4. § Ez a rendelet a kihirdetését követő 31. napon lép hatályba.

5. § A 3. § (2) bekezdése szerinti adatszolgáltatási kötelezettséget az auditor első alkalommal 2025. március 1-jéig teljesíti.

6. § Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

7. § A Szabályozott Tevékenységek Felügyeleti Hatósága kiberbiztonsági feladataival összefüggő eljárásainak igazgatási szolgáltatási díjairól szóló 15/2023. (VII. 31.) SZTFH rendelet 1. §-a helyébe a következő rendelkezés lép:

„1. § (1) A Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: Hatóság) – mint a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan.tv.) 4. § (1) bekezdés a) pontjában kijelölt nemzeti kiberbiztonsági tanúsító hatóság – eljárásában a megfelelőségértékelő szervezetnek a Kibertan.tv. 14. § (1) bekezdése szerinti nyilvántartásba (a továbbiakban: tanúsítási nyilvántartás) vételére irányuló eljárás igazgatási szolgáltatási díja
a) „alap" megbízhatósági szint esetén 390 000 Ft,
b) „jelentős" megbízhatósági szint esetén 540 000 Ft,
c) „magas" megbízhatósági szint esetén 620 000 Ft.

(2) A tanúsítási nyilvántartásba vett megfelelőségértékelő szervezetek adatváltozás-bejegyzésére irányuló eljárás igazgatási szolgáltatási díja – a (3) bekezdésben foglalt kivétellel – 60 000 Ft.

(3) A tanúsítási nyilvántartásba vett megfelelőségértékelő szervezetek adatváltozás-bejegyzésére irányuló eljárás igazgatási szolgáltatási díja 80 000 Ft, ha a nemzeti akkreditáló szerv által akkreditált státuszban bekövetkezett változás a megfelelőségértékelő szervezet azon jogosultságát érinti, hogy mely nemzeti vagy európai kiberbiztonsági tanúsítási rendszer tekintetében jogosult megfelelőségértékelési tevékenység végzésére.

(4) A Kibertan.tv. 13. § (4) bekezdése szerinti engedélyezési eljárás igazgatási szolgáltatási díja 100 000 Ft.

(5) A Kibertan.tv. 11. § (2) bekezdése szerinti megfelelőségi nyilatkozat tanúsítási nyilvántartásba vételére irányuló eljárás igazgatási szolgáltatási díja 120 000 Ft.

(6) A Hatóság – mint a Kibertan.tv. 22. § (1) bekezdése alapján kijelölt hatóság – eljárásában az auditoroknak a Kibertan.tv. 23. § (6) bekezdése szerinti nyilvántartásba (a továbbiakban: felügyeleti nyilvántartás) vételére irányuló eljárás igazgatási szolgáltatási díja
a) „alap" biztonsági osztály esetén 390 000 Ft,
b) „jelentős" biztonsági osztály esetén 540 000 Ft,
c) „magas" biztonsági osztály esetén 620 000 Ft.

(7) A felügyeleti nyilvántartásba felvett auditor adatváltozásának bejegyzésére irányuló eljárás igazgatási szolgáltatási díja 60 000 Ft.”

8. § A Szabályozott Tevékenységek Felügyeleti Hatósága kiberbiztonsági feladataival összefüggő eljárásainak igazgatási szolgáltatási díjairól szóló 15/2023. (VII. 31.) SZTFH rendelet 1. melléklete helyébe az 1. melléklet lép.

Dr. Nagy László s. k.,
elnök

1. melléklet a 7/2024. (VI. 24.) SZTFH rendelethez
„1. melléklet a 15/2023. (VII. 31.) SZTFH rendelethez

A kérelemre induló eljárások azonosítására szolgáló kódok

	A	B
1.	Az eljárás megnevezése	Az eljárás kódja
2.	megfelelőségértékelő szervezet tanúsítási nyilvántartásba történő felvételére irányuló eljárás „alap” megbízhatósági szint esetén	SZTFH-401/1/1
3.	megfelelőségértékelő szervezet tanúsítási nyilvántartásba történő felvételére irányuló eljárás „jelentős” megbízhatósági szint esetén	SZTFH-401/1/2
4.	megfelelőségértékelő szervezet tanúsítási nyilvántartásba történő felvételére irányuló eljárás „magas” megbízhatósági szint esetén	SZTFH-401/1/3
5.	megfelelőségértékelő szervezet adatai változásának tanúsítási nyilvántartásba történő bejegyzésére irányuló eljárás	SZTFH-401/2
6.	a megfelelőségértékelő szervezet nemzeti akkreditáló szerv által akkreditált státuszában bekövetkezett 1. § (3) bekezdése szerinti változás tanúsítási nyilvántartásba történő bejegyzésére irányuló eljárás	SZTFH-401/3
7.	a Kibertan.tv. 13. § (4) bekezdése szerinti engedélyezési eljárás	SZTFH-401/4
8.	a Kibertan.tv. 11. § (2) bekezdése szerinti megfelelőségi nyilatkozat tanúsítási nyilvántartásba vételére irányuló eljárás	SZTFH-403
9.	auditor szervezet felügyeleti nyilvántartásba történő felvételére irányuló eljárás „alap” biztonsági osztály esetén	SZTFH-410/1/1
10.	auditor szervezet felügyeleti nyilvántartásba történő felvételére irányuló eljárás „jelentős” biztonsági osztály esetén	SZTFH-410/1/2
11.	auditor szervezet felügyeleti nyilvántartásba történő felvételére irányuló eljárás „magas” biztonsági osztály esetén	SZTFH-410/1/3
12.	auditor adatváltozásának felügyeleti nyilvántartásba történő bejegyzésére irányuló eljárás	SZTFH-410/2

”

V. A Kormány tagjainak rendeletei

A Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (2) bekezdés a) pontjában és a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 28. § (5) bekezdésében kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 9. § (1) bekezdés 6., 7., 14. és 16. pontjában meghatározott feladatkörömben eljárva – az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (2) bekezdés a) pontjában, valamint a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 28. § (6) bekezdésében biztosított véleményezési jogkörében eljáró Szabályozott Tevékenységek Felügyeleti Hatósága elnöke véleményének kikérésével – a következőket rendelem el:

1. § (1) Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet a rendelkezésében lévő elektronikus információs rendszert az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

(2) A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertantv.) hatálya alá tartozó elektronikus információs rendszert a Kibertantv. szerinti érintett szervezet (a továbbiakban: érintett szervezet) az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.

2. § (1) Az 1. § (1) bekezdésében foglaltak szerint elvégzett besorolás alapján az elektronikus információs rendszer felett rendelkezni jogosult szervezet a 2. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket az abban meghatározott módon teljesíti.

(2) Az elektronikus információs rendszer felett rendelkezni jogosult szervezetre és elektronikus információs rendszerére az e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív, logikai és fizikai védelmi intézkedések irányadóak. Ha ezen intézkedésektől egy elektronikus információs rendszer esetében a szervezet által elvégzett kockázatelemzés alapján indokolt eltérni, akkor az 1. mellékletben meghatározottak szerint kell eljárni.

(3) Ha az elektronikus információs rendszer felett rendelkezni jogosult szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(4) Ha az elektronikus információs rendszernek több felhasználó szervezete van, az elektronikus információs rendszer felett rendelkezni jogosult szervezet a felhasználó szervezet által alkalmazható elektronikus információbiztonsági követelményeket az elektronikus információs rendszer minden felhasználó szervezete tekintetében érvényesíti.

(5) Az elektronikus információs rendszer felett rendelkezni jogosult szervezet az elektronikus információbiztonsági követelményeket úgy érvényesíti a felhasználó szervezet tekintetében, hogy a követelményeknek való megfelelés a felhasználó szervezet elektronikus információbiztonsággal kapcsolatos eljárási rendjébe beépüljön.

(6) Az elektronikus információs rendszer felett rendelkezni jogosult szervezet a kockázatelemzés és a kockázatok kezelése körében azonosítja és dokumentálja az elektronikus információs rendszer bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket a 3. melléklet szerinti fenyegetéskatalógus elemeinek vizsgálatával.

3. § (1) Az 1. § (2) bekezdésében foglaltak szerint elvégzett besorolás alapján az érintett szervezet a 2. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket az abban meghatározott módon teljesíti.

(2) Az érintett szervezetre és elektronikus információs rendszereire az e rendelet előírásai szerint kidolgozott szabályzatokban meghatározott adminisztratív, logikai és fizikai védelmi intézkedések irányadóak. Ha ezen

intézkedésektől egy elektronikus információs rendszer esetében a szervezet által elvégzett kockázatelemzés alapján indokolt eltérni, akkor az 1. mellékletben meghatározottak szerint kell eljárni.

(3) Ha az érintett szervezet rendelkezési joga az elektronikus információs rendszernek csak egyes elemeire vagy funkcióira terjed ki, a 2. mellékletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

(4) Az érintett szervezet a kockázatelemzés és a kockázatok kezelése körében azonosítja és dokumentálja az elektronikus információs rendszer bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket a 3. mellékletben foglalt fenyegetéskatalógus elemeinek vizsgálatával.

(5) Az e rendelet 1. melléklet 3.2.6. pontjában foglalt rendelkezések az érintett szervezet tekintetében nem alkalmazhatók.

4. § (1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő napon lép hatályba.

(2) Az 1. § (1) bekezdése, a 2. § és a 6. § 2025. január 1-jén lép hatályba.

5. § Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

6. § Hatályát veszti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

Rogán Antal s. k.,
Miniszterelnöki Kabinetirodát vezető miniszter

1. melléklet a 7/2024. (VI. 24.) MK rendelethez

Az elektronikus információs rendszerek biztonsági osztályba sorolása és a védelmi intézkedések bevezetésének támogatására szolgáló kockázatmenedzsment keretrendszer

1. A KOCKÁZATMENEDZSMENT KERETRENDSZER

1.1. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény hatálya alá tartozó elektronikus információs rendszerrel rendelkező szervezet, valamint a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény szerinti érintett szervezet (a továbbiakban együtt: szervezet) a biztonsági osztályba sorolás és a védelmi intézkedések bevezetésének támogatására kockázatmenedzsment keretrendszert működtet, amelynek keretében

1.1.1. a keretrendszer alkalmazására való felkészülésként

1.1.1.1. a szervezetre vonatkozóan meghatározza és dokumentumban rögzíti:

1.1.1.1.1. az elektronikus információs rendszerei védelmével kapcsolatos szerepköröket, felelősségeiket, feladataikat és az ehhez szükséges hatásköröket,

1.1.1.1.2. a kockázatmenedzsment stratégiáját, amely leírja, hogy a szervezet hogyan azonosítja, értékeli, kezeli és felügyeli a biztonsági kockázatokat,

1.1.1.1.3. a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit,

1.1.1.2. az elektronikus információs rendszerekre vonatkozóan meghatározza és dokumentumban rögzíti:

1.1.1.2.1. a rendszer által támogatandó üzleti célokat, funkciókat és folyamatokat,

1.1.1.2.2. a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy szervezeteket,

1.1.1.2.3. az érintett vagyonelemeket,

1.1.1.2.4. a rendszer szervezeti és technológiai határát,

1.1.1.2.5. a rendszer által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát,

1.1.1.2.6. a rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését az 5. pontban meghatározott elvek szerint,

1.1.1.2.7. a rendszer helyét a szervezeti architektúrában, amennyiben a szervezet rendelkezik vele;

1.1.2. a 2. pontban meghatározott irányelvek szerint biztonsági osztályba sorolja az elektronikus információs rendszereit;

1.1.3. a 2. melléklet szerint beazonosítja a biztonsági osztályhoz tartozó védelmi intézkedéseket. A beazonosított intézkedéseket kockázatelemzés alapján testre szabja. Amennyiben a kockázatelemzés indokolja, a szervezet a 3. pontban meghatározott módon eltérhet a rendszerre vonatkozó biztonsági követelményektől, illetve a 4. pont szerint alkalmazhat helyettesítő védelmi intézkedéseket. Fentiek végrehajtásával megállapítja az elektronikus információs rendszerre értelmezendő és alkalmazandó biztonsági követelményeket. A szervezet a biztonsági követelményeket a rendszerbiztonsági tervben dokumentálja, amelyet szervezet vezetője vagy az elektronikus információs rendszer biztonságáért felelős szerepkört betöltő személy hagy jóvá. A szervezet a folyamatos felügyeleti stratégiával összhangban kidolgozza a rendszerre vonatkozó védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó eljárásrendet;

1.1.4. rangsorolja, majd végrehajtja a kiválasztott és a rendszerbiztonsági tervben dokumentált intézkedéseket. Az intézkedések végrehajtása során a szervezet a rendszerbiztonsági tervet a védelmi intézkedések tényleges megvalósítása, valamint a tervtől való esetleges eltérések alapján frissíti;

1.1.5. értékeli a megvalósított védelmi intézkedéseket, amelynek érdekében

1.1.5.1. meghatározza a védelmi intézkedések értékeléséért felelős szerepkört betöltő személyeket,

1.1.5.2. kialakítja, felülvizsgálja és jóváhagyja a megvalósított védelmi intézkedések értékelésének tervét,

1.1.5.3. az értékelési tervben meghatározott értékelési eljárásrend alapján értékeli a védelmi intézkedéseket,

1.1.5.4. a védelmi intézkedések értékelésének dokumentálásaként elkészíti az észrevételeket és javaslatokat tartalmazó értékelési jelentését,

1.1.5.5. az értékelési jelentésben foglalt észrevételek és javaslatok alapján a szervezet további intézkedéseket vezet be a követelmények teljesítése érdekében, majd újraértékeli a védelmi intézkedéseket, valamint intézkedési tervet készít a fennmaradó kockázatok kezelésére;

1.1.6. a szervezet a rendszer biztonsági állapotára vonatkozó dokumentumok (rendszerbiztonsági terv, értékelési jelentés, rendszer kockázatelemzés, intézkedési terv) alapján az üzembe helyezésére vagy üzemben tartására vonatkozó kockázatokat megvizsgálja, és a szervezet vezetője más személyre át nem ruházható feladatkörében eljárva – jegyzőkönyvben dokumentált módon – dönt a rendszer használatbavételéről vagy használatának folytatásáról;

1.1.7. a védelmi intézkedések folyamatos felügyeletével az elektronikus információs rendszer teljes életciklusa alatt gondoskodik arról, hogy a bekövetkezett szervezeti, technológiai és biztonsági környezetének változása esetén a védelmi intézkedések a kockázatokkal arányosak maradjanak. Ennek keretében:

1.1.7.1. figyelemmel kíséri az elektronikus információs rendszerben vagy a működési környezetében bekövetkezett, a rendszer biztonsági helyzetét befolyásoló változásokat, és ennek alapján frissíti a vonatkozó dokumentumokat,

1.1.7.2. a folyamatos felügyeleti stratégia alapján értékeli a rendszerben megvalósított védelmi intézkedéseket, azok állapotát rendszeresen jelenti a jogosult személyek felé,

1.1.7.3. rendszeresen felülvizsgálja az elektronikus információs rendszer biztonsági állapotát, hogy megbizonyosodjon arról, hogy az azonosított kockázatok elfogadhatók-e a szervezet számára,

1.1.7.4. biztosítja, hogy a rendszer élesüzemből való kivonására vonatkozó terv tartalmazza a felmerülő kockázatok kezeléséhez tartozó intézkedéseket.

2. A BIZTONSÁGI OSZTÁLYBA SOROLÁS

2.1. Általános irányelvek

2.1.1. A szervezet az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti.

2.1.2. Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet a szervezet vezetője hagy jóvá, hatáselemzés alapján kell elvégezni. Az elektronikus információs rendszerek biztonságának felügyeletét ellátó hatóság ajánlásként hatáselemzési módszertanokat ad ki. Ha a szervezet saját hatáselemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.

2.2. Biztonsági osztályok

2.2.1. A jogszabályban meghatározott biztonsági osztályba sorolás elvégzése a szervezet felelőssége. A biztonsági osztályba sorolás elvégzése során a 2.2.2–2.2.4. pont szerinti elvek, valamint szempontok figyelembevételével jár el.

2.2.2. Az „alap" biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:

2.2.2.1. az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,

2.2.2.2. a szervezet üzleti vagy ügymenete szempontjából csekély értékű vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,

2.2.2.3. a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy

2.2.2.4. a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg.

2.2.3. A „jelentős" biztonsági osztály esetében közepes káresemény következhet be, mivel:

2.2.3.1. nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,

2.2.3.2. személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),

2.2.3.3. a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,

2.2.3.4. a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy

2.2.3.5. a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át.

2.2.4. A „magas" biztonsági osztály esetében nagy káresemény következhet be, mivel

2.2.4.1. különleges személyes adat nagy mennyiségben sérülhet,

2.2.4.2. emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,

2.2.4.3. nemzeti adatvagyon helyreállíthatatlanul megsérülhet,

2.2.4.4. az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,

2.2.4.5. a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,

2.2.4.6. súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy

2.2.4.7. a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át.

3. ELTÉRÉSEK

3.1. Biztonsági osztályok

3.1.1. A szervezet az alábbi lehetséges eltérésekkel teljesítheti a 2. mellékletben meghatározott minimális követelményeket a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával, amellett, hogy a szervezetre érvényes minden kötelezettséget figyelembe kell venni.

3.1.2. A szervezet a vonatkozó szabályozásában dokumentálja és indokolja, hogy a jelen rendeletben foglalt védelmi intézkedésektől eltérő, általa meghatározott intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, kockázatokkal arányos biztonsági követelményszintjét, és azt, hogy miért nem használhatók a jelen rendeletben megjelölt védelmi intézkedések.

3.1.3. Az eltéréseket bemutató dokumentumot a szervezet vonatkozásában a szervezet vezetője vagy a kockázatok felvállalására jogosult szerepkört betöltő személy hagyja jóvá.

3.2. Egyedi eltérések

3.2.1. Működtetéssel, környezettel kapcsolatos eltérések:

3.2.1.1. A működtetési környezet jellegétől függő védelmi intézkedések csak akkor alkalmazandók, ha az elektronikus információs rendszert az intézkedéseket szükségessé tevő környezetben használják.

3.2.2. A fizikai infrastruktúrával kapcsolatos eltérések:

3.2.2.1. A szervezeti létesítményekkel kapcsolatos védelmi intézkedések csak azokra a létesítményekre alkalmazandók, amelyek közvetlenül nyújtanak védelmet vagy biztonsági támogatást az elektronikus információs rendszernek, vagy kapcsolatosak azzal.

3.2.3. A nyilvános hozzáféréssel kapcsolatos eltérések:

3.2.3.1. A nyilvánosan hozzáférhető információkra vonatkozó védelmi intézkedéseket körültekintően kell azonosítani és alkalmazni, mivel a vonatkozó védelmi intézkedés katalógus rész egyes védelmi intézkedései (például azonosítás és hitelesítés, személyi biztonsági intézkedések) nem minden esetben alkalmazhatók az elektronikus információs rendszerhez engedélyezett nyilvános kapcsolaton keresztül hozzáférő felhasználókra.

3.2.4. Technológiai eltérések:

3.2.4.1. A specifikus technológiára [például vezeték nélküli kommunikáció, kriptográfia, nyilvános kulcsú infrastruktúrán (PKI) alapuló hitelesítési eljárás] vonatkozó védelmi intézkedések csak akkor alkalmazandók, ha ezeket a technológiákat használják az elektronikus információs rendszerben, vagy jogszabály vagy szervezetre vonatkozó szabályozó előírja ezek használatát.

3.2.4.2. A védelmi intézkedések az elektronikus információs rendszer csak azon komponenseire vonatkoznak, amelyek az intézkedés által megcélzott biztonsági képességet biztosítják vagy támogatják, és az intézkedés által csökkenteni kívánt lehetséges kockázatok forrásai.

3.2.5. Biztonsági szabályozással kapcsolatos eltérések:

3.2.5.1. A tervezett vagy már működtetett elektronikus információs rendszerekre alkalmazott védelmi intézkedések kialakítása során figyelembe kell venni a rendszer célját meghatározó jogszabályi hátteret, funkciót is.

3.2.6. A védelmi intézkedések bevezetésének fokozatosságával kapcsolatos eltérések:

3.2.6.1. A védelmi intézkedések fokozatosan vezethetők be. A fokozatosságot a védendő elektronikus információs rendszerek biztonsági osztályozása alapján lehet felállítani.

3.2.7. Az elektronikus információs rendszer dokumentáltan elkülönített, informatikai biztonsági szempontból önállóan értékelhető elemei tekintetében a védelmi intézkedések a szervezet által elfogadott kockázatmenedzsment eljárásrendben rögzített vizsgálatot követően, külön-külön egyedi eltérésekkel is alkalmazhatóak, ha az elkülönített elemek közötti határvédelemről gondoskodtak. A határvédelem megfelelőségét, valamint az egyedi eltérések okát és mértékét dokumentálni és meghatározott gyakorisággal felülvizsgálni szükséges.

4. HELYETTESÍTŐ VÉDELMI INTÉZKEDÉSEK

4.1. A helyettesítő védelmi intézkedés alkalmazása olyan eljárás, amelyet a szervezet az adott biztonsági osztályhoz tartozó védelmi intézkedés helyett kíván alkalmazni, és egyenértékű vagy összemérhető védelmet nyújt az adott elektronikus információs rendszerre valós fenyegetést jelentő veszélyforrások ellen, és a helyettesített intézkedéssel egyenértékű módon biztosít minden külső vagy belső követelménynek (például jogszabályoknak vagy szervezeti szintű szabályozóknak) való megfelelést.

4.2. Egy elektronikus információs rendszer esetén a szervezet az alábbi feltételek egyidejű fennállása esetén alkalmazhat helyettesítő intézkedést:

4.2.1. a védelmi intézkedések katalógusa nem tartalmaz az adott viszonyok között eredményesen és kockázatarányosan alkalmazható intézkedést;

4.2.2. felméri és a kockázatelemzési és kockázatkezelési eljárásrendnek megfelelően elfogadja a helyettesítő intézkedés alkalmazásával kapcsolatos kockázatot;

4.2.3. a vonatkozó dokumentumban bemutatja, hogy a helyettesítő intézkedések hogyan biztosítják az elektronikus információs rendszer egyenértékű biztonsági képességeit, biztonsági

követelményszintjét, és azt, hogy miért nem használhatók a jelen rendeletben megjelölt védelmi intézkedések;

4.2.4. a helyettesítő védelmi intézkedések alkalmazását dokumentálja, és az eljárási rendnek megfelelően a szervezet vezetőjével vagy a kockázatok felvállalására jogosult szerepkört betöltő személlyel jóváhagyatja.

5. KOCKÁZATELEMZÉS ÉS A KOCKÁZATOK KEZELÉSE

5.1. A szervezet az 1.1.1.2.6. pontban előírt kockázatelemzést és a kockázatok kezelését az alábbiakban meghatározott elvek szerint hajtja végre.

5.1.1. A szervezet értékeli az elektronikus információs rendszerrel, az általa kezelt adatokkal kapcsolatosan felmerülő kockázatokat, amelynek keretében:

5.1.1.1. Azonosítja és dokumentálja az elektronikus információs rendszer és az általa feldolgozott adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket. Az azonosítás során legalább a 3. mellékletben található fenyegetés katalógus elemeit vizsgálja.

5.1.1.2. Azonosítja a sérülékenységeket és a hajlamosító körülményeket, amelyek befolyásolják annak valószínűségét, hogy a fenyegetések a szervezeti vagyonelemek, személyek, vagy más szervezetek számára káros hatásokhoz vezetnek.

5.1.1.3. Meghatározza annak a valószínűségét, hogy az 5.1.1.1. pontban azonosított fenyegetések a szervezeti vagyonelemek, folyamatok, személyek vagy más szervezetek számára káros hatásokat eredményeznek-e, figyelembe véve az 5.1.1.2. pontban meghatározottak szerint azonosított sérülékenységeket és körülményeket, valamint a szervezet a fenyegetések kihasználhatóságával kapcsolatosan végrehajtott ellenintézkedéseit.

5.1.1.4. Meghatározza a fenyegetések szervezeti vagyonelemekre, személyekre, vagy más szervezetekre vonatkozó lehetséges káros hatásait és azok mértékét.

5.1.1.5. Meghatározza a fenyegetések káros hatásainak és azok bekövetkezésének valószínűsége alapján az eredő kockázatokat, valamint legalább négy fokozatú skálán („alacsony”, „közepes”, „magas”, „kritikus”) azok mértékét (kockázati kategória).

5.1.1.6. Dokumentálja és a szervezeti döntéshozók számára kommunikálja a kockázatelemzés eredményét a kockázatkezelési válaszlépések támogatása érdekében, valamint biztosítja a kockázatelemzési folyamat során keletkezett információk megosztását az arra jogosultakkal.

5.1.2. A szervezet az azonosított kockázatokat az alábbiak szerint kezeli:

5.1.2.1. Eldönti és dokumentumban rögzíti, hogy az egyes kockázatok kezelése érdekében az alábbiak közül egyenként mely intézkedést alkalmazza:

5.1.2.1.1. kockázat elkerülése (például az elektronikus információs rendszer vagy a rendszerelemének, funkciójának használatból való teljes körű kivezetésével),

5.1.2.1.2. kockázat csökkentése védelmi intézkedések kialakításával és működtetésével,

5.1.2.1.3. kockázat áthárítása vagy megosztása harmadik felekkel,

5.1.2.1.4. kockázat felvállalása.

5.1.2.2. Biztosítja, hogy kizárólag a legalacsonyabb kockázati kategóriába eső kockázatok esetén alkalmaz részletes indoklás nélkül kockázatfelvállalást. Az ennél magasabb kategóriába eső kockázatok esetén az egyes kockázatok felvállalását a szervezet vezetője vagy a kockázatok kezeléséért felelős szerepkört betöltő személy kockázatonként történő indoklás mellett hagyja jóvá.

5.1.2.3. A kockázatelemzés eredményét felhasználja az elektronikus információs rendszer biztonsági osztálya megállapításának, valamint az 1.1.3. pontban meghatározottak szerint a védelmi intézkedések kiválasztásának és testre szabásának támogatására.

5.1.2.4. Az 1.1.4–1.1.7. pont szerint végrehajtja, értékeli és felügyeli a kockázatcsökkentő védelmi intézkedéseket.

5.1.3. A szervezet folyamatosan nyomon követi az elektronikus információs rendszerrel kapcsolatos kockázatok változásaihoz hozzájáruló tényezőket, és ennek alapján frissíti és naprakészen tartja a kockázatelemzési dokumentumait.

2. melléklet a 7/2024. (VI. 24.) MK rendelethez

Védelmi intézkedések katalógusa

1. Programmenedzsment

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	1.1. Információbiztonsági szabályzat	1.1. A szervezet: 1.1.1. Kidolgozza és kihirdeti az információbiztonsági szabályzatot, amely: 1.1.1.1. átfogó képet nyújt a biztonsági követelményekről, valamint a követelményeknek való megfelelés érdekében a szervezet által működtetett, vagy bevezetni kívánt védelmi intézkedésekről. 1.1.1.2. meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat. 1.1.1.3. Leírja az információbiztonságért felelős szervezeti egységek közötti együttműködést. 1.1.1.4. A szervezet vezetője által kerül jóváhagyásra, aki felelősséget vállal és elszámoltatható a szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért. 1.1.2. Felülvizsgálja és frissíti az információbiztonsági szabályzatot a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően. 1.1.3. Gondoskodik arról, hogy az információbiztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.	X	X	X
3.	1.2. Elektronikus információs rendszerek biztonságáért felelős személy	1.2. A szervezet vezetője a jogszabályi követelményeknek megfelelő, az elektronikus információs rendszerek biztonságáért felelős személyt nevez ki a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására és biztosítja számára a célok eléréséhez szükséges erőforrásokat.	X	X	X
4.	1.3. Információbiztonságot érintő erőforrások	1.3. A szervezet: 1.3.1. Beépíti az információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrásokat az éves költségvetés tervezésébe és beruházási kérelmeibe, valamint dokumentál minden olyan esetet, amelyek e követelmény alól kivételt képeznek. 1.3.2. Gondoskodik arról, hogy a szükséges dokumentáció összhangban legyen a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 1.3.3. Biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez tervezett forrásokat.	X	X	X

5.	1.4. Intézkedési terv és mérföldkövei	1.4. A szervezet: 1.4.1. Bevezet egy folyamatot, amely biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó szervezeti elektronikus információs rendszerek (a továbbiakban: EIR-ek) intézkedési tervei: 1.4.1.1. ki legyenek dolgozva és karban legyenek tartva; 1.4.1.2. dokumentálják a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket, hogy megfelelően reagáljanak a szervezeti műveletek és eszközök, személyek, más szervezetek kockázataira; 1.4.1.3. a meghatározott jelentési követelmények bemutatásra kerüljenek. 1.4.2. Áttekinti az intézkedési terveket és mérföldköveket, hogy azok összhangban állnak-e a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedések szervezeti szintű prioritásaival.	X	X	X
6.	1.5. Elektronikus információs rendszerek nyilvántartása	1.5. A szervezet létrehozza és a szervezet EIR-jeiben bekövetkezett változások (pl.: új rendszer bevezetése, meglévő rendszer kivezetése) esetén frissíti, valamint a szervezet által meghatározott gyakorisággal felülvizsgálja az EIR-ek nyilvántartását.	X	X	X
7.	1.6. Biztonsági teljesítmény mérése	1.6. A szervezet kifejleszti az EIR-ei biztonsági mérésének rendszerét, folyamatosan felügyeli a teljesítménymutatókat, és rendszeres jelentéseket készít ezekről.	X	X	X
8.	1.7. Szervezeti architektúra	1.7. A szervezet kifejleszti és fenntartja a szervezeti szervezetrendszert, amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a szervezeti működésre, az eszközökre, az egyénekre és más szervezetekre.	X	X	X
9.	1.8. Szervezeti Architektúra – Tehermentesítés	1.8. A szervezet más rendszerekbe, rendszerelemekbe szervezi át vagy külső szolgáltatóhoz szervezi ki a szervezet által meghatározott és a szervezet működése szempontjából nem kritikus funkciókat vagy szolgáltatásokat.	-	-	-
10.	1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve	1.9. A szervezet a szervezet működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket.	X	X	X
11.	1.10. Kockázatmenedzsment stratégia	1.10. A szervezet: 1.10.1. Kidolgoz egy átfogó stratégiát, amely kezeli: 1.10.1.1. Az EIR-ek működésével és használatával összefüggő, a szervezet működéséhez, vagyonelemeihez, a szervezethez köthető személyekhez, és más szervezetekhez kapcsolódó biztonsági kockázatokat 1.10.1.2. Személyes adatok kezeléséből fakadó kockázatokat. 1.10.2. Az egész szervezeten belül egységesen alkalmazza a kockázatmenedzsment stratégiát. 1.10.3. A szervezet által meghatározott gyakorisággal és esetekben felülvizsgálja és frissíti a kockázatmenedzsment stratégiát, hogy meg tudjon felelni a szervezeti változásoknak.	X	X	X
12.	1.11. Engedélyezési folyamatok meghatározása	1.11. A szervezet: 1.11.1. Engedélyezési folyamatokon keresztül kezeli az EIR-ek és azok környezetének biztonsági állapotát. 1.11.2. Kijelöli a szervezet kockázatmenedzsment folyamatának felelőseit (névvel és felelősségi körrel ellátva). 1.11.3. Beilleszti az engedélyezési folyamatokat a szervezet egészét átfogó kockázatmenedzsment keretrendszerbe.	X	X	X

13.	1.12. Szervezeti működés és üzleti folyamatok meghatározása	1.12. A szervezet: 1.12.1. Meghatározza a szervezeti célokat és az üzleti folyamatokat, figyelembe véve az információbiztonságot, valamint a szervezeti működésre, eszközökre, személyekre, más szervezetekre gyakorolt kockázatokat. 1.12.2. Meghatározza a szervezeti célokból és üzleti folyamatokból adódó információvédelmi igényeket. 1.12.3. Meghatározott gyakorisággal felülvizsgálja és módosítja a szervezeti célokat és az üzleti folyamatokat.	X	X	X
14.	1.13. Belső fenyegetés elleni program	1.13.A szervezet bevezet egy belső fenyegetések elleni programot, amely magában foglalja egy több szakterületet átfogó, belső fenyegetéssel kapcsolatos biztonsági események kezelését végző csoport működtetését.	-	-	-
15.	1.14. Biztonsági személyzet képzése	1.14. A szervezet létrehozza a biztonsági személyzet képzését és fejlesztését elősegítő programot.	X	X	X
16.	1.15. Tesztelés, képzés és felügyelet	1.15. A szervezet: 1.15.1. Bevezet egy folyamatot, amely biztosítja, hogy a szervezeti EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek elvégzésére vonatkozó szervezeti tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek. 1.15.2. Felülvizsgálja és összehangolja a terveit a szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal	X	X	X
17.	1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás	1.16. A szervezet: 1.16.1. Felveszi és kialakítja a kapcsolatot a kiválasztott szakmai csoportokkal és közösségekkel annak érdekében, hogy 1.16.1.1. elősegítse a szervezethez köthető személyek folyamatos biztonsági oktatását és képzését; 1.16.1.2. naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén; 1.16.1.3. megossza az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket.	X	X	X
18.	1.17. Fenyegetettség tudatosító program	1.17. A szervezet a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot vezet be, amely magában foglalja a fenyegetések felismerését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet.	X	X	X
19.	1.18. Fenyegetettség tudatosító program – Fenyegetési információk automatizált megosztása	1.18. A szervezet automatizált mechanizmusokat alkalmaz a fenyegetésekkel kapcsolatos információk megosztási hatékonyságának maximalizálása érdekében.	-	-	-
20.	1.19. Kockázatmenedzsment keretrendszer	1.19. A szervezet: 1.19.1. Azonosítja és dokumentálja: 1.19.1.1. a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő feltételezéseit; 1.19.1.2. a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő megkötéseit; 1.19.1.3. a kockázatmenedzsment során figyelembe vett prioritásokat és kompromisszumokat; továbbá 1.19.1.4. A szervezet kockázattűrő képességét. 1.19.2. Megosztja a kockázatmenedzsment tevékenység eredményeit a szervezet által meghatározott személyekkel. 1.19.3. A szervezet által meghatározott gyakorisággal elvégzi a kockázatmenedzsment keretrendszer szempontrendszerének felülvizsgálatát és frissítését.	X	X	X

21.	1.20. Kockázatkezelésért felelős szerepkörök	1.20. A szervezet kijelöl: 1.20.1. Egy kockázatkezelésért felelős személyt, aki összehangolja a szervezeti információbiztonsági irányítási folyamatokat a stratégiai, működési és költségvetés-tervezési folyamatokkal. 1.20.2. Egy kockázati vezető szerepkört betöltő személyt, aki biztosítja a kockázatok szervezeti szintű áttekintését és elemzését, valamint a kockázatmenedzsment szervezeten belüli egységes működését.	X	X	X
22.	1.21. Ellátási lánc kockázatmenedzsment stratégiája	1.21. A szervezet: 1.21.1. Kidolgoz egy a szervezet egészére kiterjedő, az ellátási lánc kockázatainak kezelésére vonatkozó stratégiát az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával, üzemeltetésével és selejtezésével kapcsolatosan. 1.21.2. Következetesen alkalmazza az ellátási lánc kockázatmenedzsment stratégiáját minden szervezeti egységében. 1.21.3. A változások lekövetésére az általa meghatározott gyakorisággal rendszeresen felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment stratégiáját.	X	X	X
23.	1.22. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói	1.22. A szervezet azonosítja, rangsorolja és értékeli azokat a beszállítókat, amelyek a szervezet működése szempontjából kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a szervezet alapvető feladatainak ellátásához.	X	X	X
24.	1.23. Folyamatos felügyeleti stratégia	1.23. A szervezet folyamatos felügyeleti stratégiát fejleszt ki és folyamatos felügyeleti programot működtet, amely magában foglalja: 1.23.1. Az egész szervezet számára teljesítménymutatók meghatározását. 1.23.2. A felügyelet és a hatékonyság-értékelés gyakoriságának meghatározását. 1.23.3. A teljesítménymutatók folyamatos, a felügyeleti stratégia szerint történő figyelemmel kísérését. 1.23.4. A felügyelet és az elvégzett értékelések adatai közötti összefüggések és információk elemzését. 1.23.5. A védelmi intézkedések értékelések és felügyeleti információk eredményéből származtatott válaszlépések megtételét. 1.23.6. Az EIR biztonsági állapotáról rendszeres időközönként, a kijelölt személyeknek történő jelentést.	X	X	X

2. Hozzáférés-felügyelet

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	2.1. Szabályzat és eljárásrendek	2.1. A szervezet: 2.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 2.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó hozzáférés-felügyeleti szabályzatot, amely 2.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 2.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 2.1.1.2. A hozzáférés-felügyeleti eljárásrendet, amely a hozzáférés-felügyeleti szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 2.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 2.1.3. Felülvizsgálja és frissíti az aktuális hozzáférés-felügyeleti szabályzatot, a hozzáférés-felügyeleti eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X

3.	2.2. Fiókkezelés	2.2. A szervezet: 2.2.1. Meghatározza és dokumentálja a rendszerben engedélyezett és kifejezetten tiltott fióktípusokat. 2.2.2. Kijelöli a fiókkezelőket. 2.2.3. Kialakítja a csoport- és szerepkör tagsági feltételeket és kritériumokat. 2.2.4. Meghatározza: 2.2.4.1. A rendszerben engedélyezett felhasználókat. 2.2.4.2. A csoport- és szerepkör tagságokat. 2.2.4.3. A hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra. 2.2.5. A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén. 2.2.6. Létrehozza, engedélyezi, módosítja, letiltja és törli a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján. 2.2.7. Nyomon követi a fiókok használatát. 2.2.8. Értesíti a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben: 2.2.8.1. Meghatározott időn belül, amikor a fiókok már nem szükségesek. 2.2.8.2. Meghatározott időn belül, amikor a felhasználók jogviszonya megszűnik 2.2.8.3. Meghatározott időn belül, amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak. 2.2.9. Engedélyezi a rendszerhez való hozzáférést a következők alapján: 2.2.9.1. érvényes hozzáférési engedély; 2.2.9.2. tervezett rendszerhasználat; 2.2.9.3. egyéb, a szervezet által meghatározott jellemzők. 2.2.10. Ellenőrzi a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából, a meghatározott gyakorisággal. 2.2.11. Létrehoz és végrehajt egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére. 2.2.12. Összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszűntetési folyamataival.	X	X	X
4.	2.3. Fiókkezelés – Automatizált fiókkezelés	2.3. A szervezet meghatározott automatizált mechanizmusok segítségével támogatja az EIR fiókjainak kezelését.	-	X	X
5.	2.4. Fiókkezelés – Automatizált ideiglenes és vészhelyzeti fiók kezelés	2.4. Az EIR a meghatározott időtartam letelte után automatikusan eltávolítja vagy letiltja az ideiglenes és vészhelyzeti fiókokat.	-	X	X
6.	2.5. Fiókkezelés – Fiókok letiltása	2.5. Az EIR a meghatározott időtartam letelte után letiltja a fiókokat, vagy amikor a fiókok: 2.5.1. lejártak, 2.5.2. már nem kapcsolódnak felhasználókhoz vagy egyénekhez, 2.5.3. megsértik a szervezeti szabályokat, vagy 2.5.4. meghatározott ideig inaktívak voltak.	-	X	X
7.	2.6. Fiókkezelés – Automatikus naplózási műveletek	2.6. Az EIR automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket.	-	X	X
8.	2.7. Fiókkezelés – Inaktivitásból fakadó kijelentkeztetés	2.7. A szervezet megköveteli a felhasználó kijelentkeztetését egy meghatározott inaktivitási időszak leteltét követően, vagy egy meghatározott időpontban.	-	X	X
9.	2.8. Fiókkezelés – Dinamikus jogosultságkezelés	2.8. A szervezet meghatározott módon alkalmaz dinamikus jogosultságkezelési képességeket.	-	-	-

10.	2.9. Fiókkezelés – Privilegizált fiókok	2.9. A szervezet: 2.9.1. Létrehozza és kezeli a privilegizált fiókokat egy szerepköralapú vagy tulajdonságalapú hozzáférési rendszerrel összhangban. 2.9.2. Felügyeli a privilegizált szerepkörök vagy tulajdonságok hozzárendeléseit. 2.9.3. Felügyeli a szerepkörök vagy tulajdonságok változásait. 2.9.4. Visszavonja a hozzáférést, amikor a privilegizált szerepkörök vagy tulajdonságok hozzárendelése többé már nem releváns.	-	-	-
11.	2.10. Fiókkezelés – Dinamikus fiókkezelés	2.10. A szervezet a meghatározott rendszerfiókok létrehozását, aktiválását, kezelését és letiltását dinamikusan végzi.	-	-	-
12.	2.11. Fiókkezelés – Megosztott és csoportfiókok használati korlátozása	2.11. A szervezet csak meghatározott feltételeknek megfelelő megosztott és csoportfiókok használatát engedélyezi.	-	-	-
13.	2.12. Fiókkezelés – Használati feltételek	2.12. A szervezet kikényszeríti a meghatározott körülmények és a használati feltételek betartását a meghatározott rendszerfiókok esetében.	-	-	X
14.	2.13. Fiókkezelés – Fiókok szokatlan használatának felügyelete	2.13. A szervezet: 2.13.1. Monitorozza az EIR fiókjainak a meghatározott, megszokottól eltérő használatát, és 2.13.2. jelentést készít az EIR fiókjainak megszokottól eltérő használatáról a meghatározott személyeknek vagy szerepköröknek.	-	-	X
15.	2.14. Fiókkezelés – Magas kockázatú személyek fiókjának letiltása	2.14. A szervezet az általa meghatározott jelentős kockázat felfedezésétől számított meghatározott időtartamon belül letiltja az érintett felhasználók fiókjait.	-	X	X
16.	2.15. Hozzáférési szabályok érvényesítése	2.15. Az EIR a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott logikai hozzáférési jogosultságokat az információkhoz és a rendszer erőforrásaihoz.	X	X	X
17.	2.16. Hozzáférési szabályok érvényesítése – Kettős jóváhagyás	2.16. A szervezet kettős jóváhagyást követel meg a meghatározott privilegizált parancsok, vagy a szervezet által meghatározott egyéb műveletek végrehajtása esetében.	-	-	-
18.	2.17. Hozzáférési szabályok érvényesítése – Kötelező hozzáférés-ellenőrzés	2.17. Az EIR az alábbi kötelező és a szervezet által meghatározott hozzáférés-felügyeleti szabályokat érvényesíti: 2.17.1. A szabályzat egységesen érvényes a rendszeren belüli minden alanyra és objektumra. 2.17.2. A hozzáféréssel rendelkező alanyt korlátozza az alábbi tevékenységek végrehajtásában: 2.17.2.1. nem továbbíthatja az információt jogosulatlan alanyoknak vagy objektumoknak; 2.17.2.2. nem adhatja át a jogosultságait más alanyoknak; 2.17.2.3. nem módosíthatja az alanyokon, objektumokon, a rendszeren vagy rendszerelemeken meghatározott biztonsági tulajdonságokat; 2.17.2.4. nem választhatja ki az újonnan létrehozott vagy módosított objektumokhoz rendelt biztonsági tulajdonságokat és tulajdonságértékeket, amelyeket a szabályzat határoz meg; 2.17.2.5. nem módosíthatja a hozzáférés-felügyeleti szabályokat. 2.17.2.5.1. A szabályzat részletesen meghatározza, hogy mely alanyok kaphatnak olyan privilegizált státuszt, amely nem vonatkozik sem a fent említett korlátozások egy részhalmazára, sem az egészre.	-	-	-

19.	2.18. Hozzáférési szabályok érvényesítése – Mérlegelés alapú hozzáférés-felügyelet	2.18. Az EIR érvényesíti a meghatározott mérlegelés alapú hozzáférés-felügyeleti szabályokat a szervezet által meghatározott alanyok és objektumok halmazán, ahol a szabályzat meghatározza, hogy az információhoz való hozzáférést engedélyező alany az alábbiak közül egyet vagy többet megtehet: 2.18.1. Átadhatja az információt más alanyoknak vagy objektumoknak. 2.18.2. Átruházhatja a jogosultságait más alanyoknak. 2.18.3. Módosíthatja az alanyokon, objektumokon, a rendszeren vagy a rendszerelemeken található biztonsági tulajdonságokat. 2.18.4. Kiválaszthatja az újonnan létrehozott vagy módosított objektumokhoz rendelt biztonsági tulajdonságokat. 2.18.5. Módosíthatja a hozzáférés-felügyeleti szabályokat.	-	-	-
20.	2.19. Hozzáférési szabályok érvényesítése – Biztonsággal kapcsolatos információk	2.19. A szervezet megakadályozza a hozzáférést a meghatározott, biztonsági szempontból releváns információkhoz, kivéve, ha a rendszer biztonságos, de nem aktív rendszerállapotban van.	-	-	-
21.	2.20. Hozzáférési szabályok érvényesítése – Szerepkör alapú hozzáférés-ellenőrzés	2.20. A szervezet szerepkör alapú hozzáférési szabályokat alkalmaz a meghatározott alanyokra és objektumokra vonatkozóan. A hozzáféréseket a meghatározott szerepkörök és az ilyen szerepkörök betöltésére jogosult felhasználók alapján szabályozza.	-	-	-
22.	2.21. Hozzáférési szabályok érvényesítése – Hozzáférési engedélyek visszavonása	2.21. A szervezet érvényesíti a hozzáférési jogosultságok visszavonását az alanyok és az objektumok biztonsági tulajdonságainak változása esetén, a szervezet által meghatározott, a hozzáférési jogosultságok visszavonásának időzítésére vonatkozó szabályok alapján.	-	-	-
23.	2.22. Hozzáférési szabályok érvényesítése – Szabályozott továbbítás	2.22. A szervezet csak akkor továbbít információt az EIR-ből, ha: 2.22.1. a meghatározott fogadó rendszer vagy rendszerelem megfelel a szervezet által meghatározott követelményeknek, és 2.22.2. a szervezet által meghatározott követelményeket alkalmazzák a továbbítandó információ megfelelőségének ellenőrzésére.	-	-	-
24.	2.23. Hozzáférési szabályok érvényesítése – Hozzáférés-ellenőrző mechanizmusok ellenőrzött felülbírálata	2.23. A szervezet meghatározott feltételek esetén meghatározott szerepkörök számára biztosítja az automatizált hozzáférés-felügyeleti mechanizmusok ellenőrzött felülbírálatát.	-	-	-
25.	2.24. Hozzáférési szabályok érvényesítése – Meghatározott információtípusokhoz való hozzáférés korlátozása	2.24. A szervezet korlátozza a hozzáférést a meghatározott információtípusokat tartalmazó adattárakhoz.	-	-	-
26.	2.25. Hozzáférési szabályok érvényesítése – Alkalmazás-hozzáférés biztosítása és érvényesítése	2.25. A szervezet: 2.25.1. biztosítja, hogy az alkalmazások a telepítési folyamat részeként hozzáférjenek a meghatározott rendszeralkalmazásokhoz és rendszerfunkciókhoz; 2.25.2. érvényesítési mechanizmust biztosít a jogosulatlan hozzáférés megakadályozására; és 2.25.3. jóváhagyja a hozzáférési jogosultságok változásait az alkalmazás első telepítése után.	-	-	-
27.	2.26. Hozzáférési szabályok érvényesítése – Tulajdonság alapú hozzáférés-ellenőrzés	2.26. A szervezet tulajdonság alapú hozzáférés-felügyeleti szabályokat alkalmaz a meghatározott alanyok és objektumok esetében. A hozzáférési jogosultságokat és engedélyeket a szervezet által meghatározott tulajdonságok alapján szabályozza.	-	-	-

28.	2.27. Hozzáférési szabályok érvényesítése – Kötelező és mérlegelés alapú hozzáférés-felügyelet	2.27. A szervezet érvényesíti 2.27.1. a kötelező hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán; és 2.27.2. a mérlegelés alapú hozzáférés-felügyeleti szabályokat a meghatározott alanyok és objektumok halmazán.	-	-	-
29.	2.28. Információáramlási szabályok érvényesítése	2.28. A szervezet a meghatározott információáramlási szabályokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzése során.	-	X	X
30.	2.29. Információáramlási szabályok érvényesítése – Az objektumok biztonsági tulajdonságai	2.29. A szervezet meghatározott biztonsági tulajdonságokat rendel a meghatározott információkhoz, forrás- és cél objektumokhoz kapcsolódóan, hogy a meghatározott információáramlási szabályokat kikényszerítse az információáramlást érintő döntések során.	-	-	-
31.	2.30. Információáramlási szabályok érvényesítése – Feldolgozási tartományok	2.30. A szervezet védett feldolgozási tartományokat használ a meghatározott információáramlási szabályok érvényesítésére, az információáramlással kapcsolatos döntések megalapozásához.	-	-	-
32.	2.31. Információáramlási szabályok érvényesítése – Az információáramlás dinamikus irányítása	2.31. A szervezet kikényszeríti a meghatározott dinamikus információáramlási szabályokat.	-	-	-
33.	2.32. Információáramlási szabályok érvényesítése – Titkosított információk áramlásának irányítása	2.32. A szervezet az információk dekódolásával, a titkosított információáramlás blokkolásával vagy a titkosított információk átvitelével próbálkozó kommunikációs folyamat megszakításával megakadályozza, hogy titkosított információkkal megkerüljék a meghatározott információáramlás-ellenőrzési mechanizmusokat.	-	-	X
34.	2.33. Információáramlási szabályok érvényesítése – Beágyazott adattípusok	2.33. A szervezet kikényszeríti az adattípusok más adattípusokba való beágyazására vonatkozó meghatározott korlátozásokat.	-	-	-
35.	2.34. Információáramlási szabályok érvényesítése – Metaadat	2.34. A szervezet meghatározott metaadatok alapján érvényesíti az információáramlási szabályokat.	-	-	-
36.	2.35. Információáramlási szabályok érvényesítése – Egyirányú információáramlási mechanizmusok	2.35. A szervezet hardver alapú áramlásszabályozó mechanizmusok segítségével kényszeríti ki az információk egyirányú áramlását.	-	-	-
37.	2.36. Információáramlási szabályok érvényesítése – Biztonsági szűrők	2.36. A szervezet: 2.36.1. Érvényesíti az információáramlás szabályozását a meghatározott biztonsági szűrők alkalmazásával, amelyek alapján döntéseket hoz az áramlásszabályozással kapcsolatban. 2.36.2. Blokkolja, megjelöli, módosítja vagy karanténba helyezi az adatokat, a meghatározott biztonsági szabályok szerint.	-	-	-
38.	2.37. Információáramlási szabályok érvényesítése – Emberi beavatkozással történő felülvizsgálat	2.37. A szervezet meghatározott feltételeket alkalmaz az információáramlás emberi beavatkozással történő felülvizsgálatára.	-	-	-
39.	2.38. Információáramlási szabályok érvényesítése – Biztonsági szűrők engedélyezése és kikapcsolása	2.38. A szervezet lehetővé teszi a jogosultsággal rendelkező adminisztrátorok számára, hogy meghatározott feltételek szerint engedélyezzék vagy kikapcsolják a meghatározott biztonsági szűrőket.	-	-	-
40.	2.39. Információáramlási szabályok érvényesítése – Biztonsági szűrők konfigurálása	2.39. A szervezet lehetővé teszi a kiemelt jogosultsággal rendelkező adminisztrátorok számára, hogy konfigurálják a meghatározott biztonsági szűrőket a különböző biztonsági szabályok támogatása érdekében.	-	-	-
41.	2.40. Információáramlási szabályok érvényesítése – Adattípus azonosítók	2.40. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor meghatározott adattípus azonosítókat használ az információáramlási döntésekhez szükséges adatok validálására.	-	-	-

42.	2.41. Információáramlási szabályok érvényesítése – Adatok alkotóelemeire való bontása	2.41. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor az adatokat a szervezet által meghatározott elemeire bontja le annak érdekében, hogy az adatáramlási szabályokat kikényszerítő mechanizmusok működőképessége biztosított legyen.	-	-	-
43.	2.42. Információáramlási szabályok érvényesítése – Biztonsági szabályzat szűrési korlátozások	2.42. A szervezet az információk különböző biztonsági tartományok közötti átvitelekor érvényesíti a meghatározott biztonsági szabályzat alapján alkalmazott szűrőket, amelyek az adatszerkezetet és a tartalmat korlátozó, meghatározott formátumokat írnak elő.	-	-	-
44.	2.43. Információáramlási szabályok érvényesítése – Nem engedélyezett információk észlelése	2.43. A szervezet megvizsgálja az információt a különböző biztonsági tartományok közötti átvitel során annak érdekében, hogy a nem engedélyezett információ észlelése esetén - a biztonsági szabályok szerint - megtiltsa annak továbbítását.	-	-	-
45.	2.44. Információáramlási szabályok érvényesítése – Tartományhitelesítés	2.44. A szervezet egyedileg azonosítja és hitelesíti a forrás- és célpontokat (szervezetenként, rendszerenként, alkalmazásonként, szolgáltatásonként, egyénekként) az információátvitel során.	-	-	-
46.	2.45. Információáramlási szabályok érvényesítése – Metaadatok ellenőrzése	2.45. A szervezet az információk különböző biztonsági tartományok közötti átvitele során meghatározott biztonsági szűrőket alkalmaz a metaadatokra.	-	-	-
47.	2.46. Információáramlási szabályok érvényesítése – Jóváhagyott megoldások	2.46. A szervezet jóváhagyott konfigurációs megoldásokat alkalmaz az információáramlás ellenőrzésére a biztonsági tartományok között.	-	-	-
48.	2.47. Információáramlási szabályok érvényesítése – Információáramlás fizikai vagy logikai szétválasztása	2.47. A szervezet meghatározott mechanizmusokkal vagy technikákkal fizikailag vagy logikailag szétválasztja az információáramlásokat, hogy a meghatározott információtípusok szerinti elkülönítést megvalósítsa.	-	-	-
49.	2.48. Információáramlási szabályok érvényesítése – Hozzáférés korlátozása	2.48. Amikor az EIR egyetlen készülékről több különböző biztonsági tartományban található informatikai platformhoz, alkalmazáshoz vagy adathoz biztosít hozzáférést, megakadályozza az információáramlást a különböző biztonsági tartományok között.	-	-	-
50.	2.49. Információáramlási szabályok érvényesítése – Nem nyilvános információ módosítása	2.49. A szervezet a meghatározott eljárásokat alkalmazva módosítja a nem nyilvános információkat a különböző biztonsági tartományok közötti átvitel során.	-	-	-
51.	2.50. Információáramlási szabályok érvényesítése – Belső normalizált formátum	2.50. Az EIR a különböző biztonsági tartományok közötti információátvitel során a beérkező adatokat normalizált formátumba hozza, majd újra formázza, hogy azok összhangban legyenek az elvárt adatformátummal.	-	-	-
52.	2.51. Információáramlási szabályok érvényesítése – Adattisztítás	2.51. Amikor az EIR információt továbbít különböző biztonsági tartományok között, az adatokat a meghatározott szabályoknak megfelelően megtisztítja, hogy minimalizálja a rosszindulatú tartalom átvitelét.	-	-	-
53.	2.52. Információáramlási szabályok érvényesítése – Szűrési műveletek ellenőrzése	2.52. A szervezet rögzíti és ellenőrzi a tartalomszűrési műveleteket és azok eredményeit a szűrt információra vonatkozóan, a biztonsági tartományok között történő információátvitel során.	-	-	-
54.	2.53. Információáramlási szabályok érvényesítése – Redundáns szűrőmechanizmusok	2.53. A szervezet olyan tartalomszűrési megoldásokat alkalmaz a különböző biztonsági tartományok között történő információk átvitele során, amelyek redundáns és független szűrőmechanizmusokat biztosítanak minden adattípusra.	-	-	-
55.	2.54. Információáramlási szabályok érvényesítése – Lineáris szűrőcsatornák	2.54. A szervezet olyan lineáris tartalomszűrési folyamatot hajt végre a különböző biztonsági tartományok között történő információk átvitele során, amelyeket szabadon választható és kötelező hozzáférési szabályokkal kényszerít ki.	-	-	-

56.	2.55. Információáramlási szabályok érvényesítése – Összehangolt tartalomszűrés	2.55. A szervezet tartalomszűrő rendszert alkalmaz az információk különböző biztonsági tartományok közötti átvitelekor annak biztosítása érdekében, hogy: 2.55.1. a tartalomszűrő mechanizmusok hiba nélkül sikeresen végrehajthassák a feladatukat; 2.55.2. a tartalomszűrési műveletek megfelelő sorrendben történjenek, és megfeleljenek a meghatározott biztonsági szabályzati előírásainak.	-	-	-
57.	2.56. Információáramlási szabályok érvényesítése – Több folyamatot használó szűrőmechanizmusok	2.56. A szervezet a különböző biztonsági tartományok közötti információátvitel során több folyamatot használó tartalomszűrési mechanizmust valósít meg.	-	-	-
58.	2.57. Információáramlási szabályok érvényesítése – Hibás tartalom átvitelének megakadályozása	2.57. A szervezet a különböző biztonsági tartományok közötti információátvitel során megakadályozza a hibásan átadott tartalom átvitelét a fogadó tartományba.	-	-	-
59.	2.58. Információáramlási szabályok érvényesítése – Folyamatkövetelmények az információ átviteléhez	2.58. A különböző biztonsági tartományok közötti információátvitel során a szűrőcsatornák közötti információátviteli folyamat: 2.58.1. nem szűri az üzenetek tartalmát; 2.58.2. ellenőrzi és jóváhagyja a szűrési metaadatokat; 2.58.3. biztosítja, hogy a szűrési metaadatokhoz társított tartalom sikeresen átment a szűrésen; és 2.58.4. átadja a tartalmat a cél szűrőcsatornának.	-	-	-
60.	2.59. Felelősségek szétválasztása	2.59. A szervezet: 2.59.1. azonosítja és dokumentálja azokat a meghatározott feladatokat, amelyeket az egyéneknek elkülönített módon kell ellátniuk; és 2.59.2. meghatározza az EIR hozzáférési jogosultságait annak érdekében, hogy támogassa a feladatok szétválasztását.	-	X	X
61.	2.60. Legkisebb jogosultság elve	2.60. A szervezet a legkisebb jogosultság elvét alkalmazza, és a felhasználók vagy a felhasználók nevében eljáró folyamatok számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.	-	X	X
62.	2.61. Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz	2.61. A szervezet: 2.61.1. Kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonsági funkciókhoz. 2.61.2. A szervezett kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonságkritikus információkhoz.	-	X	X
63.	2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz	2.62. A szervezet megköveteli, hogy a meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező fiókok felhasználói a nem biztonsági funkciók használatához ne privilegizált fiókot vagy szerepkört használjanak.	-	X	X
64.	2.63. Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz	2.63. A szervezet csak kényszerű üzemeltetési okokból engedélyezi a hálózati hozzáférést a meghatározott privilegizált parancsokhoz, és dokumentálja az ilyen hozzáférés indoklását a rendszerbiztonsági tervében.	-	-	X
65.	2.64. Legkisebb jogosultság elve – Elkülönített feldolgozási tartományok	2.64. A szervezet elkülönített feldolgozási tartományokat biztosít a felhasználói jogosultságok pontosabb kiosztásának lehetővé tétele érdekében.	-	-	-
66.	2.65. Legkisebb jogosultság elve – Privilegizált fiókok	2.65. A szervezet az EIR privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.	-	X	X
67.	2.66. Legkisebb jogosultság elve – Privilegizált hozzáférés szervezeten kívüli felhasználók számára	2.66. A szervezet megtiltja a szervezeten kívüli felhasználók számára az EIR-hez való privilegizált hozzáférést.	-	-	-

68.	2.67. Legkisebb jogosultság elve – Felhasználói jogosultságok felülvizsgálata	2.67. A szervezet: 2.67.1. Meghatározott időközönként felülvizsgálja a szerepkörök vagy felhasználói csoportok által hozzáférhető jogosultságokat annak érdekében, hogy ellenőrizze a jogosultságok szükségességét. 2.67.2. Amennyiben szükséges, elvégzi a jogosultságok újra osztását vagy megszüntetését, hogy azok megfelelően tükrözzék a szervezet céljait és az üzleti igényeket.	-	X	X
69.	2.68. Legkisebb jogosultság elve – Jogosultsági szintek kódvégrehajtáshoz	2.68. A szervezet megakadályozza, hogy az általa meghatározott szoftverek magasabb jogosultsági szinteken fussanak, mint a szoftvert futtató felhasználók jogosultsági szintje.	-	-	-
70.	2.69. Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása	2.69. Az EIR naplózza a privilegizált funkciók végrehajtását.	-	X	X
71.	2.70. Legkisebb jogosultság elve – Nem-privilegizált felhasználók korlátozása	2.70. Az EIR megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre.	-	X	X
72.	2.71. Sikertelen bejelentkezési kísérletek	2.71. A szervezet: 2.71.1. Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. 2.71.2. EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.	X	X	X
73.	2.72. Sikertelen bejelentkezési kísérletek – Mobil eszköz törlése vagy alaphelyzetbe állítása	2.72. Előzetesen meghatározott számú egymást követő sikertelen bejelentkezési kísérletet követően a szervezet törli vagy alaphelyzetbe állítja a szervezet által meghatározott mobileszközökről származó információt, a meghatározott adattörlési és adattisztítási követelményeknek és technikáknak megfelelően.	-	-	-
74.	2.73. Sikertelen bejelentkezési kísérletek – Biometrikus bejelentkezési kísérletek korlátozása	2.73. A szervezet korlátozza a sikertelen biometrikus bejelentkezési kísérletek számát.	-	-	-
75.	2.74. Sikertelen bejelentkezési kísérletek – Alternatív hitelesítési faktor használata	2.74. A szervezet: 2.74.1. Meghatározott számú, egymást követő sikertelen bejelentkezési kísérletet követően engedélyezi az elsődleges hitelesítési faktortól eltérő, meghatározott hitelesítési faktor használatát; 2.74.2. EIR-je meghatározott ideig korlátozza az alternatív faktor használatával végrehajtott egymást követő érvénytelen bejelentkezési kísérletek számát.	-	-	-

76.	2.75. A rendszerhasználat jelzése	2.75.1. Az EIR a rendszer használata előtt megjelenít a felhasználóknak egy meghatározott rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és tartalmazza, hogy: 2.75.1.1. A felhasználók a szervezet EIR-ét használják. 2.75.1.2. A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják. 2.75.1.3. A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár. 2.75.1.4. A rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti. 2.75.2. Az EIR mindaddig fenntartja a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre vagy a rendszerhez való további hozzáférésre. 2.75.3. Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza: 2.75.3.1. A felhasználók a szervezet EIR-ét használják. 2.75.3.2. A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják. 2.75.3.3. A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.	X	X	X
77.	2.76. Legutóbbi bejelentkezési értesítés	2.76. Az EIR a sikeres bejelentkezést követően értesíti a felhasználót a legutóbbi bejelentkezés időpontjáról.	-	-	-
78.	2.77. Korábbi bejelentkezések jelzése – Sikertelen bejelentkezések	2.77. Az EIR a sikeres bejelentkezést követően értesíti a felhasználót az utolsó sikeres bejelentkezés óta történt sikertelen bejelentkezési kísérletek számáról.	-	-	-
79.	2.78. Korábbi bejelentkezések jelzése – Sikeres és sikertelen bejelentkezések	2.78. Az EIR a sikeres bejelentkezést követően tájékoztatja a felhasználót a sikeres bejelentkezések és a sikertelen bejelentkezési kísérletek számáról a meghatározott időszakra vonatkozóan.	-	-	-
80.	2.79. Korábbi bejelentkezések jelzése – Értesítés a fiókváltozásokról	2.79. A rendszer a sikeres bejelentkezést követően értesíti a felhasználót a meghatározott időszak alatt a felhasználói fiók biztonsággal kapcsolatos jellemzőinek vagy beállításainak változásairól.	-	-	-
81.	2.80. Korábbi bejelentkezések jelzése – Kiegészítő bejelentkezési információk	2.80. Az EIR a sikeres bejelentkezést követően a szervezet által meghatározott további információkat közöl a felhasználónak.	-	-	-
82.	2.81. Egyidejű munkaszakasz kezelés	2.81. A szervezet az EIR-ben meghatározott számra korlátozza az egyidejű munkaszakaszok számát minden egyes meghatározott fiókra vagy fióktípusra vonatkozóan.	-	-	X
83.	2.82. Eszköz zárolása	2.82. A szervezet: 2.82.1. Meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén, az eszköz zárolásával megakadályozza az EIR-hez való további hozzáférést. 2.82.2. Fenntartja az eszköz zárolását mindaddig, amíg a felhasználó a megfelelő azonosítási és hitelesítési eljárásokat el nem végzi.	-	X	X
84.	2.83. Eszköz zárolása – Képernyőtakarás	2.83. A szervezet az eszköz zárolása során elrejti a kijelzőn lévő információkat.	-	X	X
85.	2.84. A munkaszakasz lezárása	2.84. Az EIR automatikusan lezárja a munkaszakaszt a szervezet által meghatározott feltételek, vagy a munkaszakasz megszakítását igénylő események után.	-	X	X
86.	2.85. Munkaszakasz megszakítása – Felhasználó által kezdeményezett kijelentkezések	2.85. Az EIR biztosítja a kijelentkezési lehetőséget a felhasználó által kezdeményezett kommunikációs munkaszakaszból, ha az ahhoz történő hozzáférés hitelesítést igényel.	-	-	-
87.	2.86. Munkaszakasz megszakítása – Megszakítási üzenet	2.86. Az EIR egyértelmű kijelentkezési üzenetet jelenít meg a felhasználók számára, amely jelzi a hitelesített kommunikációs munkaszakaszok befejezését.	-	-	-

88.	2.87. Munkaszakasz megszakítása – Időkorlátozásra figyelmeztető üzenet	2.87. Az EIR egyértelmű üzenetet jelenít meg a felhasználók számára, amely jelzi, hogy a munkaszakasz a meghatározott idő leteltét követően véget ér.	-	-	-
89.	2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	2.88. A szervezet: 2.88.1. Azonosítja azon felhasználói tevékenységeket, amelyek - a szervezeti célokkal és üzleti funkciókkal összhangban - az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatók. 2.88.2. A rendszerbiztonsági tervben dokumentálja és megindokolja azokat a felhasználói tevékenységeket, amelyek azonosítás vagy hitelesítés nélkül is végrehajthatók.	X	X	X
90.	2.89. Biztonsági tulajdonságok	2.89. A szervezet: 2.89.1. Lehetővé teszi biztonsági tulajdonságértékek hozzárendelését a tárolt, feldolgozott vagy továbbított információkhoz. 2.89.2. Gondoskodik arról, hogy a tulajdonságtársítások létrejöhessenek és fennmaradhassanak az információval együtt. 2.89.3. Meghatározza azokat a biztonsági tulajdonságokat, amelyek engedélyezettek a meghatározott EIR-ek számára. 2.89.4. Meghatározza a megengedett tulajdonságértékeket vagy tulajdonságérték tartományokat a meghatározott tulajdonságokhoz. 2.89.5. Naplózza a tulajdonságok változásait. 2.89.6. Meghatározott időközönként felülvizsgálja a meghatározott biztonsági tulajdonságokat.	-	-	-
91.	2.90. Biztonsági tulajdonságok – Dinamikus tulajdonságtársítás	2.90. A szervezet dinamikusan társítja a biztonsági tulajdonságokat a meghatározott alanyokhoz és objektumokhoz, a meghatározott információbiztonsági előírásoknak megfelelően, az információk létrehozásakor és összeállításakor.	-	-	-
92.	2.91. Biztonsági tulajdonságok – Tulajdonságértékek jogosult személyek általi módosítása	2.91. A szervezet lehetőséget biztosít a jogosult személyeknek vagy a nevükben eljáró folyamatoknak, a kapcsolódó biztonsági tulajdonságértékek meghatározására vagy megváltoztatására.	-	-	-
93.	2.92. Biztonsági tulajdonságok – Tulajdonságtársítások rendszerenkénti karbantartása	2.92. A szervezet fenntartja a meghatározott biztonsági tulajdonságok sértetlenségét és hozzárendelését a meghatározott alanyokhoz és objektumokhoz.	-	-	-
94.	2.93. Biztonsági tulajdonságok – Tulajdonságok jogosult személyek által történő társítása	2.93. A szervezet lehetővé teszi a jogosult személyeknek vagy a nevükben eljáró folyamatoknak, a meghatározott biztonsági tulajdonságok és a meghatározott alanyok és objektumok társítását.	-	-	-
95.	2.94. Biztonsági tulajdonságok – Tulajdonságok megjelenítése a kimeneti objektumokon	2.94. A szervezet biztosítja, hogy az EIR az ember által olvasható formában jeleníti meg a biztonsági tulajdonságokat minden olyan objektumra vonatkozóan, amelyet az EIR a kimeneti eszközök felé továbbít, hogy azokon a meghatározott speciális terjesztési, kezelési vagy elosztási utasítások egyértelműen azonosíthatók legyenek.	-	-	-
96.	2.95. Biztonsági tulajdonságok – Tulajdonságtársítás karbantartása	2.95. A szervezet arra kötelezi a személyzetet, hogy a meghatározott biztonsági szabályokkal összhangban rendelje hozzá és tartsa fenn a meghatározott biztonsági tulajdonságokat, valamint az alanyok és objektumok meghatározott összekapcsolását.	-	-	-
97.	2.96. Biztonsági tulajdonságok – Következetes tulajdonságértelmezés	2.96. A szervezet biztosítja az elosztott rendszerelemek között továbbított biztonsági tulajdonságok következetes értelmezését.	-	-	-
98.	2.97. Biztonsági tulajdonságok – Tulajdonságtársítási technikák és technológiák	2.97. A szervezet meghatározott technikákat és technológiákat alkalmaz a biztonsági tulajdonságok információkkal való társítása során.	-	-	-
99.	2.98. Biztonsági tulajdonságok – Tulajdonságok átcsoportosítása - Átminősítési mechanizmusok	2.98. A szervezet csak meghatározott technikák vagy eljárások segítségével, hitelesített besorolás módosítási mechanizmusok alkalmazásával változtatja meg az információkhoz kapcsolódó biztonsági tulajdonságokat.	-	-	-

100.	2.99. Biztonsági tulajdonságok – A tulajdonságok konfigurálása felhatalmazott személyek által	2.99. A szervezet lehetőséget biztosít a jogosult személyek számára, hogy megváltoztassák az alanyokhoz és objektumokhoz társítható biztonsági tulajdonságok típusát és értékét.	-	-	-
101.	2.100. Távoli hozzáférés	2.100. A szervezet: 2.100.1. Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat. 2.100.2. Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően	X	X	X
102.	2.101. Távoli hozzáférés – Felügyelet és irányítás	2.101. A szervezet automatizált mechanizmusokat alkalmaz a távoli hozzáférési módok felügyeletére és ellenőrzésére.	-	X	X
103.	2.102. Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által	2.102. A szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében.	-	X	X
104.	2.103. Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok	2.103. A szervezet a távoli hozzáféréseket engedélyezett és menedzselt hálózati hozzáférés-felügyeleti pontokon keresztül irányítja.	-	X	X
105.	2.104. Távoli hozzáférés – Privilegizált parancsok és hozzáférés	2.104. A szervezet: 2.104.1. Csak olyan módon engedélyezi a távoli hozzáférést, amely értékelhető bizonyítékot szolgáltat a privilegizált jogosultságot igénylő műveletek végrehajtásához és a biztonságkritikus információk eléréséhez a meghatározott követelményeknek megfelelően, és 2.104.2. a távoli hozzáférés indokoltságát a rendszerbiztonsági tervben dokumentálja.	-	X	X
106.	2.105. Távoli hozzáférés – Hozzáférési mechanizmusra vonatkozó információk védelme	2.105. Az EIR védi a távoli hozzáférési mechanizmusokra vonatkozó információkat a jogosulatlan felhasználástól és nyilvánosságra hozataltól.	-	-	-
107.	2.106. Távoli hozzáférés – Hozzáférés megszakítása vagy letiltása	2.106. A szervezet biztosítja a rendszerhez való távoli hozzáférés meghatározott időn belüli szétkapcsolásának vagy letiltásának a lehetőségét.	-	-	-
108.	2.107. Távoli hozzáférés – Távoli parancsok hitelesítése	2.107. A szervezet meghatározott mechanizmusokat vezet be a meghatározott parancsok hitelesítésére.	-	-	-
109.	2.108. Vezeték nélküli hozzáférés	2.108. A szervezet: 2.108.1. A vezeték nélküli hozzáférés minden egyes típusára vonatkozóan konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatást alakít ki. 2.108.2. Engedélyezési eljárást folytat le a rendszerhez való vezeték nélküli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően	X	X	X
110.	2.109. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás	2.109. A szervezet az EIR-ben titkosítással és a felhasználók vagy az eszközök hitelesítésével védi a vezeték nélküli hozzáférést.	-	X	X
111.	2.110. Vezeték nélküli hozzáférés – Vezeték nélküli hálózat letiltása	2.110. A szervezet a rendszerelemekbe ágyazott vezeték nélküli hálózati hozzáférést letiltja amennyiben annak használata nem szükséges.	-	X	X
112.	2.111. Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása	2.111. A szervezet azonosítja és külön engedélyezési eljáráson keresztül jogosítja fel azokat a felhasználókat, akik jogosultak a vezeték nélküli hálózati funkciók önálló konfigurálására.	-	-	X
113.	2.112. Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény	2.112. A szervezet olyan rádióantennákat választ ki és az átviteli teljesítményszinteket oly módon kalibrálja, hogy minimalizálja annak valószínűségét, hogy a vezeték nélküli hozzáférési pontok jelei a szervezet által ellenőrzött határokon túl is foghatók legyenek.	-	-	X

114.	2.113. Mobil eszközök hozzáférés-ellenőrzése	2.113. A szervezet: 2.113.1. Kialakítja a konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatót az általa ellenőrzött mobil eszközök számára, beleértve azokat az eseteket is, amikor ezek az eszközök a szervezet által ellenőrzött területen kívül helyezkednek el. 2.113.2. Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást.	X	X	X
115.	2.114. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás	2.114. A szervezet teljes eszköztitkosítást vagy tárolóalapú titkosítást alkalmaz a meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének védelme érdekében.	-	X	X
116.	2.115. Külső elektronikus információs rendszerek használata	2.115. A szervezet: 2.115.1. Meghatározza a felhasználási feltételeket, és megállapítja, hogy az elvárt követelmények megvalósultak-e a külső rendszerekben, összhangban a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel létrehozott bizalmi kapcsolatokkal, amelyek lehetővé teszik az arra jogosult személyek számára, hogy: 2.115.1.1. hozzáférjenek a rendszerhez külső rendszerekből; és 2.115.1.2. feldolgozzák, tárolják vagy továbbítsák a szervezet által ellenőrzött információkat külső rendszerek használatával; vagy 2.115.2. megtiltja a meghatározott típusú külső rendszerek használatát.	X	X	X
117.	2.116. Külső rendszerek használata – Engedélyezett használat korlátozásai	2.116. A szervezet csak akkor engedélyezi a jogosult személyek számára a külső rendszer használatát, a rendszerhez való hozzáférést, illetve a szervezet által ellenőrzött információk feldolgozását, tárolását vagy továbbítását, ha: 2.116.1. ellenőrzésre került a külső rendszeren alkalmazott védelmi intézkedések végrehajtása, amelyeket a szervezet biztonsági szabályzatai és tervei határoznak meg; vagy 2.116.2. betartja és betartatja a jóváhagyott rendszerkapcsolati vagy feldolgozási megállapodásokat a külső rendszert üzemeltető szervezettel.	-	X	X
118.	2.117. Külső rendszerek használata – Hordozható adattárolók használatának korlátozása	2.117. A szervezet a meghatározott feltételek szerint korlátozza a jogosult személyek által külső rendszerekben használt, szervezet által ellenőrzött hordozható adattároló eszközök használatát.	-	X	X
119.	2.118. Külső rendszerek használata – A nem szervezeti tulajdonban lévő rendszerek használatának korlátozása	2.118. A szervezet a meghatározott feltételek szerint korlátozza a nem szervezeti tulajdonban lévő rendszerek és rendszerelemek használatát a szervezeti információk feldolgozására, tárolására vagy továbbítására.	-	-	-
120.	2.119. Külső rendszerek használata – Hálózati adattárolók használatának tiltása	2.119. A szervezet megtiltja a meghatározott hálózati adattároló eszközök használatát külső rendszerekben.	-	-	-
121.	2.120. Külső rendszerek használata – Hordozható adattárolók használatának tiltása	2.120. A szervezet megtiltja a szervezet által felügyelt hordozható adattároló eszközöknek a jogosult személyek által külső rendszerekben történő használatát.	-	-	-
122.	2.121. Információmegosztás	2.121. A szervezet: 2.121.1. Elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói mérlegelés szóba jöhet; 2.121.2. Automatizált mechanizmusokat vagy manuális eljárásokat alkalmaz arra, hogy segítsen a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.	-	X	X

123.	2.122. Információmegosztás – Automatizált döntéstámogatás	2.122. A szervezet automatizált mechanizmusokat alkalmaz az információmegosztási döntések érvényesítésére, amelyeket a jogosult felhasználók hajtanak végre, figyelembe véve a megosztásban érintett partnerek hozzáférési jogosultságait és az információhoz való hozzáférés korlátozásait.	-	-	-
124.	2.123. Információmegosztás – Információkeresés és visszakeresés	2.123. A szervezet olyan információkeresési és lekérdezési szolgáltatásokat alkalmaz, amelyek érvényesítik a meghatározott információmegosztási korlátozásokat.	-	-	-
125.	2.124. Nyilvánosan elérhető tartalom	2.124. A szervezet: 2.124.1. Kijelöli azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé. 2.124.2. Képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat. 2.124.3. Áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy nem tartalmaznak nem nyilvános információkat. 2.124.4. Meghatározott gyakorisággal áttekinti a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából, és eltávolítja az ilyen információkat, ha felfedezik őket.	X	X	X
126.	2.125. Adatbányászat elleni védelem	2.125. A szervezet a meghatározott adattárakon alkalmazza a meghatározott adatbányászatot megelőző és észlelő technikákat, hogy észlelje és védekezzen az engedély nélküli adatbányászat ellen.	-	-	-
127.	2.126. Hozzáférés-ellenőrzésre vonatkozó döntések	2.126. A szervezet eljárásokat alakít ki, illetve mechanizmusokat valósít meg annak érdekében, hogy a meghatározott hozzáférés-felügyeleti szabályok minden hozzáférési kérelem esetén alkalmazásra kerüljenek a hozzáférés engedélyezését megelőzően.	-	-	-
128.	2.127. Hozzáférés-ellenőrzési döntések – Hozzáférési engedélyek továbbítása	2.127. A szervezet a meghatározott hozzáférés-engedélyezési információkat a meghatározott követelmények szerint továbbítja azokba a rendszerekbe, amelyek a hozzáférés-felügyeleti döntéseket végrehajtják.	-	-	-
129.	2.128. Felhasználó- vagy a folyamatazonosító ismerete nélküli hozzáférés-ellenőrzési döntések.	2.128. A szervezet a hozzáférés-felügyeleti döntéseket olyan meghatározott biztonsági tulajdonságok alapján hajtja végre, amelyek nem tartalmazzák a felhasználó vagy a felhasználó nevében eljáró folyamat azonosítóját.	-	-	-
130.	2.129. Referenciának való megfelelőség vizsgálata	2.129. A szervezet a meghatározott hozzáférés-felügyeleti szabályzat ellenőrzésére olyan megfelelőségellenőrző megoldást valósít meg, amely manipulációbiztos, folyamatba épített és a teljes körű elemzés és tesztelés elvégzéséhez alkalmas terjedelmű.	-	-	-

3. Tudatosság és képzés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	3.1. Szabályzat és eljárásrendek	3.1. A szervezet: 3.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 3.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó tudatossági és képzési szabályzatot, amely 3.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 3.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 3.1.1.2. a tudatossági és képzési eljárásrendet, amely a tudatossági és képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 3.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a tudatossági és képzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 3.1.3. Felülvizsgálja és frissíti az aktuális tudatossági és képzési szabályzatot és a tudatossági és képzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	3.2. Biztonságtudatossági képzés	3.2. A szervezet: 3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is): 3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal. 3.2.1.2. Amennyiben az EIR-ben bekövetkezett változások ezt indokolttá teszik, vagy a szervezet által meghatározott események ezt megkövetelik. 3.2.2. Meghatározza azokat a technikákat, melyeket a rendszerfelhasználók biztonságtudatosságának növelése érdekében alkalmaz. 3.2.3. Frissíti a képzési és tudatossági tananyagot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően. 3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe.	X	X	X
4.	3.3. Biztonságtudatossági képzés – Gyakorlati feladatok	3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.	-	-	-
5.	3.4. Biztonságtudatossági képzés – Belső fenyegetés	3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.	X	X	X
6.	3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére.	-	X	X
7.	3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés	3.6. A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére.	-	-	-

8.	3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések	3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.	-	-	-
9.	3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet	3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről és 3.8.2. alkalmazza az aktuális kiberbiztonsági fenyegetési információkat a rendszerüzemeltetésben.	-	-	-
10.	3.9. Szerepkör alapú biztonsági képzés	3.9. A szervezet: 3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak: 3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel. 3.9.1.2. Amikor az EIR-ben bekövetkezett változás azt szükségessé teszi. 3.9.2. Frissíti a szerepköralapú képzés tartalmát a szervezet által meghatározott rendszerességgel és a szervezet által meghatározott események bekövetkezését követően. 3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe.	X	X	X
11.	3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések	3.10. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.	-	-	-
12.	3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések	3.11. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.	-	-	-
13.	3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok	3.12. A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.	-	-	-
14.	3.13. A biztonsági képzésre vonatkozó dokumentációk	3.13. A szervezet: 3.13.1. Dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket, ideértve az általános információbiztonsági tudatossági képzéseket és a speciális szerepkör alapú információbiztonsági képzéseket. 3.13.2. Meghatározott ideig megőrzi a képzésről készült dokumentumokat.	X	X	X
15.	3.14. Képzés eredményeiről való visszajelzés	3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.	-	-	-

4. Naplózás és elszámoltathatóság

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	4.1. Szabályzat és eljárásrendek	4.1. A szervezet: 4.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 4.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó naplózásra és elszámoltathatóságra vonatkozó szabályzatot, amely 4.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 4.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 4.1.1.2. a naplózási és elszámoltathatósági eljárásrendet, amely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 4.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 4.1.3. Felülvizsgálja és frissíti az aktuális naplózásra és elszámoltathatóságra vonatkozó szabályzatot és a naplózási és elszámoltathatósági eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	4.2. Naplózható események	4.2. A szervezet: 4.2.1. Meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az EIR-t. 4.2.2. Egyezteti a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy iránymutatással és információkkal segítse a naplózandó események kiválasztását. 4.2.3. Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket. 4.2.4. Indokolja, hogy a kiválasztott eseménytípusok, miért alkalmasak a biztonsági események utólagos kivizsgálásának támogatására; 4.2.5. Meghatározott gyakorisággal felülvizsgálja és frissíti a naplózásra kiválasztott eseménytípusokat.	X	X	X
4.	4.3. Naplóbejegyzések tartalma	4.3. A szervezet biztosítja, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek: 4.3.1. milyen típusú esemény történt; 4.3.2. mikor történt az esemény; 4.3.3. hol történt az esemény; 4.3.4. miből származott az esemény; és 4.3.5. mi volt az eseménynek a kimenetele, valamint 4.3.6. az eseményhez kapcsolódó személyek, alanyok, objektumok.	X	X	X
5.	4.4. Naplóbejegyzések tartalma – Kiegészítő naplóinformációk	4.4. Az EIR a naplóbejegyzésekben további, a szervezet által meghatározott kiegészítő információkat is rögzít.	-	X	X

6.	4.5. Naplózás tárkapacitása	4.5. A szervezet elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket.	X	X	X
7.	4.6. Napló tárkapacitás – Naplók átvitele alternatív tárolási helyszínre	4.6. A szervezet meghatározott gyakorisággal továbbítja a naplóbejegyzéseket a forrásrendszerből vagy rendszerelemből egy különálló rendszerbe, rendszerelembe vagy tárolórendszerbe.	-	-	-
8.	4.7. Naplózási hiba kezelése	4.7. A szervezet naplózási hiba esetén: 4.7.1. Riasztja a meghatározott személyeket vagy szerepköröket a szervezet által meghatározott időn belül. 4.7.2. További meghatározott intézkedéseket hajt végre.	X	X	X
9.	4.8. Naplózási hiba kezelése – Tárhelykapacitás figyelmeztetés	4.8. Az EIR a szervezet által meghatározott időn belül figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a maximális naplózási tárhely szervezet által meghatározott százalékos értékét.	-	-	X
10.	4.9. Naplózási hiba kezelése – Valós idejű riasztások	4.9. Az EIR riasztást küld a meghatározott személyeknek vagy szerepköröknek, ha a meghatározott, valós idejű riasztást igénylő hibaesemények közül bármelyik bekövetkezik.	-	-	X
11.	4.10. Naplózási hiba kezelése – Konfigurálható forgalmi küszöbértékek	4.10. A szervezet olyan konfigurálható hálózati kommunikációs forgalmi küszöbértéket alkalmaz, amely megfelel a naplózás tárolási kapacitási korlátjainak és a küszöbérték feletti forgalmat visszautasítja vagy késlelteti.	-	-	-
12.	4.11. Naplózási hiba kezelése – Leállítás hiba esetén	4.11. A szervezet meghatározott naplózási hibák esetén kezdeményezi az EIR teljes vagy részleges leállítását, vagy korlátozza az elérhető ügymeneti és üzleti funkciókat, kivéve, ha a szervezet rendelkezik alternatív naplózási képességgel.	-	-	-
13.	4.12. Naplózási hiba kezelése – Alternatív naplózási képesség	4.12. Az EIR alternatív naplózási funkciót biztosít arra az esetre, ha az elsődleges naplózási funkció meghibásodik.	-	-	-
14.	4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	4.13. A szervezet: 4.13.1. Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából. 4.13.2. Jelenti ezeket a szervezet által meghatározott személyeknek vagy szerepköröknek. 4.13.3. Módosítja a naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének szintjét, amennyiben hiteles információk és információforrások alapján a kockázat változik.	X	X	X
15.	4.14. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Automatizált folyamatintegráció	4.14. A szervezet automatizált mechanizmusokat használ a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.	-	X	X
16.	4.15. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Naplózási tárhelyek összekapcsolása	4.15. A szervezet elemzi és összekapcsolja a különböző tárhelyeken található naplóbejegyzéseket a teljes szervezetre kiterjedő helyzetfelismerés érdekében.	-	X	X
17.	4.16. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Központi vizsgálat és elemzés	4.16. Az EIR biztosítja a több rendszerelemből származó naplóbejegyzések központi felülvizsgálatát és elemzését.	-	-	-
18.	4.17. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Felügyeleti képességek integrálása	4.17. A szervezet egyesíti a naplók elemzését a sérülékenységmenedzsment során keletkezett információkkal, a teljesítményadatokkal, a rendszerfelügyeleti információkkal vagy egyéb forrásokból begyűjtött információkkal a nem megfelelő vagy szokatlan tevékenységek azonosításának javítása érdekében.	-	-	X
19.	4.18. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Összevetés a fizikai felügyelettel	4.18. A szervezet összeveti a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert adatokkal, a szokatlan, nem odaillő, gyanús vagy rosszindulatú tevékenységek azonosítására vonatkozó képességek fejlesztése érdekében.	-	-	X

20.	4.19. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Engedélyezett műveletek	4.19. A szervezet meghatározza az engedélyezett tevékenységeket minden olyan rendszerfolyamathoz, szerepkörhöz vagy felhasználóhoz, amely a naplóbejegyzések felülvizsgálatával, elemzésével és jelentésekkel kapcsolatos.	-	-	-
21.	4.20. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Privilegizált parancsok teljes szöveges elemzése	4.20. A szervezet elvégzi a naplózott privilegizált parancsok teljes szöveges elemzését a rendszer egy fizikailag és funkcionálisan elkülönített elemében vagy alrendszerében, vagy más, kifejezetten erre az elemzésre szolgáló rendszerben.	-	-	-
22.	4.21. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Összevetés a nem technológiai forrásokból származó információkkal	4.21. A szervezet összeveti a naplóbejegyzésekből származó információkat a nem technológiai forrásokból származó információkkal, a teljes szervezetre kiterjedő helyzetfelismerés javítása érdekében.	-	-	-
23.	4.22. Naplóbejegyzések csökkentése és jelentéskészítés	4.22. A szervezet lehetőséget biztosít naplóbejegyzések csökkentésre és jelentéskészítésre: 4.22.1. amely támogatja az igény esetén végzendő naplófelülvizsgálati, naplóelemzési és jelentéstételi követelményeket, valamint a biztonsági eseményeket követő tényfeltáró vizsgálatokat; 4.22.2. amely nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.	-	X	X
24.	4.23. Naplóbejegyzések csökkentése és jelentéskészítés – Automatikus feldolgozás	4.23. A szervezet gondoskodik arról, hogy a naplóbejegyzések automatikusan feldolgozhatók, rendezhetők és kereshetők legyenek a meghatározott adatmezők tekintetében.	-	X	X
25.	4.24. Időbélyegek	4.24. A szervezet: 4.24.1. Belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. 4.24.2. Időbélyegeket rögzít a naplóbejegyzésekben, amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást.	X	X	X
26.	4.25. Naplóinformációk védelme	4.25. Az EIR: 4.25.1. Megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. 4.25.2. Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor értesíti a meghatározott személyeket vagy szerepköröket.	X	X	X
27.	4.26. A naplóinformációk védelme – Egyszer írható adathordozó	4.26. Az EIR a naplóbejegyzéseket egy hardveresen kikényszerített, egyszer írható adathordozóra rögzíti.	-	-	-
28.	4.27. A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken	4.27. Az EIR a naplóbejegyzéseket meghatározott gyakorisággal eltárolja egy olyan tárhelyen, amely a keletkezési helyétől fizikailag elkülönült rendszer vagy rendszerelem része.	-	-	X
29.	4.28. A naplóinformációk védelme – Kriptográfiai védelem	4.28. A szervezet kriptográfiai eszközöket alkalmaz a naplóinformációk és a naplókezelő eszköz sértetlenségének védelmére.	-	-	X
30.	4.29. A naplóinformációk védelme – Privilegizált felhasználók hozzáférése	4.29. A szervezet a naplózási funkciók kezeléséhez csak egy meghatározott jogosultsági szinttel rendelkező felhasználói csoportnak vagy felhasználói szerepeknek ad hozzáférési jogosultságot.	-	X	X
31.	4.30. A naplóinformációk védelme – Kettős jóváhagyás	4.30. A szervezet kikényszeríti a kettős jóváhagyást a szervezet által meghatározott naplóinformációk áthelyezéséhez vagy törléséhez.	-	-	-
32.	4.31. A naplóinformációk védelme – Hozzáférés csak olvasásra	4.31. A szervezet csak olvasási hozzáférést biztosít a naplóinformációkhoz a privilegizált felhasználók vagy szerepkörök egy meghatározott részhalmazának.	-	-	-
33.	4.32. A naplóinformációk védelme – Tárolás eltérő operációs rendszert futtató rendszerelemen	4.32. Az EIR a naplóinformációkat egy olyan rendszerelemben tárolja, amely eltérő operációs rendszert futtat, mint a naplózott rendszer vagy rendszerelem.	-	-	-

34.	4.33. Letagadhatatlanság	4.33. Az EIR megcáfolhatatlan bizonyítékot szolgáltat arra, hogy egy személy vagy a nevében futó feldolgozási folyamat végrehajtott egy a szervezet által meghatározott, a letagadhatatlanság követelménye alá eső tevékenységet.	-	-	X
35.	4.34. Letagadhatatlanság – Személyazonosság társítása	4.34. Az EIR: 4.34.1. Az információ előállítójának személyazonosságát összekapcsolja az információval, a szervezet által meghatározott módon. 4.34.2. Biztosítja a jogosult személyek számára, hogy megállapíthassák az információ előállítójának személyazonosságát.	-	-	-
36.	4.35. Letagadhatatlanság – Az információt előállító egyén személyazonossági kapcsolatának hitelesítése	4.35. A szervezet: 4.35.1. meghatározott gyakorisággal ellenőrzi az információt előállító egyén személyazonosságának és az előállított információnak az összekapcsolását; és 4.35.2. ellenőrzési hiba esetén végrehajtja az szervezet által meghatározott műveleteket.	-	-	-
37.	4.36. Letagadhatatlanság – Felügyeleti lánc	4.36. A szervezet fenntartja az információ kibocsátójához és felülvizsgálójához tartozó hitelesítő adatokat a létrehozott felügyeleti láncon belül.	-	-	-
38.	4.37. Letagadhatatlanság – Az információt ellenőrző egyén személyazonossági kapcsolatának hitelesítése	4.37. A szervezet: 4.37.1. ellenőrzi az információt felülvizsgáló egyén személyazonosságának és a felülvizsgált információnak az összekapcsolását az információ átadási vagy kiadási pontjainál, a kiadás vagy az átadás előtt a szervezet által meghatározott biztonsági tartományokban; és 4.37.2. ellenőrzési hiba esetén végrehajtja az szervezet által meghatározott műveleteket.	-	-	-
39.	4.38. A naplóbejegyzések megőrzése	4.38. A szervezet a naplóbejegyzéseket a jogszabályi és a szervezeten belüli információmegőrzési követelmények szerint meghatározott időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.	X	X	X
40.	4.39. A naplóbejegyzések megőrzése – Hosszú távú visszakeresési képesség	4.39. A szervezet olyan intézkedéseket alkalmaz, amelyek biztosítják a rendszer által generált naplóbejegyzések hosszú távú visszakereshetőségét.	-	-	-
41.	4.40. Naplóbejegyzések létrehozása	4.40. Az EIR: 4.40.1. Biztosítja a naplóbejegyzés generálási képességet a "Naplózható események" pontban meghatározott naplózható eseményekre. 4.40.2. Lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az EIR egyes elemei által. 4.40.3. Naplóbejegyzéseket állít elő a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal.	X	X	X
42.	4.41. Naplóbejegyzések létrehozása – Az egész rendszerre kiterjedő és időbeli naplózási nyomvonal.	4.41. Az EIR a szervezet által meghatározott rendszerelemekből származó naplóbejegyzésekből egy rendszerszintű naplót állít össze, amely a szervezet által meghatározott tűréshatáron belüli időbélyegek alapján kerül összekapcsolásra.	-	-	X
43.	4.42. Naplóbejegyzések létrehozása – Szabványos formátumok	4.42. Az EIR az egész rendszerre kiterjedő szabványos formátumú naplóbejegyzésekből álló naplót állít össze.	-	-	-
44.	4.43. Naplóbejegyzések létrehozása – Felhatalmazott személyek változtatásai	4.43. Az EIR lehetőséget biztosít a meghatározott személyeknek vagy szerepköröknek, hogy megváltoztassák az egyes rendszerelemek naplózását a meghatározott eseménykritériumok alapján egy meghatározott időtartamon belül.	-	-	X

45.	4.44. Információk kiszivárgásának figyelemmel kísérése	4.44. A szervezet: 4.44.1. Rendszeresen figyelemmel kíséri a meghatározott nyílt forrású információkat vagy információs oldalakat a szervezeti információk jogosulatlan nyilvánosságra hozatalának bizonyítékaiért. 4.44.2. Ha fény derül az információ nyilvánosságra hozatalára: 4.44.2.1. értesíti a meghatározott személyeket vagy szerepköröket; és 4.44.2.2. további meghatározott intézkedéseket hajt végre.	-	-	-
46.	4.45. Információ kiszivárgásának figyelemmel kísérése – Automatizált eszközök használata	4.45. A szervezet meghatározott automatizált mechanizmusok segítségével figyelemmel kíséri a nyílt forrású információkat és információs oldalakat.	-	-	-
47.	4.46. Információ kiszivárgásának figyelemmel kísérése – Figyelemmel kísért webhelyek felülvizsgálata	4.46. A szervezet meghatározott gyakorisággal felülvizsgálja a figyelemmel kísért nyílt forrású információs oldalak listáját.	-	-	-
48.	4.47. Információ kiszivárgásának figyelemmel kísérése – Információk jogosulatlan másolása	4.47. A szervezet felderítési technikákat, folyamatokat és eszközöket alkalmaz annak meghatározására, hogy külső entitások jogosulatlan módon másolják-e a szervezeti információkat.	-	-	-
49.	4.48. Munkaszakasz-ellenőrzés	4.48. A szervezet: 4.48.1. Gondoskodik arról, hogy bizonyos felhasználók vagy szerepkörök meghatározott körülmények között rögzíthessék, megtekinthessék, meghallgathassák vagy naplózhassák egy felhasználói munkaszakasz tartalmát. 4.48.2. A munkaszakasz ellenőrzési tevékenységeket a hatályos jogszabályokkal, szabályzatokkal, irányelvekkel összhangban dolgozza ki és valósítja meg.	-	-	-
50.	4.49. Munkaszakasz ellenőrzés – Rendszerindítás	4.49. Az EIR automatikusan elindítja a munkaszakasz ellenőrzéshez szükséges folyamatokat a rendszerindításkor.	-	-	-
51.	4.50. Munkaszakasz ellenőrzése – Távoli megfigyelés és lehallgatás	4.50. A szervezet biztosítja és megvalósítja azt a képességet, hogy az arra feljogosított felhasználók valós időben távolról megtekinthessék és meghallgathassák a létrehozott felhasználói munkaszakaszhoz kapcsolódó tartalmat.	-	-	-
52.	4.51. Szervezeten átívelő naplózás	4.51. A szervezet meghatározott módszereket alkalmaz a meghatározott naplóinformációk külső szervezetekkel történő egyeztetésére, amikor a naplóinformációt a szervezeti határokon túlra továbbítják.	-	-	-
53.	4.52. Szervezeten átívelő naplózás – Naplóinformációk megosztása	4.52. A szervezet biztosítja a meghatározott naplóinformációkat a meghatározott szervezetek számára az adott információmegosztási megállapodások alapján.	-	-	-

5. Értékelés, engedélyezés és monitorozás

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	5.1. Szabályzat és eljárásrendek	5.1. A szervezet: 5.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 5.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságértékelési szabályzatot, amely 5.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 5.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal. 5.1.1.2. A biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 5.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonságértékelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 5.1.3. Felülvizsgálja és frissíti az aktuális biztonságértékelési szabályzatot és a biztonságértékelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	5.2. Biztonsági értékelések	5.2. A szervezet: 5.2.1. Kiválasztja az elvégzendő értékelés típusának megfelelő értékelő személyt vagy csoportot. 5.2.2. Biztonságértékelési tervet készít, amely leírja az értékelés hatókörét, beleértve: 5.2.2.1. az értékelendő védelmi intézkedéseket, azok kiterjesztését és továbbfejlesztését; 5.2.2.2. a védelmi intézkedések hatékonyságának megállapításához használt értékelési eljárásokat; 5.2.2.3. az értékelési környezetet, az értékelő csoportot, az értékelő szerepköröket és feladataikat. 5.2.3. Biztosítja, hogy a biztonságértékelési tervet az engedélyezésre jogosult felelős vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálja és jóváhagyja. 5.2.4. Meghatározott gyakorisággal értékeli az EIR és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését. 5.2.5. Elkészíti a biztonságértékelés eredményét összefoglaló jelentést. 5.2.6. Gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek a szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.	X	X	X
4.	5.3. Biztonsági értékelések – Független értékelők	5.3. A 1. § (1) bekezdés hatálya alá tartozó szervezet - a honvédelmi célú rendszerek kivételével - független értékelőket vagy értékelőcsoportokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.	-	X	X
5.	5.4. Biztonsági értékelések – Kiberbiztonsági audit	5.4. A 1. § (2) bekezdés hatálya alá tartozó szervezet független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.	X	X	X

6.	5.5. Biztonsági értékelések – Speciális értékelések	5.5. A szervezet a védelmi intézkedések értékelése céljából rendszeresen bejelentett, vagy bejelentés nélküli: 5.5.1. mélységi monitorozást végezhet; 5.5.2. biztonsági berendezéseket alkalmazhat; 5.5.3. automatizált biztonsági teszteseteket hajthat végre; 5.5.4. sérülékenységszkennelést végezhet; 5.5.5. rosszhiszemű felhasználó teszteket hajthat végre; 5.5.6. belső fenyegetettség értékelést végezhet; 5.5.7. teljesítmény- és terhelési teszteket hajthat végre; 5.5.8. adatvesztés vagy adatszivárgás értékelést végezhet; 5.5.9. a szervezet által meghatározott egyéb biztonsági értékeléseket végezhet.	-	-	X
7.	5.6. Biztonsági értékelések – Külső szervezetek eredményeinek felhasználása	5.6. A vizsgált szervezet alkalmazza a meghatározott külső szervezetek által végzett értékelések eredményeit saját EIR-eiben, feltéve, hogy azok megfelelnek a szervezet által támasztott elvárásoknak.	-	-	-
8.	5.7. Információcsere	5.7. A szervezet: 5.7.1. Jóváhagyja és szabályozza az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal, továbbá figyelembe veszi a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat. 5.7.2. Minden egyes információcsere-megállapodás keretében dokumentálja az egyes rendszerek interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét, valamint rögzíti a megosztott információk hatásának szintjét is. 5.7.3. Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat.	X	X	X
9.	5.8. Információcsere – Átviteli engedélyek	5.8. A szervezet az adattovábbítás elfogadása előtt gondoskodik róla és ellenőrzi, hogy a kapcsolódó rendszerek között adatokat továbbító személyek vagy rendszerek rendelkeznek-e az adatátvitelhez szükséges jogosultságokkal.	-	-	X
10.	5.9. Információcsere – Áthaladó információcsere	5.9. A szervezet: 5.9.1. Az "Információcsere" pont szerint meghatározott EIR-ek által azonosítja a más rendszerek felé történő információáramlást (downstream). 5.9.2. Intézkedéseket hajt végre annak biztosítása érdekében, hogy az áthaladó információáramlás (downstream) megszűnjön, amikor az ezt biztosító rendszerek védelmi intézkedéseinek ellenőrzése vagy hitelesítése nem lehetséges.	-	-	-
11.	5.10. Az intézkedési terv és mérföldkövei	5.10. A szervezet: 5.10.1. Intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására, hogy a védelmi intézkedések értékelése során feltárt gyengeségeket vagy hiányosságokat kijavítsák, valamint a rendszer ismert sérülékenységeit csökkentsék vagy megszüntessék. 5.10.2. Rendszeresen frissíti az intézkedési tervet és a mérföldköveket, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.	X	X	X
12.	5.11. Az intézkedési terv és mérföldkövek – Pontosság és naprakészség automatizált támogatása	5.11. A szervezet meghatározott automatizált mechanizmusok segítségével biztosítja az EIR intézkedési tervének és mérföldköveinek pontosságát, naprakészségét és elérhetőségét.	-	-	-

13.	5.12. Engedélyezés	5.12. A szervezet: 5.12.1. Kijelöl egy engedélyezésért felelős személyt, aki az EIR-ért felel. 5.12.2. Kijelöl egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel. 5.12.3. Biztosítja, hogy az engedélyezésért felelős személy az EIR használatbavételét megelőzően: 5.12.3.1. elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; és 5.12.3.2. a szervezet vezetőjével engedélyezteti a rendszer működését. 5.12.4. Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát. 5.12.5. Rendszeresen felülvizsgálja az engedélyeket.	X	X	X
14.	5.13. Engedélyezés – Közös engedélyezés – Szervezeten belüli	5.13. A szervezet olyan együttes engedélyezési folyamatot alkalmaz, amely ugyanazon szervezet több engedélyezőjét is magában foglalja.	-	-	-
15.	5.14. Engedélyezés – Közös engedélyezés – Szervezetek közötti	5.14. A szervezet a szervezetek közötti engedélyezés esetén olyan együttes engedélyezési folyamatot alkalmaz, amely magában foglalja ugyanazon szervezet több engedélyezőjét, és legalább egy olyan engedélyező szerepben lévő személyt, aki nem a saját szervezetéhez tartozik.	-	-	-
16.	5.15. Folyamatos felügyelet	5.15. A szervezet kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket: 5.15.1. A rendszerszintű metrikák meghatározását. 5.15.2. Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére. 5.15.3. A védelmi intézkedések folyamatos értékelését. 5.15.4. Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését. 5.15.5. A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését. 5.15.6. A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket. 5.15.7. az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek.	X	X	X
17.	5.16. Folyamatos felügyelet – Független értékelés	5.16. A szervezet független értékelőket vagy értékelőcsoportokat alkalmaz az EIR-ben lévő védelmi intézkedések folyamatos ellenőrzésére.	-	X	X
18.	5.17. Folyamatos felügyelet – Trendelemzés	5.17. A szervezet trendelemzéseket alkalmaz, hogy a tapasztalati adatok alapján megállapítsa, szükséges-e módosítani a védelmi intézkedések végrehajtását, a folyamatos felügyeleti tevékenységek gyakoriságát, valamint a folyamatos felügyeleti folyamatban alkalmazott tevékenységtípusokat.	-	-	-
19.	5.18. Folyamatos felügyelet – Kockázatmonitorozás	5.18. A szervezet biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza: 5.18.1. a hatékonyság ellenőrzését; 5.18.2. a megfelelés ellenőrzését; és 5.18.3. a változások nyomon követését.	X	X	X
20.	5.19. Folyamatos felügyelet – Következetesség elemzése	5.19. A szervezet az általa meghatározott intézkedéseket alkalmazza, hogy ellenőrizze a szabályzatok kialakítását, illetve a végrehajtott védelmi intézkedések azzal konzisztens működését.	-	-	-

21.	5.20. Folyamatos felügyelet – Felügyelet automatizált támogatása	5.20. A szervezet az általa meghatározott automatizált mechanizmusok segítségével biztosítja, hogy a rendszer felügyeleti eredményei pontosak és naprakészek legyenek, valamint rendelkezésre álljanak.	-	-	-
22.	5.21. Behatolásvizsgálat (penetration testing)	5.21. A szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.	-	-	-
23.	5.22. Behatolásvizsgálat – Független szakértő vagy csapat	5.22. A szervezet független szakértőt vagy csapatot alkalmaz az EIR vagy a rendszerelemek behatolásvizsgálatának elvégzésére.	-	-	X
24.	5.23. Behatolásvizsgálat – „Vörös csapat” (red team) gyakorlatok	5.23. A szervezet meghatározott „vörös csapat” (red team) gyakorlatokat hajt végre annak érdekében, hogy szimulálja a támadók kísérleteit a szervezeti EIR-ek kompromittálására a vonatkozó szabályok szerint.	-	-	-
25.	5.24. Behatolásvizsgálat – Fizikai környezet	5.24. A szervezet meghatározott gyakorisággal olyan eljárásokat alkalmaz az EIR fizikai környezetének behatolásvizsgálatára, amelyek magukba foglalják a bejelentett vagy be nem jelentett, a védelmi intézkedések megkerülésére vagy kijátszására irányuló kísérleteket.	-	-	-
26.	5.25. Belső rendszerkapcsolatok	5.25. A szervezet: 5.25.1. Engedélyezi a szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását. 5.25.2. Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét. 5.25.3. Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat. 5.25.4. Meghatározott gyakorisággal felülvizsgálja minden belső kapcsolat további szükségességét.	X	X	X
27.	5.26. Belső rendszerkapcsolatok – Megfelelőségi ellenőrzések	5.26. A szervezet a biztonsági szabályoknak való megfelelőség ellenőrzést végez a rendszerelemeken, a belső kapcsolatok létrehozása előtt.	-	-	-

6. Konfigurációkezelés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	6.1. Szabályzat és eljárásrendek	6.1. A szervezet: 6.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 6.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó konfigurációkezelési szabályzatot, amely 6.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 6.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 6.1.1.2. A konfigurációkezelési eljárásrendet, amely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 6.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a konfigurációkezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 6.1.3. Felülvizsgálja és frissíti az aktuális konfigurációkezelési szabályzatot és a konfigurációkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően	X	X	X
3.	6.2. Alapkonfiguráció	6.2. A szervezet: 6.2.1. Kifejleszti, dokumentálja és karbantartja az EIR alapkonfigurációját. 6.2.2. Elvégzi az EIR alapkonfigurációjának felülvizsgálatát és frissítését: 6.2.2.1. meghatározott időközönként; 6.2.2.2. ha azt a meghatározott körülmények indokolják, vagy 6.2.2.3. az EIR vagy rendszerelemek telepítésekor vagy frissítésekor.	X	X	X
4.	6.3. Alapkonfiguráció – Automatikus támogatás a pontosság és a napra készségérdekében	6.3. A szervezet automatizált mechanizmusokat alkalmaz az EIR naprakész, teljes, pontos és állandóan rendelkezésre álló alapkonfigurációjának karbantartására.	-	X	X
5.	6.4. Alapkonfiguráció – Korábbi konfigurációk megőrzése	6.4. A szervezet megőrzi az EIR alapkonfigurációjának a szervezet által meghatározott számú korábbi verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.	-	X	X
6.	6.5. Alapkonfiguráció – Fejlesztési és tesztkörnyezetek	6.5. A szervezet egy-egy alapkonfigurációt tart fenn a rendszerfejlesztési és tesztkörnyezetekhez, amelyeket külön kezel az élesüzemi alapkonfigurációtól.	-	-	-

7.	6.6. Alapkonfiguráció – Rendszerek és rendszerelemek konfigurálása magas kockázatú területekre	6.6. A szervezet: 6.6.1. Meghatározott konfigurációs beállításokkal ellátott meghatározott EIR-eket vagy rendszerelemeket biztosít a szervezet által jelentős kockázatúnak ítélt helyszínen történő felhasználáshoz. 6.6.2. Meghatározott védelmi intézkedéseket alkalmaz a rendszerekre vagy rendszerelemekre a jelentős kockázatú helyszínekről történő visszatérést követően.	-	X	X
8.	6.7. A konfigurációváltozások felügyelete (változáskezelés)	6.7. A szervezet: 6.7.1. Meghatározza és dokumentálja a változáskezelési felügyelet ellenőrzés hatálya alá eső rendszermódosításokat. 6.7.2. Megvizsgálja, valamint biztonsági szempontokat érvényesítve jóváhagyja vagy elutasítja a konfigurációra vonatkozó módosítási javaslatokat. 6.7.3. Dokumentálja az EIR-ben történt változtatásokra vonatkozó döntéseket. 6.7.4. Megvalósítja a jóváhagyott változtatásokat az EIR-ben. 6.7.5. Meghatározott időtartamig nyilvántartja és visszakereshetően megőrzi az EIR-ben megvalósított változtatások dokumentumait. 6.7.6. Ellenőrzi és felülvizsgálja a konfiguráció ellenőrzés hatálya alá eső változtatásokkal kapcsolatos tevékenységeket. 6.7.7. Koordinálja és felügyeli a konfigurációváltoztatásokat egy erre a célra kijelölt egység (például személy, testület, szoftver, folyamat stb.) által, amelyet meghatározott gyakorisággal vagy a konfigurációmódosítási feltételek fennállása esetén alkalmaznak.	-	X	X
9.	6.8. A konfigurációváltozások felügyelete – Automatizált dokumentáció, értesítés és változtatási tilalom	6.8. A szervezet meghatározott automatizált mechanizmusokat alkalmaz: 6.8.1. az EIR-ben javasolt változtatások dokumentálására; 6.8.2. a jóváhagyásra jogosultak értesítése a javasolt változtatási igényekről; 6.8.3. azon változások kiemelésére, amelyeket még nem hagytak jóvá vagy késedelmesen hagytak jóvá; 6.8.4. a még nem jóváhagyott változások végrehajtásának megakadályozására; 6.8.5. az EIR-ben végrehajtott változások teljes dokumentálására; 6.8.6. a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.	-	-	X
10.	6.9. A konfigurációváltozások felügyelete – Változások tesztelése, jóváhagyása és dokumentálása	6.9. A szervezet teszteli, jóváhagyja és dokumentálja az EIR változtatásait azok bevezetése előtt.	-	X	X
11.	6.10. A konfigurációváltozások felügyelete – Automatizált változásbevezetés	6.10. A szervezet meghatározott automatizált mechanizmusok segítségével hajtja végre az alapkonfiguráció módosítását és a frissített alapkonfiguráció telepítését az EIR-ben.	-	-	-
12.	6.11. A konfigurációváltozások felügyelete – Automatizált biztonsági válaszlépések	6.11. A szervezet automatikusan végrehajtja a meghatározott biztonsági válaszlépéseket, amennyiben az alapkonfigurációt jogosulatlanul megváltoztatják.	-	-	-
13.	6.12. A konfigurációváltozások felügyelete – Kriptográfia kezelése	6.12. A szervezet az általa meghatározott védelmi intézkedésekhez használt kriptográfiai mechanizmusokat a konfigurációkezelés hatálya alá vonja.	-	-	X
14.	6.13. A konfigurációváltozások felügyelete – Rendszer változásainak felülvizsgálata	6.13. A szervezet meghatározott gyakorisággal, vagy a szervezet által meghatározott körülmények esetén megvizsgálja a rendszerben történt változásokat annak megállapítása érdekében, hogy történtek-e jogosulatlan változtatások.	-	-	-
15.	6.14. A konfigurációváltozások felügyelete – Konfiguráció megváltoztatásának	6.14. A szervezet meghatározott körülmények esetén megakadályozza vagy korlátozza az EIR konfigurációjának módosítását.	-	-	-

	megakadályozása vagy korlátozása				
16.	6.15. Biztonsági hatásvizsgálatok	6.15. A szervezet még a változtatások bevezetése előtt megvizsgálja az EIR-ben tervezett változtatásoknak az információbiztonsági hatásait.	X	X	X
17.	6.16. Biztonsági hatásvizsgálatok – Különálló tesztkörnyezetek	6.16. A szervezet elkülönített tesztkörnyezetben vizsgálja a változtatásokat, mielőtt azokat éles rendszerben alkalmazná, keresve a biztonsági hatásokat, amelyek hiányosságokból, sérülékenységekből, kompatibilitási problémákból vagy szándékos rosszindulatból adódhatnak.	-	-	X
18.	6.17. Biztonsági hatásvizsgálatok – Követelmények ellenőrzése	6.17. A szervezet a rendszermódosítások után ellenőrzi, hogy a védelmi intézkedések helyesen lettek-e bevezetve, megfelelően működnek-e, és biztosítják-e a kívánt eredményeket, figyelembe véve az EIR biztonsági követelményeit.	-	X	X
19.	6.18. A változtatásokra vonatkozó hozzáférés korlátozások	6.18. A szervezet meghatározza, dokumentálja, jóváhagyja és érvényesíti azokat a fizikai és logikai hozzáférési korlátozásokat, amelyek az EIR változtatásaihoz kapcsolódnak.	X	X	X
20.	6.19. A változtatásokra vonatkozó hozzáférés korlátozások – Automatizált hozzáférés-érvényesítés és naplóbejegyzések	6.19. Az EIR: 6.19.1. automatizált mechanizmusok segítségével érvényesíti a hozzáférési korlátozásokat, és 6.19.2. automatikusan előállítja a naplóbejegyzéseket az érvényesítési műveletekről.	-	-	X
21.	6.20. A változtatásokra vonatkozó hozzáférés korlátozások – Kettős jóváhagyás	6.20. A szervezet kettős jóváhagyást alkalmaz a változások végrehajtásához, a szervezet által meghatározott rendszerelemek és rendszerszintű információk esetében.	-	-	-
22.	6.21. A változtatásokra vonatkozó hozzáférés korlátozások – Jogosultságok korlátozása élesüzemi rendszerek esetén	6.21. A szervezet: 6.21.1. Korlátozza a rendszerelemek és a rendszerrel kapcsolatos információk módosítására vonatkozó jogosultságokat az élesüzemi környezetben. 6.21.2. Meghatározott időközönként felülvizsgálja és újraértékeli a jogosultságokat.	-	-	-
23.	6.22. A változtatásokra vonatkozó hozzáférés korlátozások – Szoftverkönyvtári jogosultságok korlátozása	6.22. A szervezet korlátozza a szoftverkönyvtárakban lévő szoftverek módosítására vonatkozó jogosultságokat.	-	-	-
24.	6.23. Konfigurációs beállítások	6.23. A szervezet 6.23.1. Kialakítja és dokumentálja a rendszerelemekben alkalmazott egységes biztonsági konfigurációs beállításokat, amelyek az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot képviselik. 6.23.2. Elvégzi a konfigurációs beállításokat az EIR valamennyi elemében. 6.23.3. Azonosítja, dokumentálja és elfogadja a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket. 6.23.4. Figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait a szervezeti szabályzatokkal és eljárásokkal összhangban.	X	X	X
25.	6.24. Konfigurációs beállítások – Automatizált kezelés, alkalmazás és ellenőrzés	6.24. A szervezet az által meghatározott automatizált mechanizmusok segítségével irányítja, alkalmazza és ellenőrzi a szervezet által meghatározott rendszerelemek konfigurációs beállításait.	-	-	X
26.	6.25. Konfigurációs beállítások – Reagálás a jogosulatlan változtatásokra	6.25. A szervezet meghatározott lépéseket tesz a szervezet által meghatározott konfigurációs beállítások jogosulatlan módosításaira válaszul.	-	-	X

27.	6.26. Legszűkebb funkcionalitás	6.26. A szervezet: 6.26.1. Az EIR-t úgy konfigurálja, hogy az csak az ügy- és üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa. 6.26.2. Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat.	X	X	X
28.	6.27. Legszűkebb funkcionalitás – Rendszeres felülvizsgálat	6.27. A szervezet: 6.27.1. Meghatározott gyakorisággal átvizsgálja az EIR-t, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat. 6.27.2. Kikapcsolja vagy eltávolítja azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyeket szükségtelennek vagy nem biztonságosnak ítél.	-	X	X
29.	6.28. Legszűkebb funkcionalitás – Program futtatásának megakadályozása	6.28. A szervezet megakadályozza a program futtatását, amennyiben az nem a meghatározott szabályzatok és eljárásrendek szerint történik.	-	X	X
30.	6.29. Legszűkebb funkcionalitás – Regisztrációs követelményeknek való megfelelés	6.29. A szervezet biztosítja, hogy a funkciók, portok, protokollok és szolgáltatások regisztrációja megfeleljen a meghatározott követelményeknek.	-	-	-
31.	6.30. Legszűkebb funkcionalitás – Engedély nélküli szoftverek — Kivételes letiltás	6.30. A szervezet: 6.30.1. Azonosítja az EIR-ben a nem engedélyezett szoftvereket. 6.30.2. Alkalmazza az alapértelmezett engedélyezés és a kivétel alapú tiltás szabályt, amely megtiltja a nem engedélyezett szoftverek futtatását. 6.30.3. Rendszeresen felülvizsgálja és frissíti az EIR-ben nem engedélyezett szoftverek listáját.	-	-	-
32.	6.31. Legszűkebb funkcionalitás – Engedélyezett Szoftverek — Kivételes Engedélyezés	6.31. A szervezet: 6.31.1. Azonosítja az EIR-en vagy EIR által futtatható szoftvereket. 6.31.2. Alkalmazza az alapértelmezett tiltás és a kivétel alapú engedélyezés szabályt a rendszeren futtatható szoftverek esetében. 6.31.3. Meghatározott gyakorisággal felülvizsgálja és frissíti az engedélyezett szoftverek listáját.	-	X	X
33.	6.32. Legszűkebb funkcionalitás – Korlátozott jogosultságú zárt környezetek	6.32. A szervezet megköveteli, hogy a meghatározott felhasználók által telepített szoftvereket fizikai vagy virtuális gépi környezetben korlátozott jogosultságokkal futtassák.	-	-	-
34.	6.33. Legszűkebb funkcionalitás – Kódvégrehajtás védett környezetekben	6.33. A szervezet a bináris vagy gépi kód futtatását csak korlátozott fizikai vagy virtuális környezetben és a meghatározott személyek vagy szerepkörök külön jóváhagyásával engedélyezi, ha az ilyen kód: 6.33.1. korlátozott garanciájú vagy garancia nélküli forrásból származik; 6.33.2. forráskódját nem bocsátották rendelkezésre.	-	-	-
35.	6.34. Legszűkebb funkcionalitás – Bináris vagy gépi futtatható kód	6.34. A szervezet: 6.34.1. megtiltja az olyan forrásból származó bináris vagy gépi futtatható kódok használatát, amelynek nincs vagy korlátozott a garanciája, vagy amelynek a forráskódját nem bocsátották rendelkezésre; 6.34.2. kivételeket csak nyomós szervezeti érdek vagy működési követelmények esetén engedélyez a felelős engedélyező tisztviselő jóváhagyásával.	-	-	-
36.	6.35. Legszűkebb funkcionalitás – Nem engedélyezett hardverek használatának tilalma	6.35. A szervezet: 6.35.1. Azonosítja azokat a hardverelemeket, amelyek használata az EIR-ben engedélyezett. 6.35.2. Megtiltja a nem engedélyezett hardverelemek használatát vagy csatlakoztatását. 6.35.3. Meghatározott gyakorisággal felülvizsgálja és frissíti az engedélyezett hardverelemek listáját.	-	-	-

37.	6.36. Rendszerelem leltár	6.36. A szervezet: 6.36.1. Leltárt készít az EIR elemeiről. 6.36.1.1. A leltár pontosan tükrözi az EIR-t. 6.36.1.2. A leltár tartalmazza a rendszeren belül található összes elemet. 6.36.1.3. Megakadályozza az elemek kettős elszámolását. 6.36.1.4. A leltár a nyomon követés és a jelentéstétel szempontjából a szükséges részletességet biztosítja. 6.36.1.5. A leltárban szereplő információk lehetővé teszik a rendszerelemekkel történő hatékony elszámolást. 6.36.2. Meghatározott gyakorisággal felülvizsgálja és frissíti a rendszerelemek leltárát.	X	X	X
38.	6.37. Rendszerelem leltár – Frissítések a telepítés és eltávolítás során	6.37. A szervezet a rendszerelemek leltárát frissíti minden egyes rendszerelem telepítése, eltávolítása és frissítése alkalmával.	-	X	X
39.	6.38. Rendszerelem leltár – Automatizált karbantartás	6.38. A szervezet meghatározott automatizált mechanizmusokat alkalmaz a rendszerelem leltár naprakészségének, teljességének, pontosságának és hozzáférhetőségének a fenntartására.	-	-	X
40.	6.39. Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése	6.39. A szervezet: 6.39.1. Meghatározott gyakorisággal, automatizált mechanizmusok segítségével vizsgálja a rendszerben található jogosulatlan hardver-, szoftver-, és firmware-elemek jelenlétét. 6.39.2. A jogosulatlan elemek észlelése esetén letiltja az ilyen elemek hálózati hozzáférését, izolálja a rendszerelemeket és értesíti a szervezet által meghatározott személyeket vagy szerepköröket.	-	-	X
41.	6.40. Rendszerelem leltár – Elszámoltathatósággal kapcsolatos információk	6.40. A szervezet a rendszerelem leltárt olyan módon alakítja ki, amely lehetővé teszi a rendszerelemek kezeléséért felelős és számonkérhető személyek azonosítását név, munkakör és szerepkör alapján.	-	-	X
42.	6.41. Rendszerelem leltár – Értékelés alatt álló konfigurációk és jóváhagyott eltérések	6.41. Az értékelés alatt álló rendszerelem konfigurációknak, valamint az aktuálisan telepített konfigurációktól való minden jóváhagyott eltérésnek szerepelnie kell a rendszerelem leltárában.	-	-	-
43.	6.42. Rendszerelem leltár – Központi adattár	6.42. A szervezet egy központi adattárat biztosít a rendszerelem leltárának.	-	-	-
44.	6.43. Rendszerelem leltár – Automatizált helymeghatározás	6.43. A szervezet automatizált mechanizmusokat alkalmaz a rendszerelemek földrajzi hely szerinti nyomon követésének támogatására.	-	-	-
45.	6.44. Rendszerelem leltár – Rendszerelemek rendszerhez rendelése	6.44. A szervezet: 6.44.1. Minden rendszerelemet legalább egy EIR-hez rendel. 6.44.2. A hozzárendelésről visszaigazolást kap a szervezet által meghatározott személyektől vagy szerepköröktől.	-	-	-
46.	6.45. Konfigurációkezelési terv	6.45. A szervezet kialakít, dokumentál és végrehajt egy, az EIR-re vonatkozó konfigurációkezelési tervet, amely: 6.45.1. figyelembe veszi a szerepköröket, a felelősségeket, és a konfigurációkezelési folyamatokat és eljárásokat; 6.45.2. bevezet egy folyamatot a rendszerfejlesztési életciklus folyamán a konfigurációs elemek azonosítására a konfigurációs elemek konfigurációjának kezelése céljából; 6.45.3. meghatározza az EIR konfigurációs elemeit, és a konfigurációs elemeket a konfigurációkezelés hatálya alá helyezi; 6.45.4. a meghatározott személyek vagy szerepkörök által kerül felülvizsgálatra és jóváhagyásra; 6.45.5. védi a konfigurációkezelési tervet a jogosulatlan közzététellel és módosítással szemben.	-	X	X

47.	6.46. Konfigurációkezelési terv – Felelősség hozzárendelése	6.46. A szervezet a konfigurációkezelési folyamat fejlesztésének felelősségét olyan személyre bízza, aki közvetlenül nem vesz részt a rendszerfejlesztésben.	-	-	-
48.	6.47. A szoftverhasználat korlátozásai	6.47. A szervezet: 6.47.1. Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak. 6.47.2. A másolatok és megosztások ellenőrzésére nyomon követi a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát. 6.47.3. Ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására.	X	X	X
49.	6.48. A szoftverhasználat korlátozásai – Nyílt-forráskódú szoftver	6.48. A szervezet meghatározott korlátozásokat alkalmaz a nyílt forráskódú szoftverek használatára vonatkozóan.	-	-	-
50.	6.49. Felhasználó által telepített szoftver	6.49. A szervezet: 6.49.1. Megfogalmazza az EIR vonatkozásában a szervezetre érvényes követelményeket, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségeit. 6.49.2. Érvényesíti a szoftvertelepítésre vonatkozó szabályokat a szervezet által meghatározott módszerek szerint. 6.49.3. Meghatározott gyakorisággal ellenőrzi a szabályok betartását	X	X	X
51.	6.50. Felhasználó által telepített szoftverek – Szoftvertelepítés privilegizált státusszal	6.50. A szervezet csak a kifejezetten privilegizált jogosultsággal rendelkező felhasználóknak engedélyezi a szoftverek telepítését.	-	-	-
52.	6.51. A felhasználó által telepített szoftverek – Automatizált kikényszerítés és felügyelet	6.51. A szervezet automatizált mechanizmusokat alkalmaz a szoftvertelepítési szabályok kikényszerítésére és ellenőrzésére.	-	-	-
53.	6.52. Információ helyének azonosítása és dokumentálása	6.52. A szervezet: 6.52.1. azonosítja és dokumentálja a meghatározott információk, valamint azon konkrét rendszerelemeket helyét, amelyeken az információfeldolgozásra és tárolásra kerül; 6.52.2. azonosítja és dokumentálja azokat a felhasználókat, akik hozzáféréssel rendelkeznek a rendszerhez és a rendszerelemekhez, ahol az információ feldolgozásra és tárolásra kerül; és 6.52.3. dokumentálja azokat a változásokat, amelyek az információ feldolgozásának és tárolásának helyét érintik.	-	X	X
54.	6.53. Aláírt rendszerelemek	6.53. A szervezet megakadályozza a meghatározott szoftver- és firmware-összetevők telepítését még annak ellenőrzését megelőzően, hogy az összetevő digitális aláírása a szervezet által jóváhagyott tanúsítvánnyal megtörtént.	-	-	-

7. Készenléti tervezés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	7.1. Szabályzat és eljárásrendek	7.1. A szervezet: 7.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 7.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó üzletmenet-folytonosságra vonatkozó szabályzatot, amely 7.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 7.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 7.1.1.2. az üzletmenet-folytonosságra vonatkozó eljárásrendet, amely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 7.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 7.1.3. Felülvizsgálja és frissíti az aktuális üzletmenet-folytonosságra vonatkozó szabályzatot és az üzletmenet-folytonosságra vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X

3.	7.2. Üzletmenet-folytonossági terv	7.2. A szervezet: 7.2.1. Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely: 7.2.1.1. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket; 7.2.1.2. tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat; 7.2.1.3. kijelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket és azok elérhetőségeit; 7.2.1.4. meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat; 7.2.1.5. tartalmazza az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek; 7.2.1.6. szabályozza az üzletmenet-folytonossági információk megosztását; és 7.2.1.7. a szervezet által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott. 7.2.2. Megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint A szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az EIR-ekre vonatkozó üzletmenet-folytonossági tervet. 7.2.3. Összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével; 7.2.4. Meghatározott gyakorisággal felülvizsgálja az EIR-hez kapcsolódó üzletmenet-folytonossági tervet. 7.2.5. Az EIR vagy a működési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet. 7.2.6. Tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket. 7.2.7. Az üzletmenet-folytonossági terv tesztelése, gyakorlata vagy tényleges alkalmazása során levont tanulságokat beépíti a tesztelési és gyakorlati folyamatokba. 7.2.8. Gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető és módosítható.	X	X	X
4.	7.3. Üzletmenet-folytonossági terv – Összehangolás a kapcsolódó tervekkel	7.3. A szervezet egyezteti az üzletmenet-folytonossági tervet a kapcsolódó tervekért felelős szervezeti egységekkel.	-	X	X
5.	7.4. Üzletmenet-folytonossági terv – Kapacitás tervezése	7.4. A szervezet megtervezi a folyamatos működéshez szükséges információfeldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.	-	-	X
6.	7.5. Üzletmenet-folytonossági terv – Üzleti (ügymeneti) funkciók visszaállítása	7.5. A szervezet meghatározza az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.	-	X	X
7.	7.6. Üzletmenet-folytonossági terv – Alapfeladatok és alapfunkciók folyamatossága	7.6. A szervezet az alapfeladatok és alapfunkciók folyamatosságát úgy tervezi meg, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő. Fenntartható legyen a folyamatosság az EIR elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.	-	-	X

8.	7.7. Üzletmenet-folytonossági terv – Alternatív feldolgozási és tárolási helyszínek	7.7. A szervezet a folytonosság fenntartása érdekében megtervezi az alapfeladatok vagy alapfunkciók minimális, vagy akár veszteség nélküli átirányítását alternatív feldolgozási vagy tárolási helyszínekre, amíg az EIR vissza nem állítható az elsődleges feldolgozási vagy tárolási helyszínen.	-	-	-
9.	7.8. Üzletmenet-folytonossági terv – Együttműködés külső szolgáltatókkal	7.8. A szervezet összehangolja saját üzletmenet-folytonossági tervét a külső szolgáltatókkal, hogy a folyamatos működéshez szükséges követelmények teljesíthetők legyenek.	-	-	-
10.	7.9. Üzletmenet-folytonossági terv – Kritikus erőforrások meghatározása	7.9. A szervezet meghatározza az összes szervezet működése szempontjából kritikus erőforrást, amelyek az alapfeladatok vagy az alapvető üzleti folyamatok működéséhez szükségesek.	-	X	X
11.	7.10. A folyamatos működésre felkészítő képzés	7.10. A szervezet: 7.10.1. Az EIR felhasználói számára szerepkörüknek vagy felelősségi körüknek megfelelő folyamatos működésre felkészítő képzést tart: 7.10.1.1. szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül; 7.10.1.2. amikor az EIR változásai ezt szükségessé teszik; 7.10.1.3. a szervezet által meghatározott gyakorisággal. 7.10.2. Meghatározott gyakorisággal vagy meghatározott eseményeket követően felülvizsgálja és frissíti a folyamatos működésre felkészítő képzés tartalmát.	X	X	X
12.	7.11. A folyamatos működésre felkészítő képzés – Szimulált események	7.11. A szervezet a folyamatos működésre felkészítő képzésben szimulált eseményeket alkalmaz, hogy elősegítse a személyzet hatékony reagálását a szervezet működése szempontjából kritikus helyzetekben.	-	-	X
13.	7.12. A folyamatos működésre felkészítő képzés – A képzési környezetben használt mechanizmusok	7.12. A szervezet valós működési mechanizmusokat alkalmaz, hogy ezáltal alaposabb és valósághűbb vészhelyzeti képzési környezetet biztosítson.	-	-	-
14.	7.13. Üzletmenet-folytonossági terv tesztelése	7.13. A szervezet: 7.13.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az EIR-re vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és a szervezet felkészültségének felmérése céljából; értékeli az üzletmenet-folytonossági terv tesztelési eredményeit; 7.13.2. felülvizsgálja az üzletmenet-folytonossági terv tesztelési eredményeit; 7.13.3. a felülvizsgálat eredményei alapján, szükség esetén javítja a tervet.	-	X	X
15.	7.14. Üzletmenet-folytonossági terv tesztelése – Összehangolás a kapcsolódó tervekkel	7.14. A szervezet egyezteti az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel.	-	X	X
16.	7.15. Üzletmenet-folytonossági terv tesztelése – Alternatív feldolgozási helyszín	7.15. A szervezet teszteli az üzletmenet folytonossági tervet az alternatív feldolgozási helyszínen: 7.15.1. a vészhelyzeti személyzetnek a létesítménnyel és az elérhető erőforrásokkal való megismertetése érdekében; és 7.15.2. az alternatív feldolgozási helyszín képességeinek értékelése és a vészhelyzeti műveletek támogatása céljából.	-	-	X
17.	7.16. Üzletmenet-folytonossági terv tesztelése – Automatizált tesztelés	7.16. A szervezet meghatározott automatizált mechanizmusok segítségével teszteli az üzletmenet-folytonossági tervet.	-	-	-
18.	7.17. Üzletmenet-folytonossági terv tesztelése – Teljes helyreállítás és rekonstrukció	7.17. Az üzletmenet-folytonossági terv tesztelésének részét képezi a rendszer teljes és az utolsó ismert állapotba történő helyreállítása.	-	-	-
19.	7.18. Üzletmenet-folytonossági terv tesztelése – Öntesztelés	7.18. A szervezet meghatározott mechanizmusokat alkalmaz az EIR vagy rendszerelem működésének zavarására és hátrányos befolyásolására.	-	-	-

20.	7.19. Biztonsági tárolási helyszín	7.19. A szervezet: 7.19.1. létrehoz egy biztonsági tárolási helyszínt, beleértve a szükséges megállapodásokat, a rendszer biztonsági mentési információinak tárolásához és visszakereséséhez; 7.19.2. biztosítja, hogy a biztonsági tárolási helyszín ugyanolyan szintű védelmi intézkedéseket biztosítson, mint az elsődleges helyszín.	-	X	X
21.	7.20. Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől	7.20. A szervezet megfelelően elkülöníti a biztonsági tárolási helyszínt az elsődleges tárolási helyszíntől, az azonos veszélyeknek való kitettségük csökkentése érdekében.	-	X	X
22.	7.21. Biztonsági tárolási helyszín – Helyreállítási idő és helyreállítási pont céljai	7.21. A szervezet a biztonsági tárolási helyszínt úgy konfigurálja, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.	-	-	X
23.	7.22. Biztonsági tárolási helyszín – Hozzáférhetőség	7.22. A szervezet azonosítja a potenciális hozzáférési problémákat a biztonsági tárolási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határoz meg.	-	X	X
24.	7.23. Alternatív feldolgozási helyszín	7.23. A szervezet: 7.23.1. Kijelöl egy alternatív feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésre, az EIR előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - az alternatív helyszínen újrakezdhesse, vagy folytathassa. 7.23.2. Gondoskodik arról, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek az alternatív feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak, akár külső szervezettel kötött szerződések által biztosítva. 7.23.3. Biztosítja, hogy az alternatív feldolgozási helyszín védelmi intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal	-	X	X
25.	7.24. Alternatív feldolgozási helyszín – Elkülönítés az elsődleges helyszíntől	7.24. A szervezet olyan alternatív feldolgozási helyszínt jelöl ki, amely megfelelően elkülönül az elsődleges feldolgozási helyszíntől, az azonos fenyegetésekkel szembeni kitettség csökkentése érdekében.	-	X	X
26.	7.25. Alternatív feldolgozási helyszín – Hozzáférhetőség	7.25. A szervezet azonosítja a potenciális hozzáférési problémákat az alternatív feldolgozási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határoz meg.	-	X	X
27.	7.26. Alternatív feldolgozási helyszín – Szolgálatás prioritása	7.26. A szervezet az alternatív feldolgozási helyszínre vonatkozóan olyan megállapodásokat köt, és olyan intézkedéseket vezet be, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal) összhangban álló szolgáltatásprioritási rendelkezéseket tartalmaznak.	-	X	X
28.	7.27. Alternatív feldolgozási helyszín – Használatra való felkészítés	7.27. A szervezet úgy készíti fel az alternatív feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.	-	-	X
29.	7.28. Alternatív feldolgozási helyszín – Az elsődleges helyszínre való visszatérés akadályoztatása	7.28. A szervezet tervet készít és felkészül azokra a körülményekre, amikor nem lehetséges a visszatérés az elsődleges feldolgozási helyszínre.	-	-	-
30.	7.29. Telekommunikációs szolgáltatások	7.29. A szervezet tartalék infokommunikációs szolgáltatásokat létesít. Erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az EIR alapfunkcióinak, vagy meghatározott műveleteinek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.	-	-	X

31.	7.30. Telekommunikációs szolgáltatások – Szolgáltatásprioritási rendelkezések	7.30. Amennyiben A szervezet által igénybe vett elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor annak tartalmaznia kell a szolgáltatásprioritási rendelkezéseket, összhangban a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal).	-	X	X
32.	7.31. Telekommunikációs szolgáltatások – Kritikus meghibásodási pont	7.31. A szervezet olyan tartalék infokommunikációs szolgáltatásokat vesz igénybe, amelyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét.	-	X	X
33.	7.32. Telekommunikációs szolgáltatások – Elsődleges és másodlagos szolgáltatók különválasztása	7.32. A szervezet tartalék infokommunikációs szolgáltatásokat szerez be, nem csak az elsődleges szolgáltatóktól, hanem a tőlük elkülönült független szolgáltatóktól is, hogy csökkentse a szervezet azonos fenyegetéseknek való kitettségét.	-	-	X
34.	7.33. Telekommunikációs szolgáltatások – Szolgáltatói üzletmenet-folytonossági terv	7.33. A szervezet: 7.33.1. Előírja, hogy az elsődleges és a tartalék infokommunikációs szolgáltatóknak rendelkezniük kell üzletmenet-folytonossági tervvel. 7.33.2. Felülvizsgálja a szolgáltatók üzletmenet-folytonossági terveit annak érdekében, hogy megfelelnek-e az általa meghatározott üzletmenet-folytonossági követelményeknek. 7.33.3. Meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját.	-	-	X
35.	7.34. Telekommunikációs szolgáltatások – Másodlagos távközlési szolgáltatás tesztelése	7.34. A szervezet meghatározott gyakorisággal teszteli a tartalék infokommunikációs szolgáltatásokat.	-	-	-
36.	7.35. Az elektronikus információs rendszer mentései	7.35. A szervezet: 7.35.1. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. 7.35.2. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt rendszerszintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. 7.35.3. Meghatározott gyakorisággal mentést készít az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. 7.35.4. Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a biztonsági tárolási helyszínen.	X	X	X
37.	7.36. Az elektronikus információs rendszer mentései – Megbízhatóság és sértetlenség tesztelése	7.36. A szervezet meghatározott gyakorisággal teszteli a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.	-	X	X
38.	7.37. Az elektronikus információs rendszer mentései – Visszaállítás tesztelése mintavétellel	7.37. A szervezet a helyreállítási terv tesztelésének részeként egy kiválasztott mintát használ a mentett információkból az EIR kiválasztott funkcióinak helyreállítása során.	-	-	X
39.	7.38. Az elektronikus információs rendszer mentései – Kritikus információk elkülönített tárhelye	7.38. A szervezet az EIR szervezet működése szempontjából kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak mentéseit az elsődleges feldolgozási helyszíntől elkülönített létesítményben vagy egy tűzbiztos tárolóban tárolja.	-	-	X
40.	7.39. Az elektronikus információs rendszer mentései – Átvitel másodlagos tárolási helyszínre	7.39. A szervezet meghatározott adatátviteli sebességgel vagy meghatározott idő alatt, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal, átmásolja az EIR mentésének információit az alternatív tárolási helyszínre.	-	-	X

41.	7.40. Az elektronikus információs rendszer mentései – Redundáns másodlagos rendszer	7.40. A szervezet az EIR biztonsági mentését egy másodlagos, redundáns rendszeren tárolja, amely az elsődleges EIR-től különálló helyen található, és információvesztés vagy működési zavarok nélkül állítható üzembe.	-	-	-
42.	7.41. Az elektronikus információs rendszer mentései – Kettős jóváhagyás a törlésre vagy megsemmisítésre	7.41. A szervezet kettős jóváhagyáshoz köti a szervezet által meghatározott biztonsági mentési információk törlését vagy megsemmisítését.	-	-	-
43.	7.42. Az elektronikus információs rendszer mentései – Kriptográfiai védelem	7.42. A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy megakadályozza a meghatározott biztonsági mentési információk jogosulatlan felfedését és módosítását.	-	X	X
44.	7.43. Az elektronikus információs rendszer helyreállítása és újraindítása	7.43. A szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.	X	X	X
45.	7.44. Az elektronikus információs rendszer helyreállítása és újraindítása – Tranzakciók helyreállítása	7.44. A szervezet tranzakció alapú EIR-ek esetén tranzakció-helyreállítást hajt végre.	-	X	X
46.	7.45. Az elektronikus információs rendszer helyreállítása és újraindítása – Meghatározott időn belüli visszaállítás	7.45. A szervezet biztosítja, hogy a rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani, olyan ellenőrzött konfigurációból és sértetlenségvédett információkból, amelyek a rendszerelem ismert működési állapotát reprezentálják.	-	-	X
47.	7.46. Az elektronikus információs rendszer helyreállítása és újraindítása – Rendszerelem védelem	7.46. A szervezet védi azokat a rendszerelemeket, amelyeket a helyreállítás során használnak.	-	-	-
48.	7.47. Alternatív kommunikációs protokollok	7.47. A szervezet biztosítja a meghatározott alternatív kommunikációs protokollok alkalmazását a műveletek folyamatosságának fenntartása érdekében.	-	-	-
49.	7.48. Átállás biztonságos üzemmódra	7.48. Az érintett EIR a szervezet által meghatározott korlátozásokkal rendelkező biztonságos üzemmódba vált, amennyiben a szervezet által meghatározott feltételek észlelésre kerülnek.	-	-	-
50.	7.49. Alternatív biztonsági mechanizmusok alkalmazása	7.49. A szervezet a meghatározott tartalék vagy kiegészítő biztonsági mechanizmusokat alkalmazza a meghatározott biztonsági funkciók megvalósítására, amikor az elsődleges biztonsági funkció megvalósítása nem elérhető vagy veszélyeztetett.	-	-	-

8. Azonosítás és hitelesítés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	8.1. Szabályzat és eljárásrendek	8.1. A szervezet: 8.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 8.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési szabályzatot, amely 8.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 8.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal. 8.1.1.2. az azonosítási és hitelesítési eljárásrendet, amely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 8.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 8.1.3. Felülvizsgálja és frissíti az aktuális azonosítási és hitelesítési szabályzatot és az azonosítási és hitelesítési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	8.2. Azonosítás és hitelesítés	8.2. A szervezet egyedileg azonosítja és hitelesíti a felhasználókat, és egyedi azonosítóhoz kapcsolja a felhasználók által végzett tevékenységeket.	X	X	X
4.	8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	8.3. A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.	X	X	X
5.	8.4. Azonosítás és hitelesítés (felhasználók) – Nem-privilegizált fiókok többtényezős hitelesítése	8.4. A szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.	-	X	X
6.	8.5. Azonosítás és hitelesítés (felhasználók) – Egyéni azonosítás csoportos hitelesítéssel	8.5. Amikor a szervezet közös használatú fiókokat vagy hitelesítő eszközöket alkalmaz, akkor a felhasználókat egyénileg azonosítja, mielőtt hozzáférést biztosítana a közös használatú fiókokhoz vagy erőforrásokhoz.	-	-	X
7.	8.6. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – különálló eszköz	8.6. A szervezet többtényezős hitelesítést vezet be a privilegizált vagy nem privilegizált fiókokhoz való helyi, hálózati vagy távoli hozzáféréshez úgy, hogy: 8.6.1. az egyik tényezőt egy a rendszertől különálló eszköz biztosítja; 8.6.2. az eszköz megfelel a szervezet által meghatározott erősségű védelmi követelményeknek.	-	-	-
8.	8.7. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem	8.7. A szervezet visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált és a nem privilegizált fiókokhoz való hozzáféréshez.	X	X	X
9.	8.8. Azonosítás és hitelesítés (felhasználók) – Egyszeri bejelentkezés (SSO)	8.8. A szervezet biztosítja, hogy az egyszeri bejelentkezési képesség (SSO) rendelkezésre álljon a meghatározott rendszerfiókok és szolgáltatások számára.	-	-	-
10.	8.9. Azonosítás és hitelesítés (felhasználók) – Másodlagos hitelesítési csatorna	8.9. A szervezet másodlagos hitelesítési csatornát alkalmaz, az általa meghatározott feltételek fennállása esetén, a kért művelet vagy hitelesítés ellenőrzése érdekében.	-	-	-

11.	8.10. Eszközök azonosítása és hitelesítése	8.10. A szervezet egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköztípusokat, mielőtt helyi, távoli, hálózati vagy egyéb kapcsolatot létesítene velük.	-	X	X
12.	8.11. Eszközök azonosítása és hitelesítése – Kétirányú kriptográfiai hitelesítés	8.11. A szervezet hitelesíti a szervezet által meghatározott eszközöket vagy eszköztípusokat, mielőtt kétirányú kriptográfiai hitelesítéssel helyi vagy távoli hálózati, vagy egyéb kapcsolatot létesítene velük.	-	-	-
13.	8.12. Eszközök azonosítása és hitelesítése – Dinamikus címkiosztás	8.12. A szervezet: 8.12.1. dinamikus címkiosztás esetén standardizálja a meghatározott címkiosztással kapcsolatos információk tárolását és a bérleti időtartamot; valamint 8.12.2. ellenőrzi a címkiosztással kapcsolatos információkat a címek kiosztásakor.	-	-	-
14.	8.13. Eszközök azonosítása és hitelesítése – Eszköztanúsítványok	8.13. A szervezet az általa meghatározott konfigurációkezelési folyamatok mentén kezeli az eszközök azonosításához és hitelesítéséhez használt tanúsítványokat	-	-	-
15.	8.14. Azonosító kezelés	8.14. A szervezet: 8.14.1. Az egyéni, csoport, szerepkör vagy eszköz azonosítók kiosztását a szervezet által meghatározott személyek vagy szerepkörök engedélyéhez köti. 8.14.2. Kiválaszt egy azonosítót, amely azonosítja az egyént, csoportot, szerepkört, szolgáltatást vagy eszközt. 8.14.3. Hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz. 8.14.4. Meghatározott ideig megakadályozza az azonosítók újbóli felhasználását.	X	X	X
16.	8.15. Azonosító kezelés – Fiókazonosítók nyilvános azonosítóként való használatának tiltása	8.15. A szervezet megtiltja, hogy fiókok azonosítói megegyezzenek az egyéni fiókok nyilvánosan hozzáférhető azonosítóival.	-	-	-
17.	8.16. Azonosító kezelés – Felhasználói státusz azonosítása	8.16. A szervezet a felhasználói azonosítókhoz státuszjelölést rendel.	-	X	X
18.	8.17. Azonosító kezelés – Dinamikus kezelés	8.17. A szervezet dinamikusan kezeli az egyéni azonosítókat a meghatározott dinamikus azonosítókezelési szabályoknak megfelelően.	-	-	-
19.	8.18. Azonosító kezelés – Szervezetek közötti kezelés	8.18. A szervezet koordinálja a szervezetközi azonosítók használatát a meghatározott külső szervezetek esetében.	-	-	-
20.	8.19. Azonosító kezelés – Álnevesített azonosítók	8.19. A szervezet álnevesített (pszeudonim), nem újra felhasználható azonosítókat alkalmaz.	-	-	-
21.	8.20. Azonosító kezelés – Attribútumkarbantartás és -védelem	8.20. A szervezet megőrzi az egyedileg azonosított személyek, eszközök vagy szolgáltatások attribútumait egy meghatározott, védett központi tárhelyen.	-	-	-

22.	8.21. A hitelesítésre szolgáló eszközök kezelése	8.21. A szervezet a hitelesítő eszközöket az alábbiak szerint kezeli: 8.21.1. A kezdeti hitelesítő eszköz kiosztásának részeként ellenőrzi a hitelesítő eszközt megkapó egyén, csoport, szerepkör, szolgáltatás vagy eszköz identitását. 8.21.2. Meghatározza a szervezet által kiadott hitelesítő eszköz kezdeti tartalmát. 8.21.3. Biztosítja, hogy a hitelesítő eszközök a tervezett felhasználáshoz megfelelő erősségű mechanizmussal rendelkezzenek. 8.21.4. Adminisztratív eljárásokat alakít ki és hajt végre a kezdeti hitelesítő eszközök kiosztásához, az elveszett, kompromittált vagy sérült hitelesítő eszközökhöz, valamint a hitelesítő eszközök visszavonásához. 8.21.5. Gondoskodik a hitelesítő eszközök kezdeti tartalmának megváltoztatásáról az első használat előtt. 8.21.6. Gondoskodik a hitelesítő eszközök tartalmának megváltoztatásáról vagy frissítéséről meghatározott gyakorisággal, vagy amikor meghatározott események bekövetkeznek. 8.21.7. Megvédi a hitelesítő eszközök tartalmát az illetéktelen nyilvánosságra hozatal és módosítás ellen. 8.21.8. Megköveteli, hogy az egyének és eszközök konkrét védelmi intézkedéseket alkalmazzanak, illetve hajtsanak végre a hitelesítő eszközök védelme érdekében. 8.21.9. Megváltoztatja a csoporthoz vagy szerepkörhöz rendelt fiókok hitelesítő eszközeinek tartalmát, amikor a fiókokhoz tartozó tagok közül valaki eltávolításra kerül.	X	X	X
23.	8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés	8.22. A szervezet: 8.22.1. Fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti, továbbá minden olyan esetben, amikor a szervezeti jelszavakat közvetlenül vagy közvetett módon veszélyeztetik. 8.22.2. Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján. 8.22.3. A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja. 8.22.4. A jelszavakat egy jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva tárolja. 8.22.5. Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén. 8.22.6. Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a nyomtatható karaktereket. 8.22.7. Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában. 8.22.8. A jelszavakra a szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti.	X	X	X

24.	8.23. A hitelesítésre szolgáló eszközök kezelése – Nyilvános kulcs alapú hitelesítés	8.23.1. A nyilvános kulcs alapú hitelesítés esetén: 8.23.1.1. A szervezet biztosítja a megfelelő privát kulcshoz való jogosult hozzáférést. 8.23.1.2. A szervezet összekapcsolja a hitelesített azonosítót az egyén vagy csoport fiókjával. 8.23.1.2.1. Amikor a nyilvános kulcsú infrastruktúra (PKI) kerül felhasználásra: 8.23.1.3. Ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is. 8.23.1.4. Megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.	-	X	X
25.	8.24. A hitelesítésre szolgáló eszközök kezelése – Hitelesítők módosítása az átadás előtt	8.24. A szervezet a rendszerelemek fejlesztőit és telepítőit arra kötelezi, hogy egyedi hitelesítő adatokat biztosítsanak, vagy változtassák az alapértelmezett hitelesítő adatokat az átadás és telepítés előtt.	-	-	-
26.	8.25. A hitelesítésre szolgáló eszközök kezelése – A hitelesítő eszközök védelme	8.25. A szervezet a hitelesítő eszközöket az információk biztonsági besorolásának megfelelő védelemmel látja el, amelyekhez a hitelesítő eszköz a hozzáférést biztosítja.	-	X	X
27.	8.26. A hitelesítésre szolgáló eszközök kezelése – Nincsenek beágyazott titkosítatlan statikus hitelesítők	8.26. Az EIR biztosítja, hogy ne legyenek titkosítatlan, statikus hitelesítők beépítve az alkalmazásokba vagy más statikus tárolási formákba.	-	-	-
28.	8.27. A hitelesítésre szolgáló eszközök kezelése – Több rendszerbeli felhasználó fiókok	8.27. A szervezet biztonsági követelményeket határoz meg, hogy kezelje a több rendszerben is fiókkal rendelkező egyének általi kompromittálási kockázatot.	-	-	-
29.	8.28. A hitelesítésre szolgáló eszközök kezelése – Egyesített hitelesítő adatok kezelése	8.28. A szervezet meghatározza, hogy mely külső szervezetekkel kapcsolatban használható vagy engedélyezhető a hitelesítő adatok egyesítése.	-	-	-
30.	8.29. A hitelesítésre szolgáló eszközök kezelése – Dinamikus hitelesítési adatkapcsolat	8.29. A szervezet képes a felhasználói személyazonosságokat és a hitelesítő adatokat dinamikusan összekapcsolni a szervezeti szabályok alapján.	-	-	-
31.	8.30. A hitelesítésre szolgáló eszközök kezelése – Biometrikus hitelesítés hatékonysága	8.30. A szervezet olyan biometrikus hitelesítési mechanizmusokat alkalmaz, amelyek megfelelnek a biometrikus eszközökkel szemben meghatározott minőségi követelményeknek.	-	-	-
32.	8.31. A hitelesítésre szolgáló eszközök kezelése – A gyorsítótárban tárolt hitelesítők lejárata	8.31. A szervezet tiltja a gyorsítótárazott hitelesítési adatok meghatározottnál hosszabb idejű használatát.	-	-	-
33.	8.32. A hitelesítésre szolgáló eszközök kezelése – A megbízható PKI tanúsítványtárak kezelése	8.32. A szervezet a PKI-alapú hitelesítéshez egy szervezeti szintű módszertant alkalmaz, ami meghatározza a megbízható PKI tanúsítványtárak tartalmának kezelését minden platformon, beleértve a hálózatokat, operációs rendszereket, böngészőket és alkalmazásokat.	-	-	-
34.	8.33. A hitelesítésre szolgáló eszközök kezelése – Személyes jelenlét melletti vagy megbízható külső fél általi hitelesítőeszköz kibocsátás	8.33. A szervezet előírja, hogy a meghatározott típusú vagy különleges hitelesítőeszközök kiadása személyes jelenlét mellett vagy egy megbízható külső fél által történjen, a szervezet által meghatározott hitelesítés szolgáltató előtt, a szervezet által meghatározott személyek vagy szerepkörök jóváhagyása után.	-	-	-
35.	8.34. A hitelesítésre szolgáló eszközök kezelése – Hamis biometrikus adatokat felhasználó támadások	8.34. A szervezet biometrikus azonosításon alapuló hitelesítéseknél olyan mechanizmusokat alkalmaz, amelyek képesek a támadások - beleértve a hamis biometrikus adatok (például: ujjlenyomat, arckép) használatával elkövetett támadások - észlelésére.	-	-	-
36.	8.35. A hitelesítésre szolgáló eszközök kezelése – Jelszókezelők	8.35. A szervezet: 8.35.1. Meghatározott jelszókezelőt használ a jelszavak előállításához és kezeléséhez. 8.35.2. A jelszavakat a szervezet által meghatározott ellenőrző mechanizmusokkal védi.	-	-	-

37.	8.36. Hitelesítési információk visszajelzésének elrejtése	8.36. Az EIR fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt a jogosulatlan személyek általi felfedésétől és felhasználásától.	X	X	X
38.	8.37. Hitelesítés kriptográfiai modul esetén	8.37. Az EIR olyan mechanizmusokat alkalmaz a kriptográfiai modul hitelesítéséhez, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, szabályzatoknak, szabványoknak.	X	X	X
39.	8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	8.38. Az EIR egyedileg azonosítja és hitelesíti a szervezeten kívüli felhasználókat, tevékenységüket, valamint a nevükben futó folyamatokat.	X	X	X
40.	8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata	8.39. A szervezet meghatározott profilokat alkalmaz az azonosítási folyamat során.	X	X	X
41.	8.40. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – PKI alapú hitelesítő adatok elfogadása	8.40. A szervezet elfogadja és ellenőrzi a PKI hitelesítő adatokat, amelyek megfelelnek a szervezet által meghatározott előírásoknak.	-	-	-
42.	8.41. Szolgáltatás azonosítása és hitelesítése	8.41. A szervezet egyedileg azonosítja és hitelesíti a meghatározott rendszerszolgáltatásokat és alkalmazásokat, mielőtt kapcsolatot létesítene az eszközökkel, felhasználókkal, szolgáltatásokkal vagy alkalmazásokkal.	-	-	-
43.	8.42. Helyzetfüggő hitelesítés	8.42. A szervezet megköveteli, hogy a rendszerhez hozzáférő egyének meghatározott kiegészítő hitelesítési technikákat vagy eszközöket alkalmazzanak meghatározott konkrét körülmények vagy helyzetek esetén.	-	-	-
44.	8.43. Újrahitelesítés	8.43. A szervezet meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az újrahitelesítést.	X	X	X
45.	8.44. Személyazonosság igazolása	8.44. A szervezet: 8.44.1. Azonosítja azokat a felhasználókat, akiknek a rendszerekhez való logikai szintű hozzáféréshez olyan felhasználói fiókra van szükségük, ami teljesíti a vonatkozó szabványokban vagy irányelvekben meghatározott szintű, a személyazonosság bizonyítására vonatkozó követelményeket. 8.44.2. A felhasználói azonosítókat hozzárendeli egy egyedi személyhez 8.44.3. Összegyűjti, hitelesíti és ellenőrzi a személyazonosságot igazoló bizonyítékokat	-	X	X
46.	8.45. Személyazonosság igazolása – Felettes jóváhagyása	8.45. A szervezet előírja, hogy a logikai hozzáféréshez szükséges fiók regisztrációs folyamatában szerepeljen a felettes vagy a támogató (vezető) engedélye.	-	-	-
47.	8.46. Személyazonosság igazolása – Személyazonosság bizonyítéka	8.46. A szervezet megköveteli a személyazonosságot igazoló bizonyíték bemutatását a fiókok regisztrációját végző szervnél.	-	X	X
48.	8.47. Személyazonosság igazolása – Személyazonossági bizonyítékok hitelesítése és ellenőrzése	8.47. A szervezet megköveteli a bemutatott személyazonosságot igazoló bizonyíték meghatározott módszerekkel történő hitelesítését és ellenőrzését.	-	X	X
49.	8.48. Személyazonosság igazolása – Személyes jelenlét melletti hitelesítés és ellenőrzés	8.48. A szervezet megköveteli, hogy a személyazonosságot igazoló bizonyítékok hitelesítését és ellenőrzését személyes jelenlét mellett a fiókok regisztrációját végző szerv előtt kell elvégezni.	-	-	X
50.	8.49. Személyazonosság igazolása – Cím megerősítése	8.49. A szervezet megköveteli, hogy egy regisztrációs kód vagy megerősítő értesítés egy másodlagos csatornán keresztül kerüljön kézbesítésre, hogy a felhasználók nyilvántartásba vett (fizikai vagy elektronikus) címe ellenőrzésre kerüljön.	-	X	X
51.	8.50. Személyazonosság igazolása – Külsőleg hitelesített személyazonosság elfogadása	8.50. A szervezet elfogadja a külsőleg igazolt személyazonosságokat a szervezet által meghatározott személyazonosság megbízhatósági szinten.	-	-	-

9. Biztonsági események kezelése

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	9.1. Szabályzat és eljárásrendek	9.1. A szervezet: 9.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 9.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonsági eseménykezelési szabályzatot, amely 9.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 9.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 9.1.1.2. a biztonsági eseménykezelési eljárásrendet, amely a biztonsági eseménykezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 9.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonsági eseménykezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 9.1.3. Felülvizsgálja és frissíti az aktuális biztonsági eseménykezelési szabályzatot és a biztonsági eseménykezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	9.2. Képzés a biztonsági események kezelésére	9.2. A szervezet: 9.2.1. Biztonsági eseménykezelési képzést biztosít a felhasználóknak a rájuk bízott szerepek és felelősségek szerint: 9.2.1.1. A biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követően, illetve a rendszerhez való hozzáférés megszerzéstől számított meghatározott időn belül. 9.2.1.2. Amikor a rendszer változásai szükségessé teszik. 9.2.1.3. Ezt követően meghatározott gyakorisággal. 9.2.2. A szervezet meghatározott gyakorisággal, valamint meghatározott eseményeket követően felülvizsgálja és frissíti a biztonsági események kezelésére vonatkozó képzés tartalmát.	X	X	X
4.	9.3. Képzés a biztonsági események kezelésére – Szimulált események	9.3. A szervezet szimulált eseményeket épít be a biztonsági események kezelésére vonatkozó képzésbe, hogy elősegítse a személyzet számára a válsághelyzetekben szükséges reagálást.	-	-	X
5.	9.4. Képzés a biztonsági események kezelésére – Automatizált képzési környezet	9.4. A szervezet automatizált mechanizmusokat alkalmaz, hogy a biztonsági eseménykezelési képzéséhez valósághű környezetet biztosítson.	-	-	X
6.	9.5. Biztonsági események kezelésének tesztelése	9.5. A szervezet meghatározott módon és gyakorisággal teszteli a rendszerre vonatkozó biztonsági eseménykezelési képességek hatékonyságát.	-	X	X
7.	9.6. Biztonsági események kezelésének tesztelése – Automatizált tesztelés	9.6. A szervezet meghatározott automatizált eszközök használatával teszteli a biztonsági eseménykezelési képességét.	-	-	-
8.	9.7. Biztonsági események kezelésének tesztelése – Összehangolás a kapcsolódó tervekkel	9.7. A szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel.	-	X	X

9.	9.8. Biztonsági események kezelésének tesztelése – Folyamatos fejlesztés	9.8. A szervezet a tesztelés során keletkezett kvalitatív és kvantitatív adatokat felhasználva 9.8.1. megállapítja a biztonsági eseménykezelési folyamatok hatékonyságát; 9.8.2. folyamatosan fejleszti a biztonsági eseménykezelési folyamatokat; és 9.8.3. olyan biztonsági eseménykezelési intézkedéseket és mérőszámokat alkalmaz, amelyek pontosak, következetesek és reprodukálhatók.	-	-	-
10.	9.9. Biztonsági események kezelése	9.9.1. A szervezet: 9.9.2. Biztonsági eseménykezelési képességet alakít ki, amely összhangban van a biztonsági eseménykezelési tervvel, és magában foglalja a felkészülést, az észlelést és elemzést, az elszigetelést, a felszámolást és a helyreállítást. 9.9.3. A szervezet összehangolja a biztonsági eseménykezelési tevékenységeket az üzletmenet-folytonossági tervezési tevékenységekkel. 9.9.4. A szervezet beépíti a folyamatos biztonsági eseménykezelési tevékenységekből származó tanulságokat a biztonsági eseménykezelési eljárásokba, képzésbe és tesztelésbe. 9.9.5. A szervezet biztosítja, hogy a biztonsági eseménykezelési tevékenységek összehasonlíthatók és kiszámíthatók legyenek a szervezeten belül.	X	X	X
11.	9.10. Biztonsági események kezelése – Automatizált eseménykezelő folyamatok	9.10. A szervezet meghatározott automatizált mechanizmusok segítségével támogatja a biztonsági eseménykezelési folyamatot.	-	X	X
12.	9.11. Biztonsági események kezelése – Dinamikus újrakonfigurálás	9.11. A szervezet a meghatározott rendszerelemekhez kapcsolódó dinamikus újrakonfigurálási funkciót épít be a biztonsági eseményekre történő reagálási képességébe.	-	-	-
13.	9.12. Biztonsági események kezelése – Működés folytonossága	9.12. A szervezet a szervezeti célok teljesülésének és az üzleti funkciók folyamatosságának biztosítása érdekében osztályozza a biztonsági eseményeket, és az egyes osztályokhoz rendelt meghatározott válaszlépéseket hajtja végre a biztonsági eseményekre reagálva.	-	-	-
14.	9.13. Biztonsági események kezelése – Információk korrelációja	9.13. A szervezet korrelálja a biztonsági eseményekre vonatkozó információkat a szervezet egyéb releváns információival az átfogóbb helyzetfelismerés és -értékelés érdekében.	-	-	X
15.	9.14. Biztonsági események kezelése – Rendszer automatikus leállítása	9.14. A szervezet olyan konfigurálható képességet alkalmaz, amely automatikusan leállítja a rendszert a meghatározott biztonsági szabályok megsértésének észlelése esetén.	-	-	-
16.	9.15. Biztonsági események kezelése – Belső fenyegetések	9.15. A szervezet biztonsági eseménykezelési képességet alakít ki a belső fenyegetésekkel kapcsolatos eseményekre vonatkozóan.	-	-	-
17.	9.16. Biztonsági események kezelése – Belső fenyegetések – Szervezeten belüli együttműködés	9.16. A szervezet a meghatározott szervezeti egységek bevonásával koordinálja a belső fenyegetések kezelésére szolgáló biztonsági eseménykezelési képességet.	-	-	-
18.	9.17. Biztonsági események kezelése – Együttműködés külső szervezetekkel	9.17. A szervezet a kijelölt külső szervezetekkel együttműködve korrelálja és megosztja a biztonsági eseményekkel kapcsolatos információit, hogy átfogó képet kapjon a biztonsági eseményekről, és hatékonyabban tudjon reagálni rájuk.	-	-	-
19.	9.18. Biztonsági események kezelése – Dinamikus válaszadási képesség	9.18. A szervezet dinamikus reagálási képességeket alkalmaz a biztonsági események kezelésére.	-	-	-
20.	9.19. Biztonsági események kezelése – Ellátási lánc koordinációja	9.19. A szervezet összehangolja az ellátási láncban bekövetkező biztonsági események kezelését az ellátási láncban részt vevő szervezetekkel.	-	-	-
21.	9.20. Biztonsági események kezelése – Integrált eseménykezelő csoport	9.20. A szervezet létrehoz és fenntart egy integrált biztonsági eseménykezelő csoportot, amely a szervezet által meghatározott időn belül bármely kijelölt helyszínen bevethető.	-	-	X

22.	9.21. Biztonsági események kezelése – Kártékony kód és forenzikus vizsgálat	9.21. A szervezet elemzi a kártékony kódokat és minden más olyan nyomot, amelyek a biztonsági esemény után maradtak a rendszerben.	-	-	-
23.	9.22. Biztonsági események kezelése – Viselkedéselemzés	9.22. A szervezet elemzi a rendellenes vagy feltételezhetően rosszindulatú viselkedést, amely meghatározott környezettel vagy erőforrásokkal kapcsolatos.	-	-	-
24.	9.23. Biztonsági események kezelése – Biztonsági műveleti központ	9.23. A szervezet létrehoz és fenntart egy biztonsági műveleti központot.	-	-	-
25.	9.24. Biztonsági események kezelése – Szervezeti kapcsolatok és jóhírnév helyreállítása	9.24. A szervezet: 9.24.1. kezeli külső kapcsolatait egy bekövetkezett biztonsági eseményhez kötődően; és 9.24.2. lépéseket tesz a szervezet hírnevének helyreállítására.	-	-	-
26.	9.25. A biztonsági események nyomonkövetése	9.25. A szervezet nyomon követi és dokumentálja az EIR biztonsági eseményeit.	X	X	X
27.	9.26. A biztonsági események nyomonkövetése – Automatizált nyomon követés, adatgyűjtés és elemzés	9.26. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági események nyomonkövetésére, a biztonsági eseményekre vonatkozó információk gyűjtésére és vizsgálatára.	-	-	X
28.	9.27. A biztonsági események jelentése	9.27. A szervezet: 9.27.1. Kötelezi a személyzetet arra, hogy jelentse a biztonsági esemény gyanúját vagy bekövetkeztét. 9.27.2. Jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározott szervek felé.	X	X	X
29.	9.28. A biztonsági események jelentése – Automatizált jelentés	9.28. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági események bejelentésének támogatására.	-	X	X
30.	9.29. A biztonsági események jelentése – Eseményekkel kapcsolatos sérülékenységek	9.29. A szervezet megköveteli a biztonsági eseményekkel kapcsolatosan az EIR-ek sérülékenységeinek jelentését a szervezet által meghatározott személyeknek vagy szerepköröknek.	-	-	-
31.	9.30. A biztonsági események jelentése – Ellátási lánc koordinációja	9.30. A szervezet megosztja a biztonsági eseményekkel kapcsolatos információkat az érintett termék vagy szolgáltatás szállítójával, valamint más szervezetekkel, amelyek részt vesznek az érintett rendszerek vagy rendszerelemek ellátási láncában, vagy annak irányításában.	-	X	X
32.	9.31. Segítségnyújtás a biztonsági események kezeléséhez	9.31. A szervezet támogatást biztosít a biztonsági események kezeléséhez és jelentéséhez az EIR felhasználói számára.	X	X	X
33.	9.32. Segítségnyújtás biztonsági események kezeléséhez – Automatizált támogatás az információk és a támogatás elérhetőségéhez	9.32. A szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségét és a támogatást.	-	X	X
34.	9.33. Segítségnyújtás biztonsági események kezeléséhez – Külső szolgáltatókkal való koordináció	9.33. A szervezet: 9.33.1. biztosítja, hogy a biztonsági eseménykezelő tevékenység és a rendszer védelmi képességeinek külső szolgáltatói közötti kommunikáció hatékony és zökkenőmentes legyen; és 9.33.2. azonosítja a biztonsági eseménykezelő tevékenység szereplőit a külső szolgáltatók számára.	-	-	-

35.	9.34. Biztonsági eseménykezelési terv	9.34. A szervezet: 9.34.1. A hatályos jogszabályoknak megfelelően kidolgozza a biztonsági eseménykezelési tervet, amely: 9.34.1.1. A szervezet számára iránymutatást ad a biztonsági események kezelési módjaira. 9.34.1.2. Ismerteti a biztonsági eseménykezelés struktúráját és szervezetét. 9.34.1.3. Átfogó képet nyújt arról, hogy a biztonsági eseménykezelés hogyan illeszkedik az általános szervezeti struktúrába. 9.34.1.4. Kielégíti az adott szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit. 9.34.1.5. Meghatározza a bejelentésköteles biztonsági eseményeket. 9.34.1.6. Metrikákat alkalmaz a biztonsági eseménykezelési folyamatok működésének belső mérésére. 9.34.1.7. Meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési folyamatok bővítésére, hatékonyabbá tételére és fenntartására. 9.34.1.8. Meghatározza a biztonsági eseményekkel kapcsolatos információmegosztás módját. 9.34.1.9. Meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet, amelyet a szervezet által meghatározott személyek és szerepkörök jóváhagynak. 9.34.1.10. Meghatározza a biztonsági eseménykezelés felelőseit. 9.34.2. Kihirdeti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő személyek és szervezeti egységek számára. 9.34.3. Frissíti a biztonsági eseménykezelési tervet, figyelembe véve az EIR és a szervezet változásait, vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat. 9.34.4. Ismerteti a biztonsági eseménykezelési terv változásait a szervezet által meghatározott biztonsági eseménykezelésért felelős személyzettel. 9.34.5. Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.	X	X	X
36.	9.35. Információszivárgásra adott válaszlépések	9.35. A szervezet az információszivárgásra az alábbi válaszokat adja: 9.35.1. Meghatározza, hogy mely személyek vagy szerepkörök felelnek az ilyen események kezeléséért. 9.35.2. Azonosítja az információszivárgásban érintett konkrét adatokat. 9.35.3. Olyan kommunikációs csatornán keresztül értesíti az információszivárgásról a meghatározott személyeket vagy szerepköröket, amely nem köthető az információszivárgáshoz. 9.35.4. Elszigeteli a jogosulatlan adatkezelésben érintett rendszert vagy rendszerelemet. 9.35.5. Eltávolítja az információkat a jogosulatlan adatkezelésben érintett rendszerből vagy rendszerelemből. 9.35.6. Azonosítja azokat a további rendszereket vagy rendszerelemeket, amelyek érintettek lehetnek a jogosulatlan adatkezelésben. 9.35.7. Végrehajtja a szervezet által meghatározott további intézkedéseket.	-	-	-
37.	9.36. Információszivárgásra adott válaszlépések – Képzés	9.36. A szervezet meghatározott gyakorisággal megtartja az információszivárgási események kezelésére vonatkozó képzést.	-	-	-

38.	9.37. Információszivárgásra adott válaszlépések – Szivárgást követő műveletek	9.37. A szervezet meghatározott intézkedéseket hajt végre annak érdekében, hogy az információszivárgásban érintett szervezethez köthető személyek folyamatosan el tudják látni kijelölt feladatukat, amíg az információszivárgásban érintett rendszereken javító intézkedések folynak.	-	-	-
39.	9.38. Információszivárgásra adott válaszlépések – Illetéktelen hozzáférés	9.38. A szervezet meghatározott intézkedéseket alkalmaz azokkal a személyekkel szemben, akik olyan információkhoz férnek hozzá, amelyek kívül esnek hozzáférési jogosultságaikon.	-	-	-

10. Karbantartás

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	10.1. Szabályzat és eljárásrendek	10.1. A szervezet: 10.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 10.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó karbantartási szabályzatot, amely 10.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 10.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 10.1.1.2. a karbantartási eljárásrendet, amely a karbantartási szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 10.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a karbantartási szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 10.1.3. Felülvizsgálja és frissíti az aktuális karbantartási szabályzatot és a karbantartási eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	10.2. Szabályozott karbantartás	10.2. A szervezet: 10.2.1. Ütemezi, dokumentálja és felülvizsgálja a rendszerelemek karbantartásának, javításának és cseréjének nyilvántartásait a gyártó vagy szállító specifikációi és a szervezeti követelmények szerint. 10.2.2. Jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik-e, és hogy a rendszert vagy a rendszerelemeket a helyszínen szervizelik-e, vagy más helyszínre szállítják. 10.2.3. Megköveteli, hogy a szervezet által meghatározott személyek vagy szerepkörök egyedileg jóváhagyják a rendszer vagy a rendszerelemek szervezeti létesítményekből történő elszállítását külső karbantartás, javítás vagy csere céljából. 10.2.4. Biztonságosan törli a szervezet által meghatározott besorolású információkat a hozzájuk kapcsolódó adathordozókról, mielőtt azokat a szervezeti létesítményeiből külső karbantartás, javítás vagy csere céljából elszállítanák. 10.2.5. Ellenőrzi a védelmi intézkedések megfelelő működését a karbantartás, javítás vagy csere után. 10.2.6. Rögzíti a szervezet által meghatározott információkat a szervezeti karbantartási nyilvántartásokba.	X	X	X
4.	10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek	10.3.1. A szervezet automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására. 10.3.2. Naprakész, pontos és teljes nyilvántartást vezet minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási tevékenységről.	-	-	X

5.	10.4. Karbantartási eszközök	10.4. A szervezet: 10.4.1. Jóváhagyja, nyilvántartásba veszi és ellenőrzi az EIR-hez kapcsolódó karbantartási eszközöket. 10.4.2. A nyilvántartásokat a szervezet az általa meghatározott időközönként felülvizsgálja.	-	X	X
6.	10.5. Karbantartási eszközök – Eszközök vizsgálata	10.5. A szervezet ellenőrzi a karbantartó személyzet által használt eszközöket, a nem megfelelő, vagy nem engedélyezett módosítások észlelése érdekében.	-	X	X
7.	10.6. Karbantartási eszközök – Adathordozók vizsgálata	10.6. A szervezet az EIR-ben történő felhasználást megelőzően ellenőrizi a diagnosztikai és tesztprogramok adathordozóit, hogy tartalmaznak-e kártékony kódot.	-	X	X
8.	10.7. Karbantartási eszközök – Jogosulatlan elszállítás megakadályozása	10.7. A szervezet megakadályozza a szervezeti információkat tartalmazó karbantartó eszközök elszállítását az alábbiak szerint: 10.7.1. Ellenőrzi, hogy a berendezésen van-e szervezeti információ. 10.7.2. Megsemmisíti a berendezést vagy biztonságosan törli annak tartalmát. 10.7.3. A berendezést a létesítményben tartja és megőrzi; 10.7.4. kivéve, ha a szervezet által meghatározott személyek vagy szerepkörök egyike kifejezetten engedélyezi a berendezésnek a létesítményből történő elszállítását.	-	X	X
9.	10.8. Karbantartási eszközök – Korlátozott eszközhasználat	10.8. A szervezet a karbantartási eszközök használatát csak a megfelelő engedéllyel rendelkező személyek számára teszi lehetővé.	-	-	-
10.	10.9. Karbantartási eszközök – Privilegizált jogosultsággal való futtatás	10.9. A szervezet monitorozza a privilegizált jogosultsággal futtatott karbantartási eszközök használatát.	-	-	-
11.	10.10. Karbantartási eszközök – Szoftverfrissítések és javítások	10.10. A szervezet ellenőrzi a karbantartási eszközöket, hogy megbizonyosodjon arról, hogy azokon a legújabb szoftverfrissítések és javítások telepítésre kerültek.	-	-	-
12.	10.11. Távoli karbantartás	10.11. A szervezet: 10.11.1. Jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket. 10.11.2. Csak akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, amennyiben az összhangban áll a szervezeti szabályokkal és az EIR rendszerbiztonsági tervében dokumentált. 10.11.3. Erős hitelesítési eljárásokat alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásakor. 10.11.4. Nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről. 10.11.5. Lezárja a munkaszakaszokat és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.	X	X	X
13.	10.12. Távoli karbantartás – Naplózás és felülvizsgálat	10.12. A szervezet: 10.12.1. Naplózza azokat a távoli karbantartási és diagnosztikai munkaszakaszokat, amelyeket a szervezet meghatározott naplózási eseményként definiál. 10.12.2. felülvizsgálja és elemzi a karbantartási és diagnosztikai munkaszakaszok naplóbejegyzéseit, a rendellenességek észlelése céljából.	-	-	-
14.	10.13. Távoli karbantartás – Azonos szintű biztonság és adattörlés	10.13. A szervezet: 10.13.1. megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan EIR-ből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a karbantartott rendszer biztonsági képességeivel, vagy amennyiben ez nem biztosított, 10.13.2. megköveteli, hogy a karbantartandó elemet az EIR-ből eltávolítsák, a karbantartást megelőzően minden szervezeti információt biztonságosan töröljenek az érintett rendszerelemről. A karbantartási folyamat végrehajtását követően az érintett elemet átvizsgálják a potenciálisan kártékony szoftverek észlelése érdekében, mielőtt az EIR-hez csatlakoztatnák.	-	-	X

15.	10.14. Távoli karbantartás – Hitelesítés és a karbantartási munkaszakaszok szétválasztása	10.14. A szervezet az alábbi intézkedésekkel védi a munkaszakaszokat a távoli karbantartás során: 10.14.1. Olyan hitelesítő eszközöket kell alkalmazni, amelyek ellenállnak a visszajátszásos támadásoknak. 10.14.2. A karbantartási munkaszakaszok el kell különíteni a rendszer többi hálózati munkaszakaszától a következő módokon: 10.14.2.1. Fizikailag elkülönített kommunikációs útvonalak használatával; vagy 10.14.2.2. logikailag elkülönített kommunikációs útvonalak használatával.	-	-	-
16.	10.15. Távoli karbantartás – Jóváhagyások és értesítések	10.15. A szervezet: 10.15.1. megköveteli a minden távoli karbantartási munkaszakasz meghatározott személyek vagy szerepkörök által történő jóváhagyását, és 10.15.2. értesíti a meghatározott személyeket vagy szerepköröket a tervezett távoli karbantartás időpontjáról.	-	-	-
17.	10.16. Távoli karbantartás – Kriptográfiai védelem	10.16. A szervezet meghatározott kriptográfiai mechanizmusokat alkalmaz a távoli karbantartási és diagnosztikai tevékenységhez használt kommunikáció sértetlenségének és bizalmasságának védelme érdekében.	-	-	-
18.	10.17. Távoli karbantartás – Kapcsolat megszakításának megerősítése	10.17. A szervezet ellenőrzi a munkaszakaszok és a hálózati kapcsolatok megszűnését a távoli karbantartási és diagnosztikai munkaszakasz befejezése után.	-	-	-
19.	10.18. Karbantartó személyek	10.18. A szervezet: 10.18.1. Kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére, és nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó szervezetekről vagy személyekről. 10.18.2. Ellenőrzi az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait. 10.18.3. Kijelöli a szervezethez tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyeket arra, hogy felügyeljék a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.	X	X	X
20.	10.19. Karbantartó személyek – Nem megfelelő ellenőrzöttségű személyek	10.19. A szervezet: 10.19.1. Eljárásokat dolgoz ki a nem megfelelő biztonsági ellenőrzöttségű karbantartó személyzet tevékenységének szabályozására. 10.19.1.1. Azokat a karbantartó személyeket, akik nem rendelkeznek a szükséges hozzáférési jogosultságokkal, a szervezet által jóváhagyott, megfelelő hozzáférési jogosultsággal és szaktudással rendelkező személyek kísérik és felügyelik őket a karbantartási és diagnosztikai tevékenységek során. 10.19.1.2. A karbantartási és diagnosztikai tevékenységek megkezdése előtt minden volatilis adattároló eszközt biztonságosan töröl, a nem volatilis eszközök esetében gondoskodik az adattároló eltávolításáról vagy fizikailag leválasztja a rendszerről. 10.19.2. Alternatív biztonsági folyamatot alakít ki arra az esetre, ha egy rendszerelemet nem lehet törölni, eltávolítani vagy a rendszerről leválasztani.	-	-	X
21.	10.20. Karbantartó személyek – Nem rendszer karbantartás	10.20. A szervezet biztosítja, hogy a rendszerhez közvetlenül nem kapcsolódó, de a rendszer fizikai közelében tartózkodó, kísérettel nem rendelkező karbantartási tevékenységeket végző személyzet rendelkezzen a szükséges hozzáférési engedélyekkel.	-	-	-
22.	10.21. Kellő időben történő karbantartás	10.21. A szervezet meghatározza, hogy mely rendszerelemek esetén, milyen időtartamon belül szükséges karbantartási támogatást vagy pótalkatrészt biztosítani hiba esetén.	-	X	X
23.	10.22. Kellő időben történő karbantartás – Megelőző karbantartás	10.22. A szervezet meghatározott gyakorisággal megelőző karbantartást végez a kijelölt rendszerelemeken.	-	-	-

24.	10.23. Kellő időben történő karbantartás – Prediktív karbantartás	10.23. A szervezet meghatározott gyakorisággal prediktív karbantartást végez a kijelölt rendszerelemeken.	-	-	-
25.	10.24. Kellő időben történő karbantartás – Prediktív karbantartás automatizált támogatása	10.24. A szervezet meghatározott automatizált mechanizmusok segítségével végzi el a prediktív karbantartási adatok átvitelét egy karbantartáskezelő rendszerbe.	-	-	-
26.	10.25. Terepi karbantartás szabályozása	10.25. A szervezet korlátozza vagy megtiltja a meghatározott EIR-ek vagy rendszerelemek terepen végzett karbantartását, vagy azt kizárólag a meghatározott, megbízható karbantartó létesítményekben engedélyezi.	-	-	-

11. Adathordozók védelme

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	11.1. Szabályzat és eljárásrendek	11.1. A szervezet: 11.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 11.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó adathordozók védelmére vonatkozó szabályzatot, amely 11.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 11.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 11.1.1.2. az adathordozók védelmére vonatkozó eljárásrendet, amely az adathordozók védelmére vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 11.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az adathordozók védelmére vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 11.1.3. Felülvizsgálja és frissíti az aktuális, adathordozók védelmére vonatkozó szabályzatot és az adathordozók védelmére vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	11.2. Hozzáférés az adathordozókhoz	11.2. A szervezet korlátozza a hozzáférést a meghatározott digitális vagy analóg adathordozókhoz, és ezt a hozzáférést kizárólag a szervezet által meghatározott személyek vagy szerepkörök számára engedélyezi.	X	X	X
4.	11.3. Adathordozók címkézése	11.3. A szervezet: 11.3.1. Megjelöli az EIR adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket. 11.3.2. Mentesíti a meghatározott adathordozótípusokat a jelölési kötelezettség alól, ha az adathordozók a szervezet által meghatározott ellenőrzött területeken belül maradnak.	-	X	X
5.	11.4. Adathordozók tárolása	11.4. A szervezet: 11.4.1. Fizikailag ellenőrzi és biztonságosan tárolja mind a digitális, mind az analóg adathordozókat az arra engedélyezett vagy kijelölt helyen. 11.4.2. Védi az EIR adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy a rajtuk tárolt adatot biztonságosan nem törlik.	-	X	X
6.	11.5. Adathordozók tárolása – Automatizált korlátozott hozzáférés	11.5. A szervezet korlátozza a hozzáférést az adathordozókat tároló ellenőrzött területekhez, valamint a szervezet által meghatározott automatizált mechanizmusok segítségével naplózza a hozzáféréseket és a hozzáférési kísérleteket.	-	-	-

7.	11.6. Adathordozók szállítása	11.6. A szervezet: 11.6.1. A szervezet által meghatározott védelmi intézkedéssel védi és ellenőrzi az adathordozókat az ellenőrzött területen kívülre történő szállítás alatt. 11.6.2. Biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás alatt. 11.6.3. Dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket. 11.6.4. A jogosult személyekre korlátozza az adathordozók szállításával kapcsolatos tevékenységeket.	-	X	X
8.	11.7. Adathordozók szállítása – Kijelölt felelős	11.7. A szervezet egy felügyeleti feladattal megbízott személyt jelöl ki az adathordozók ellenőrzött területeken kívüli szállítása során.	-	-	-
9.	11.8. Adathordozók törlése	11.8. A szervezet: 11.8.1. A meghatározott, biztonságos törlési technikákkal és eljárásokkal törli az EIR meghatározott adathordozóit a leselejtezés, a szervezet ellenőrzési körén kívülre kerülés, vagy az újra felhasználásra való kibocsátás előtt. 11.8.2. A törlési mechanizmusokat az információ biztonsági besorolásával és sértetlenségi követelményével arányosan választja ki és alkalmazza.	X	X	X
10.	11.9. Adathordozók törlése – Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	11.9. A szervezet felülvizsgálja, jóváhagyja, nyomonköveti, dokumentálja és ellenőrzi az adathordozók biztonságos törlésével és megsemmisítésével kapcsolatos tevékenységeket.	-	-	X
11.	11.10. Adathordozók törlése – Berendezés tesztelése	11.10. A szervezet a biztonságos törléshez alkalmazott eszközöket és eljárásokat a szervezet által meghatározott időközönként teszteli.	-	-	X
12.	11.11. Adathordozók törlése – Roncsolásmentes technikák	11.11. A szervezet roncsolásmentes adattörlési technikákat alkalmaz a meghatározott hordozható tárolóeszközökön, mielőtt azokat a szervezet által meghatározott körülmények között csatlakoztatná a rendszerhez.	-	-	X
13.	11.12. Adathordozók törlése – Kettős jóváhagyás	11.12. A szervezet kettős jóváhagyáshoz köti a meghatározott EIR adathordozóinak biztonságos törlését.	-	-	-
14.	11.13. Adathordozók törlése – Adatok távoli törlése vagy megsemmisítése	11.13. A szervezet kialakítja a képességet a távoli információtörlésre vagy felülírásra a meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott feltételek teljesülése mellett.	-	-	-
15.	11.14. Adathordozók használata	11.14. A szervezet: 11.14.1. Korlátozza vagy tiltja a szervezet által meghatározott típusú adathordozók használatát a szervezet által meghatározott EIR-eken vagy rendszerelemeken, a szervezet által meghatározott irányítási mechanizmusok alkalmazásával. 11.14.2. Megtiltja a hordozható adattároló eszközök használatát a szervezeti EIR-ekben, ha azoknak nincs azonosítható tulajdonosa.	X	X	X
16.	11.15. Adathordozók használata – Biztonságos törlésnek ellenálló adathordozók használatának tiltása	11.15. A szervezet megtiltja a biztonságos törlésnek ellenálló adathordozók használatát a szervezeti EIR-ekben.	-	-	-
17.	11.16. Adathordozók visszaminősítése	11.16. A szervezet: 11.16.1. Létrehoz egy, a szervezet által meghatározott adathordozó-visszaminősítési folyamatot, amely magában foglalja a törlendő információ biztonsági besorolásának megfelelő szintű mechanizmusok alkalmazását. 11.16.2. Ellenőrzi, hogy az adathordozó-visszaminősítési folyamat megfelel-e az eltávolítandó információ biztonsági besorolásának, valamint az információt potenciálisan átvevők hozzáférési jogosultságainak. 11.16.3. Azonosítja a visszaminősítést igénylő adathordozókat. 11.16.4. Meghatározott folyamat segítségével visszaminősíti az azonosított adathordozókat.	-	-	-

18.	11.17. Adathordozók visszaminősítése – Folyamat dokumentációja	11.17. A szervezet a szervezet által meghatározott gyakorisággal teszteli a visszaminősítés során használatos eszközöket és eljárásokat, hogy biztosítsa a visszaminősítési műveletek sikeres végrehajtását.	-	-	-
19.	11.18. Adathordozók visszaminősítése – Berendezés tesztelése	11.18. A szervezet a szervezet által meghatározott gyakorisággal teszteli a visszaminősítés során használatos eszközöket és eljárásokat, hogy biztosítsa a visszaminősítési műveletek sikeres végrehajtását.	-	-	-

12. Fizikai és környezeti védelem

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	12.1. Szabályzat és eljárásrendek	12.1. A szervezet: 12.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 12.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó fizikai védelmi szabályzatot, amely 12.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 12.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 12.1.1.2. a fizikai és környezeti védelemre vonatkozó eljárásrendet, amely a fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 12.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a fizikai védelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 12.1.3. Felülvizsgálja és frissíti az aktuális fizikai védelmi szabályzatot és a fizikai és környezeti védelemre vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	12.2. A fizikai belépési engedélyek	12.2. A szervezet 12.2.1. Összeállítja, jóváhagyja és kezeli az EIR-eknek helyet adó létesítményekbe belépésre jogosultak listáját. 12.2.2. Belépési jogosultságot igazoló dokumentumokat, hitelesítő eszközöket (például: kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépni szándékozó részére. 12.2.3. A szervezeti előírások szerinti gyakorisággal rendszeresen felülvizsgálja a belépésre jogosult személyek listáját. 12.2.4. Eltávolítja a belépésre jogosult személyek listájáról azokat, akik már nem jogosultak a belépésre.	X	X	X
4.	12.3. Fizikai belépési engedélyek – Szerep- vagy feladatkör alapú hozzáférés	12.3. A szervezet szerepkör vagy beosztás alapján engedélyezi a fizikai belépést az EIR-nek helyet adó létesítménybe.	-	-	-
5.	12.4. Fizikai belépési engedélyek – Kétféle azonosító megléte	12.4. A szervezet előírja, hogy a látogatóknak kétféle, a szervezet által meghatározott és elfogadott azonosító okmányt kell bemutatniuk az EIR-nek helyet adó létesítménybe történő belépéshez. A szervezet határozza meg az általa elfogadhatónak ítélt azonosító okmányok listáját.	-	-	-
6.	12.5. Fizikai belépési engedélyek – Kíséret nélküli hozzáférés korlátozása	12.5. A szervezet a szükséges biztonsági ellenőrzéssel és hozzáférési jogosultsággal rendelkező személyzetre korlátozza a kíséret nélküli fizikai belépést az EIR-nek helyet adó létesítmény területére.	-	-	-

7.	12.6. A fizikai belépés ellenőrzése	12.6. A szervezet: 12.6.1. Kizárólag a szervezet által meghatározott be- és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést. 12.6.1.1. Ellenőrzi az egyéni jogosultságokat a létesítménybe való belépés előtt. 12.6.1.2. Ellenőrzi a létesítménybe való be- és kilépést a meghatározott fizikai beléptető rendszerek vagy eszközök illetve őrök segítségével. 12.6.2. Naplózza a fizikai be- illetve kilépéseket. 12.6.3. Ellenőrzés alatt tartja a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket. 12.6.4. Kíséri a létesítménybe ad hoc belépésre jogosultakat, és figyelemmel követi a tevékenységüket. 12.6.5. Megóvja a kulcsokat, hozzáférési kódokat és az egyéb fizikai hozzáférést biztosító eszközöket. 12.6.6. Nyilvántartást vezet a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissíti azt. 12.6.7. Meghatározott rendszerességgel megváltoztatja a hozzáférési kódokat és kulcsokat, illetve ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát.	X	X	X
8.	12.7. A fizikai belépés ellenőrzése – Rendszer hozzáférés	12.7. A szervezet a létesítménybe történő fizikai belépés ellenőrzésén túlmenően külön engedélyhez köti a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak.	-	-	X
9.	12.8. A fizikai belépés ellenőrzése – Létesítmény és rendszerek	12.8. A szervezet meghatározott gyakorisággal biztonsági ellenőrzéseket végez a létesítmény vagy rendszer fizikai határain annak érdekében, hogy megakadályozza az információk kiszivárogtatását vagy a rendszerelemek eltávolítását.	-	-	-
10.	12.9. A fizikai belépés ellenőrzése – Folyamatos élőerős felügyelet	12.9. A szervezet az EIR-nek helyet adó létesítménynek meghatározott fizikai hozzáférési pontjain 24 órás őrszolgálatot biztosít a hét minden napján.	-	-	-
11.	12.10. A fizikai belépés ellenőrzése – Zárható házak vagy burkolatok	12.10. A szervezet a meghatározott rendszerelemek védelmében zárható fizikai házat vagy egyéb burkolatot alkalmaz a jogosulatlan fizikai hozzáférés megakadályozására.	-	-	-
12.	12.11. A fizikai belépés ellenőrzése – Manipuláció elleni védelem	12.11. A szervezet meghatározott manipuláció elleni technológiákat alkalmaz a fizikai beavatkozások vagy módosítások észlelésének és megakadályozásának érdekében a szervezet által meghatározott rendszerelemeken.	-	-	-
13.	12.12. A fizikai belépés ellenőrzése – Fizikai akadályok	12.12. A szervezet fizikai akadályok használatával korlátozza a különböző területekhez való hozzáférést.	-	-	-
14.	12.13. A fizikai belépés ellenőrzése – Beléptető helyiségek	12.13. A szervezet hozzáférés-ellenőrző előtereket használ az általa meghatározott helyszíneken a létesítményeken belül.	-	-	-
15.	12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	12.14. A szervezet meghatározott biztonsági követelményeket alkalmaz a fizikai hozzáférés szabályozására a saját létesítményeiben található meghatározott rendszerelosztókhoz (például: csatlakozók, elosztók) és átviteli vezetékekhez.	-	X	X
16.	12.15. A kimeneti eszközök hozzáférés-ellenőrzése	12.15. A szervezet ellenőrzi az EIR kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek hozzá az előállított kimenetekhez.	-	X	X
17.	12.16. A kimeneti eszközök hozzáférés-ellenőrzése – Személyazonossághoz kapcsolhatóság	12.16. A szervezet a kimeneti eszközökből származó információk fogadását vagy átvételét a fogadó vagy átvevő személy azonosításhoz köti.	-	-	-

18.	12.17. A fizikai hozzáférések felügyelete	12.17. A szervezet: 12.17.1. Ellenőrzi a fizikai hozzáféréseket az EIR-eket tartalmazó létesítményekben, hogy észlelje a fizikai biztonsági eseményeket és reagáljon rájuk. 12.17.2. Rendszeresen átvizsgálja a fizikai hozzáférések naplóit, és azonnal áttekinti azokat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak. 12.17.3. Összehangolja az ellenőrzések, vizsgálatok eredményeit a szervezet eseménykezelési képességével.	X	X	X
19.	12.18. A fizikai hozzáférések felügyelete – Behatolásjelző és megfigyelő berendezések	12.18. A szervezet fizikai behatolásjelző és felügyeleti berendezések alkalmazásával ellenőrzi a fizikai hozzáférési pontokat az EIR-nek helyet adó létesítményekben.	-	X	X
20.	12.19. A fizikai hozzáférések felügyelete – Automatizált betörés felismerés válaszadás	12.19. A szervezet képes felismerni a szervezet által meghatározott típusú behatolásokat, és a szervezet által meghatározott válaszintézkedések meghozatalát kezdeményezi a szervezet által meghatározott automatizált mechanizmusok használatával.	-	-	-
21.	12.20. A fizikai hozzáférések felügyelete – Kamerás megfigyelés	12.20. A szervezet: 12.20.1. Meghatározott működési területeken videómegfigyelést alkalmaz. 12.20.2. Meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet, amelyet a szervezet által meghatározott személyek és szerepkörök jóváhagynak. 12.20.3. Meghatározott időtartamig megőrzi a videófelvételeket.	-	-	-
22.	12.21. A fizikai hozzáférések felügyelete – Rendszerekhez való fizikai hozzáférés-ellenőrzése	12.21. A szervezet a létesítménybe történő fizikai belépések ellenőrzésén túl külön figyelmet fordít az EIR egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépésekre.	-	-	X
23.	12.22. Látogatói hozzáférési naplók	12.22. A szervezet: 12.22.1. Meghatározott ideig megőrzi az EIR-eknek helyet adó létesítményekbe történt látogatói belépésekről szóló információkat. 12.22.2. Meghatározott gyakorisággal felülvizsgálja a látogatói belépésekről szóló nyilvántartást. 12.22.3. A látogatói belépésekről szóló nyilvántartásban észlelt rendellenességeket azonnal jelenti a meghatározott személynek vagy szerepkörnek.	X	X	X
24.	12.23. Látogatói hozzáférési naplók – Nyilvántartások automatizált karbantartása és felülvizsgálata	12.23. A szervezet automatizált eszközöket alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez és átvizsgálásához.	-	-	X
25.	12.24. Áramellátó berendezések és kábelezés	12.24. A szervezet védi az EIR áramellátását biztosító berendezéseket és a kábelezést a sérülésektől és rongálásoktól.	-	X	X
26.	12.25. Áramellátó berendezések és kábelezés – Redundáns kábelezés	12.25. A szervezet redundáns tápellátó kábelútvonalakat alkalmaz, amelyeket egymástól meghatározott távolságra helyez el.	-	-	-
27.	12.26. Áramellátó berendezések és kábelezés – Automatikus feszültségszabályozás	12.26. A szervezet automatikus feszültségszabályozót alkalmaz a meghatározott EIR és a szervezet működése szempontjából kritikus rendszerelemeknél.	-	-	-
28.	12.27. Vészkikapcsolás	12.27. A szervezet: 12.27.1. Lehetőséget biztosít az EIR vagy egyedi rendszerelemek áramellátásának kikapcsolására vészhelyzetben. 12.27.2. Gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről az arra jogosult személyek számára. 12.27.3. Megakadályozza a jogosulatlan vészkikapcsolást.	-	X	X
29.	12.28. Vészhelyzeti tápellátás	12.28. A szervezet az elsődleges áramforrás kiesése esetén, a tevékenységéhez méretezett szünetmentes áramellátást biztosít az EIR szabályos leállításához, vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.	-	X	X

30.	12.29. Vészhelyzeti tápellátás – Tartalék áramellátás – Minimális működési képesség	12.29. A szervezet az elsődleges áramforrás kiesése esetén automatikus vagy manuális aktiválású hosszútávú alternatív áramellátást biztosít az EIR minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.	-	-	X
31.	12.30. Vészhelyzeti tápellátás – Tartalék áramellátás – Önellátás	12.30. A szervezet automatikusan vagy kézzel aktiválható alternatív áramellátást biztosít az EIR számára, amely: 12.30.1. önálló; 12.30.2. nem függ a hálózati áramellátástól; 12.30.3. képes fenntartani a minimálisan szükséges működési képességet vagy a teljes működési képességet az elsődleges áramforrás hosszabb ideig tartó kiesése esetén.	-	-	-
32.	12.31. Vészvilágítás	12.31. A szervezet alkalmaz és karbantart egy automatikus vészvilágítási rendszert a létesítményben, amely áramszünet esetén aktiválódik, és megvilágítja a vészkijáratokat és a menekülési útvonalakat.	X	X	X
33.	12.32. Vészvilágítás – Alapvető üzleti (ügymeneti) funkciók	12.32. A szervezet biztosítja a vészvilágítást a létesítményen belül minden olyan területen, amely támogatja az üzleti funkciókat.	-	-	-
34.	12.33. Tűzvédelem	12.33. A szervezet független energiaforrással rendelkező tűzérzékelő, illetve tűzoltó rendszereket tart fenn és alkalmaz az EIR-ek védelme érdekében.	X	X	X
35.	12.34. Tűzvédelem – Érzékelőrendszerek – Automatikus élesítés és értesítés	12.34. A szervezet az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a szervezet által kijelölt tűzvédelmi felelősnek.	-	X	X
36.	12.35. Tűzvédelem – Tűzoltó berendezések – Automatikus élesítés és értesítés	12.35. A szervezet: 12.35.1. Az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a szervezet által kijelölt tűzvédelmi felelősnek. 12.35.2. Automatikus tűzoltó berendezést alkalmaz, ha a létesítményben nincs állandó személyzet.	-	-	X
37.	12.36. Tűzvédelem – Hatósági ellenőrzések	12.36. A szervezet biztosítja, hogy a létesítményt a jogszabályi előírásoknak megfelelő ellenőrök a vonatkozó jogszabályok szerint és a szervezet által meghatározott gyakorisággal tűzvédelmi ellenőrzésnek vessék alá, és az azonosított hiányosságokat a vonatkozó jogszabályok és a szervezet által meghatározott időn belül orvosolják.	-	-	-
38.	12.37. Környezeti védelmi intézkedések	12.37. A szervezet: 12.37.1. Meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és a sugárzást az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (például: adatközpont, szerver szoba, központi gépterem). 12.37.2. Felügyeli a környezeti szabályozási szinteket a szervezet által meghatározott gyakorisággal	X	X	X
39.	12.38. Környezeti védelmi intézkedések – Automatikus szabályozás	12.38. A szervezet automatizált környezeti szabályozó eszközöket alkalmaz a létesítményben, hogy megakadályozza azokat az ingadozásokat, amelyek potenciálisan károsak lehetnek az EIR-re nézve.	-	-	-
40.	12.39. Környezeti védelmi intézkedések – Felügyeleti riasztások és értesítések	12.39. Az adott szervezet egy olyan biztonsági rendszert használ, amely figyelmezteti a kijelölt személyeket vagy szerepeket, ha olyan változások történnek, amelyek potenciálisan veszélyeztethetik az embereket vagy a berendezéseket.	-	-	-
41.	12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	12.40. Védi az EIR-t a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetők és működőképesek, valamint a nélkülözhetetlen szerepköröket betöltő személyek számára ismertek legyenek.	X	X	X

42.	12.41. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem – Automatizálás támogatása	12.41. A szervezet automatizált mechanizmusokat alkalmaz az EIR közelében megjelenő folyadékszivárgás észlelésére, valamint a szervezet által kijelölt személyek riasztására.	-	-	X
43.	12.42. Be- és kiszállítás	12.42. A szervezet 12.42.1. Engedélyezi és felügyeli a szervezet által meghatározott típusú rendszerelemek létesítménybe történő beszállítását és kiszállítását a létesítményből; és 12.42.2. nyilvántartást vezet ezekről.	X	X	X
44.	12.43. Munkavégzésre kijelölt alternatív helyszín	12.43. A szervezet: 12.43.1. meghatározza és dokumentálja az alternatív munkavégzési helyeket a munkavállalók számára; 12.43.2. meghatározza a védelmi intézkedéseket az alternatív munkavégzési helyeken; 12.43.3. értékeli a védelmi intézkedések hatékonyságát az alternatív munkavégzési helyeken; 12.43.4. biztosítja a szükséges eszközöket a munkavállalók számára, hogy egy biztonsági esemény bekövetkezése esetén kommunikálni tudjanak az információbiztonságért felelős személyekkel.	-	X	X
45.	12.44. Az elektronikus információs rendszer elemeinek elhelyezése	12.44. A szervezet úgy helyezi el az EIR elemeit, hogy a legkisebb mértékre csökkentse a szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt, valamint a jogosulatlan hozzáférés lehetőségét.	-	-	X
46.	12.45. Információszivárgás	12.45. A szervezet megvédi az EIR-t az elektromágneses jelek kisugárzása miatt bekövetkező információszivárgástól.	-	-	-
47.	12.46. Eszközök felügyelete és nyomon követése	12.46. A szervezet olyan technológiákat alkalmaz, amelyek képesek a szervezet által meghatározott eszközök helyének és mozgásának nyomon követésére a szervezet által ellenőrzött területeken belül.	-	-	-
48.	12.47. Elektromágneses impulzus elleni védelem	12.47. A szervezet meghatározott védelmi intézkedéseket alkalmaz az EIR-ek és rendszerelemek védelmére az elektromágneses impulzusok okozta károk ellen.	-	-	-
49.	12.48. Rendszerelemek jelölése	12.48. A szervezet kijelöli az EIR-ben azokat a hardverelemeket, amelyek képesek meghatározott biztonsági besorolású információkat feldolgozni, tárolni és továbbítani.	-	-	-
50.	12.49. Létesítmény elhelyezkedése	12.49. A szervezet: 12.49.1. Figyelembe veszi a fizikai és környezeti veszélyeket az EIR-nek helyet adó létesítmény megtervezésekor. 12.49.2. A meglévő létesítményeknél figyelembe veszi a szervezeti kockázatmenedzsment stratégiában szereplő fizikai és környezeti veszélyeket.	-	-	-

13. Tervezés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	13.1. Szabályzat és eljárásrendek	13.1. A szervezet: 13.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 13.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságtervezési szabályzatot, amely 13.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 13.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 13.1.1.2. a biztonságtervezési eljárásrendet, amely a biztonságtervezési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 13.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonságtervezési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 13.1.3. Felülvizsgálja és frissíti az aktuális biztonságtervezési szabályzatot és a biztonságtervezési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X

3.	13.2. Rendszerbiztonsági terv	13.2. A szervezet: 13.2.1. Az EIR-hez rendszerbiztonsági tervet készít, amely: 13.2.1.1. Összhangban áll a szervezeti felépítéssel. 13.2.1.2. Meghatározza az EIR-t alkotó rendszerelemeket. 13.2.1.3. Meghatározza az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait az ügymeneti és üzleti folyamatok szempontjából. 13.2.1.4. Azonosítja azokat a személyeket, akik az EIR szerepeit és felelősségeit betöltik. 13.2.1.5. Meghatározza az EIR által feldolgozott, tárolt és továbbított információtípusokat. 13.2.1.6. Megfelelően alátámasztott módon meghatározza az EIR jogszabály szerinti biztonsági osztályát. 13.2.1.7. Felsorolja az EIR-t érintő konkrét fenyegetéseket. 13.2.1.8. Meghatározza az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait vagy azoktól való függőségeit. 13.2.1.9. Dokumentálja a rendszerre vonatkozó biztonsági követelményeket. 13.2.1.10. Meghatározza a biztonsági alapkövetelményeket és szükség esetén az ezen felül alkalmazott kiegészítő védelmi intézkedéseket. 13.2.1.11. Meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, intézkedésbővítéseket és azok indoklását, végrehajtja a jogszabály szerinti biztonsági feladatokat. 13.2.1.12. Tartalmazza az EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek. 13.2.1.13. Tartalmazza a EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek. 13.2.1.14. A terveket a jóváhagyó felelős áttekinti és jóváhagyja a terv végrehajtása előtt. 13.2.2. Gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyek és szerepkörök megismerjék (ideértve annak változásait is). 13.2.3. Meghatározott gyakorisággal felülvizsgálja a rendszerbiztonsági tervet. 13.2.4. Frissíti a rendszerbiztonsági tervet az EIR-ben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén. 13.2.5. Gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.	X	X	X

4.	13.3. Viselkedési szabályok	13.3.1. A szervezet megfogalmazza és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet. 13.3.2. A szervezet az EIR-hez való hozzáférés engedélyezése előtt dokumentált nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az EIR használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja. 13.3.3. A szervezet meghatározott gyakorisággal felülvizsgálja és frissíti az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet, a viselkedési szabályok betartását. 13.3.4. A szervezet gondoskodik arról, hogy a viselkedési szabályok korábbi változatát megismerő személyek elolvassák és újra dokumentált nyilatkozattételt tegyenek a viselkedési szabályok elfogadásáról, azok felülvizsgálata vagy frissítése esetén.	X	X	X
5.	13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások	13.4. A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be: 13.4.1. a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása; 13.4.2. a szervezeti információk közzétételének korlátozása nyilvános weboldalakon; és 13.4.3. a szervezet által biztosított azonosító és hitelesítő adatok használatának korlátozása külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor.	X	X	X
6.	13.5. Működési koncepció	13.5. A szervezet: 13.5.1. Kidolgozza az EIR működési koncepcióját, amely leírja, hogy a szervezet milyen módon kívánja működtetni az EIR-t az információbiztonság szempontjából 13.5.2. Meghatározott gyakorisággal felülvizsgálja és frissíti a működési koncepciót.	-	-	-
7.	13.6. Információbiztonsági architektúra leírás	13.6. A szervezet: 13.6.1. Elkészíti az EIR információbiztonsági architektúra leírását. 13.6.1.1. Összegzi az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló követelményeket és megközelítést. 13.6.1.2. Megfogalmazza, hogy az információbiztonsági architektúra hogyan illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt. 13.6.1.3. Leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket. 13.6.2. Az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja és frissíti az információbiztonsági architektúra leírást. 13.6.3. Biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben, a működési koncepcióban és a beszerzésekben.	-	X	X
8.	13.7. Információbiztonsági architektúra leírás – Mélységi védelem	13.7. A szervezet az EIR információbiztonsági architektúrájának megtervezésekor mélységi védelmi megközelítést alkalmaz, amely: 13.7.1. meghatározott védelmi intézkedéseket rendel a szervezet által meghatározott helyekhez és architekturális rétegekhez; továbbá 13.7.2. biztosítja, hogy a védelmi intézkedések összehangoltan és egymást erősítve működjenek.	-	-	-

9.	13.8. Információbiztonsági architektúra leírás – Beszállítói diverzifikáció	13.8. A szervezet megköveteli, hogy az általa meghatározott helyeken és architekturális rétegekben alkalmazott biztonsági megoldások különböző beszállítóktól származzanak.	-	-	-
10.	13.9. Központi kezelés	13.9. A szervezet központilag kezeli a meghatározott védelmi intézkedéseket és a hozzájuk kapcsolódó folyamatokat.	-	-	-
11.	13.10. Biztonsági követelmények kiválasztása	13.10. A szervezet kiválasztja az EIR számára az 1. melléklet 1.1.3. ponttal összhangban a biztonsági követelményeket.	X	X	X
12.	13.11. Biztonsági követelmények testre szabása	13.11. A szervezet testre szabja a kiválasztott biztonsági követelményeket.	X	X	X

14. Személyi biztonság

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	14.1. Szabályzat és eljárásrendek	14.1. A szervezet: 14.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 14.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó személyi biztonságra vonatkozó szabályzatot, amely 14.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 14.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 14.1.1.2. a személyi biztonságra vonatkozó eljárásrendet, amely a személyi biztonságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 14.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a személyi biztonságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 14.1.3. Felülvizsgálja és frissíti az aktuális személyi biztonságra vonatkozó szabályzatot és a személyi biztonságra vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	14.2. Munkakörök biztonsági szempontú besorolása	14.2. A szervezet: 14.2.1. minden szervezeti munkakörhöz hozzárendel egy kockázati besorolást; 14.2.2. átvilágítási kritériumokat állít fel a munkaköröket betöltő egyének számára; és 14.2.3. meghatározott gyakorisággal felülvizsgálja és frissíti a kockázati besorolást.	X	X	X
4.	14.3. Személyek háttérellenőrzése	14.3. A szervezet: 14.3.1. ellenőrzi az egyéneket, mielőtt engedélyezné a hozzáférésüket a rendszerhez; és 14.3.2. ismételten ellenőrzi az egyéneket a meghatározott feltételeknek megfelelően, ha változás történt az egyén jogosultsági szintjében vagy munkakörében, illetve meghatározott gyakorisággal.	X	X	X
5.	14.4. Személyek háttérellenőrzése – Különleges védelmi intézkedéseket igénylő információk	14.4. A szervezet ellenőrzi, hogy azok az egyének, akik hozzáférnek egy speciális védelmet igénylő információkat feldolgozó, tároló vagy továbbító rendszerhez 14.4.1. rendelkeznek-e érvényes hozzáférési engedéllyel; és 14.4.2. esetükben teljesülnek-e a szervezet által meghatározott további személyzeti ellenőrzési kritériumok.	-	-	-

6.	14.5. Személyek munkaviszonyának megszűnése	14.5. A szervezet az egyéni munkaviszony megszűnésekor: 14.5.1. Meghatározott időn belül letiltja a rendszerhez való hozzáférést. 14.5.2. Megszünteti vagy visszavonja az adott személyhez kapcsolódó összes hitelesítő eszközt és jogosultságot. 14.5.3. Lefolytatja a kilépési interjúkat, amelyek meghatározott információbiztonsági témákat tartalmaznak. 14.5.4. Visszaveszi az összes biztonsági szempontból releváns szervezeti EIR-hez kapcsolódó biztonsági eszközöket. 14.5.5. Fenntartja a hozzáférést a megszűnt munkaviszonyú személy által ellenőrzött szervezeti információkhoz és rendszerekhez.	X	X	X
7.	14.6. Személyek munkaviszonyának megszűnése – Munkaviszony megszűnését követő követelmények	14.6. A szervezet: 14.6.1. Tájékoztatja az elbocsátott munkavállalókat a jogilag kötelező, munkaviszony megszüntetése után érvényes követelményekről, amelyek a szervezeti információk védelmére vonatkoznak. 14.6.2. A munkaviszony megszüntetésének folyamatában megköveteli, hogy az elbocsátott munkavállalók aláírjanak egy nyilatkozatot a munkaviszony megszüntetése utáni követelmények tudomásulvételéről.	-	-	-
8.	14.7. Személyek munkaviszonyának megszűnése – Automatizált intézkedések	14.7. A szervezet meghatározott automatizált mechanizmusokat alkalmaz annak érdekében, hogy értesítse a meghatározott személyeket vagy szerepköröket az egyén kilépésével összefüggő tevékenységekről, illetve, hogy megszüntesse a hozzáférést a rendszer erőforrásaihoz.	-	-	X
9.	14.8. Az áthelyezések, átirányítások és kirendelések kezelése	14.8. A szervezet: 14.8.1. A folyamatos működés követelményeivel összhangban felülvizsgálja és megerősíti a rendszerekhez és létesítményekhez rendelt érvényes logikai és fizikai hozzáférési jogosultságokat minden olyan esetben, amikor az egyének a szervezeten belül más munkakörbe kerülnek áthelyezésre vagy átirányításra. 14.8.2. Meghatározott időn belül kezdeményezi az áthelyezési és átirányítási intézkedéseket. 14.8.3. Szükség szerint módosítja a hozzáférési jogosultságot, hogy az megfeleljen az áthelyezés vagy átirányítás miatt bekövetkező változások működési szükségleteinek. 14.8.4. Meghatározott időn belül értesíti a megadott személyeket vagy szerepköröket.	X	X	X
10.	14.9. Hozzáférési megállapodások	14.9. A szervezet: 14.9.1. Kidolgozza és dokumentálja a szervezeti EIR-ekhez való hozzáférés szabályait. 14.9.2. A szervezet által meghatározott gyakorisággal felülvizsgálja és frissíti a hozzáférési szabályokat. 14.9.3. Ellenőrzi, hogy a szervezeti információkhoz és rendszerekhez hozzáférést igénylő személyek 14.9.3.1. a hozzáférés megadása előtt megismerték és dokumentált módon elfogadták a vonatkozó hozzáférési szabályokat; és 14.9.3.2. a hozzáférési szabályok változása esetén, vagy a szervezet által meghatározott gyakorisággal megismerték és dokumentált módon elfogadták az aktuális hozzáférési szabályokat az EIR-ekhez való hozzáférés megtartása érdekében.	X	X	X
11.	14.10. Hozzáférési megállapodások – Munkaviszony megszűnése után is fennálló kötelezettségek	14.10. A szervezet: 14.10.1. Tájékoztatja az egyéneket a munkaviszonyuk megszűnése után is érvényes, jogilag kötelező információvédelmi követelményekről. 14.10.2. Megköveteli az egyénektől, hogy aláírásukkal elismerjék ezeket a követelményeket, mielőtt először hozzáférnének a védett információkhoz.	-	-	-

12.	14.11. Külső személyekhez kapcsolódó biztonsági követelmények	14.11. A szervezet: 14.11.1. Személyi biztonsági követelményeket állít fel a külső szolgáltatókkal szemben, amelyek magukba foglalják a szükséges biztonsági szerepköröket és felelősségeket. 14.11.2. Megköveteli a külső szolgáltatóktól, hogy tartsák be a szervezet által meghatározott személyi biztonsági szabályokat. 14.11.3. Dokumentálja a személyi biztonsági követelményeket. 14.11.4. Megköveteli a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkeztek. 14.11.5. Ellenőrzi, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek.	X	X	X
13.	14.12. Fegyelmi intézkedések	14.12. A szervezet: 14.12.1. Fegyelmi eljárást kezdeményez azokkal az egyénekkel szemben, akik nem tartják be az információbiztonsági szabályokat és eljárásokat. 14.12.2. Meghatározott időn belül értesíti a szervezet által meghatározott személyeket vagy szerepköröket, amikor fegyelmi eljárás kerül megindításra, azonosítva az eljárás alá vont személyt és az eljárás okát.	X	X	X
14.	14.13. Munkaköri leírások	14.13. A szervezet belefoglalja a biztonsági szerepköröket és felelősségeket a szervezeti munkaköri leírásokba.	X	X	X

15. Kockázatkezelés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	15.1. Szabályzat és eljárásrendek	15.1. A szervezet: 15.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 15.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó kockázatmenedzsment szabályzatot, amely 15.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 15.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 15.1.1.2. a kockázatelemzési és kockázatkezelési eljárásrendet, amely a kockázatmenedzsment szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 15.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 15.1.3. Felülvizsgálja és frissíti az aktuális kockázatmenedzsment szabályzatot és a kockázatelemzési és kockázatkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	15.2. Biztonsági osztályba sorolás	15.2. A szervezet: 15.2.1. Biztonsági osztályba sorolja az EIR-t; 15.2.2. A rendszerbiztonsági tervben dokumentálja a biztonsági osztályba sorolás eredményeit, beleértve az azt alátámasztó indoklást is. 15.2.3. Ellenőrzi, hogy a szervezet vezetője jóváhagyta a biztonsági osztályba sorolási döntést.	X	X	X
4.	15.3. Biztonsági osztályba sorolás – Hatásszintek súlyozása	15.3. A szervezet elvégzi a szervezeti EIR-ek működési hatása szerinti rangsorolását annak érdekében, hogy még részletesebben meghatározhassa a rendszerek hatásszintjeit.	-	-	-

5.	15.4. Kockázatelemzés	15.4. A szervezet: 15.4.1. Rendszerszintű kockázatelemzést végez, amely magába foglalja: 15.4.1.1. a rendszerre vonatkozó fenyegetések és sérülékenységek azonosítását; 15.4.1.2. a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy a rendszer megsemmisítésének valószínűségének és káros hatásainak megállapítását, valamint az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan; 15.4.1.3. személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségének és mértékének megállapítását. 15.4.2. Integrálja a szervezet, a szervezeti célok vagy üzleti folyamatok szempontjából végzett kockázatelemzés eredményeit és a kockázatkezelési döntéseket a rendszerszintű kockázatelemzésekkel. 15.4.3. Dokumentálja a kockázatelemzés eredményeit a kockázatelemzési jelentésben és a szervezet által meghatározott dokumentumokban. 15.4.4. Meghatározott gyakorisággal áttekinti a kockázatelemzés eredményeit. 15.4.5. Megismerteti a kockázatelemzés eredményeit a meghatározott személyekkel vagy szerepkörökkel. 15.4.6. Meghatározott gyakorisággal frissíti a kockázatelemzést vagy minden olyan esetben, amikor jelentős változások történnek a rendszerben, annak működési környezetében, vagy más olyan körülményekben, amelyek befolyásolhatják a rendszer biztonsági állapotát.	X	X	X
6.	15.5. Kockázatelemzés – Ellátási lánc	15.5. A szervezet: 15.5.1. Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában. 15.5.2. Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatására.	X	X	X
7.	15.6. Kockázatelemzés – Különböző forrásokból származó információk felhasználása	15.6. A szervezet minden lehetséges forrásból (all-source-intelligence) származó információt felhasznál a kockázatok értékelésében.	-	-	-
8.	15.7. Kockázatelemzési és kockázatkezelési eljárásrend – Dinamikus fenyegetésfelismerés	15.7. A szervezet folyamatosan értékeli az aktuális kiberfenyegetettségi helyzetét az általa meghatározott eszközökkel.	-	-	-
9.	15.8. Kockázatelemzési és kockázatkezelési eljárásrend – Prediktív elemzés	15.8. A szervezet fejlett, automatizált elemzési képességeket alkalmaz, hogy előre jelezze és azonosítsa a meghatározott EIR-ek vagy rendszerelemek kockázatait.	-	-	-
10.	15.9. Sérülékenységek ellenőrzése	15.9. A szervezet: 15.9.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel ellenőrzi az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek. 15.9.2. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.	X	X	X

11.	15.10. Sérülékenységmenedzsment	15.10. A szervezet: 15.10.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel szkenneli az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek. 15.10.2. Olyan sérülékenységmenedzsment eszközöket és technikákat alkalmaz, amelyek elősegítik az eszközök közötti átjárhatóságot és automatizálják a sérülékenységkezelési folyamat egyes lépéseit a következők szerint: 15.10.2.1. felsorolja a platformokat, szoftverhibákat és helytelen konfigurációkat; 15.10.2.2. ellenőrző listákat és tesztelési eljárásokat alkalmaz; és 15.10.2.3. méri az egyes sérülékenységek hatásait. 15.10.3. Elemzi a sérülékenységmenedzsment jelentéseket és a vizsgálatok eredményeit, 15.10.4. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően. 15.10.5. Megosztja a sérülékenységmenedzsment folyamatból és a követelmények értékeléséből származó információkat a meghatározott személyekkel vagy szerepkörökkel, hogy segítsenek kiküszöbölni a hasonló sérülékenységeket más rendszerekben. 15.10.6. Olyan sérülékenységmenedzsment eszközöket alkalmaz, amelyek képesek a vizsgálandó sérülékenységek egyszerű frissítésére.	-	X	X
12.	15.11. Sérülékenységmenedzsment – Sérülékenységi adatbázis frissítése	15.11. A szervezet meghatározott gyakorisággal, valamint minden új vizsgálat megkezdése előtt, továbbá új sérülékenységek azonosítása és jelentése esetén frissíti az EIR-ben szkennelt sérülékenységek körét.	-	X	X
13.	15.12. Sérülékenységmenedzsment – A lefedettség szélessége és mélysége	15.12. A szervezet meghatározza a sérülékenységmenedzsment folyamat hatókörét és mélységét.	-	-	-
14.	15.13. Sérülékenységmenedzsment – Felfedezhető információk	15.13. A szervezet megállapítja, hogy milyen információk érhetők el az EIR-ről, annak kompromittálása nélkül, és ez alapján szükség esetén korrekciós intézkedéseket hajt végre.	-	X	X
15.	15.14. Sérülékenységmenedzsment – Privilegizált hozzáférés	15.14. A szervezet privilegizált hozzáférést biztosít a meghatározott rendszerelemekhez a szervezet által meghatározott sérülékenységmenedzsment tevékenységek elvégzéséhez.	-	X	X
16.	15.15. Sérülékenységmenedzsment – Automatizált trendelemzések	15.15. A szervezet meghatározott automatizált mechanizmusok segítségével összehasonlítja a sérülékenységszkennelések eredményeit.	-	-	-
17.	15.16. Sérülékenységmenedzsment – Naplóbejegyzések felülvizsgálata	15.16. A szervezet átvizsgálja a korábbi naplóbejegyzéseket, hogy megállapítsa, hogy egy meghatározott, az EIR-ben azonosított sérülékenységet korábban kihasználták-e egy meghatározott időszakban.	-	-	-
18.	15.17. Sérülékenységmenedzsment – Észlelt információk összekapcsolása	15.17. A szervezet a sérülékenységmenedzsment eszközök kimeneteit annak érdekében korrelálja, hogy megállapítsa az összetett sérülékenységek és többlépcsős támadási vektorok jelenlétét.	-	-	-
19.	15.18. Sérülékenységmenedzsment – Sérülékenységi információk fogadása	15.18. A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.	X	X	X

20.	15.19. Technikai megfigyeléssel szembeni intézkedések	15.19. A szervezet meghatározott gyakorisággal, vagy egyes előre meghatározott események bekövetkezésekor, vagy ráutaló jelek észlelése esetén az előre meghatározott helyszíneken ellenőrzi a technikai megfigyelőeszközök jelenlétét.	-	-	-
21.	15.20. Kockázatokra adott válasz	15.20. A szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.	X	X	X
22.	15.21. Rendszerelemek kritikusságának elemzése	15.21. A szervezet azonosítja a szervezet működése szempontjából kritikus rendszerelemeket és funkciókat - a meghatározott EIR-ekre, rendszerelemekre vagy rendszerszolgáltatásokra vonatkozó kritikussági elemzés végrehajtásával - a rendszerfejlesztési életciklus meghatározott döntési pontjain.	-	X	X
23.	15.22. Fenyegetés felderítés	15.22.1. A szervezet létrehoz és fenntart egy fenyegetés-felderítő képességet, hogy: 15.22.1.1. keresse a kompromittálódás jeleit a szervezeti EIR-ekben; és 15.22.1.2. felderítse, nyomon kövesse és elhárítsa a meglévő védelmi mechanizmusokat megkerülő fenyegetéseket. 15.22.2. Meghatározott gyakorisággal alkalmazza a fenyegetés-felderítő képességét.	-	-	-

16. Rendszer- és szolgáltatásbeszerzés

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	16.1. Szabályzat és eljárásrendek	16.1. A szervezet: 16.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 16.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó beszerzési szabályzatot, amely 16.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 16.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 16.1.1.2. a beszerzési eljárásrendet, amely a beszerzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 16.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a beszerzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 16.1.3. Felülvizsgálja és frissíti az aktuális beszerzési szabályzatot és a beszerzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	16.2. Erőforrások rendelkezésre állása	16.2. A szervezet: 16.2.1. Az üzletmenet és üzleti folyamatok tervezése során meghatározza az EIR vagy rendszerszolgáltatás magas szintű információbiztonsági követelményeit. 16.2.2. Biztosítja az EIR és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként. 16.2.3. Elkülönített tételként kezeli az EIR-ek biztonságát a beruházás tervezési dokumentumaiban.	X	X	X
4.	16.3. A rendszer fejlesztési életciklusa	16.3.1. Az EIR-ek teljes életútján, minden életciklusukban figyelemmel kíséri azok információbiztonsági helyzetét. 16.3.2. A fejlesztési életciklus egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket. 16.3.3. Azonosítja az információbiztonsági szerepkörökkel és felelősségi körökkel rendelkező személyeket. 16.3.4. Beépíti a szervezeti információbiztonsági kockázatmenedzsment folyamatot a rendszerfejlesztési életciklus tevékenységeibe.	X	X	X
5.	16.4. A rendszer fejlesztési életciklusa – Preprodukciós környezet kezelése	16.4. A szervezet gondoskodik a preprodukciós környezetek kockázatarányos védelméről a rendszer, rendszerelem vagy rendszerszolgáltatás teljes életciklusa során.	-	-	-
6.	16.5. A rendszer fejlesztési életciklusa – A preprodukciós környezetben kezelt adatok	16.5. A szervezet: 16.5.1. Jóváhagyja, dokumentálja és ellenőrzi az éles környezetből származó adatok használatát az EIR, rendszerelem vagy rendszerszolgáltatás preprodukciós környezetében. 16.5.2. Biztosítja az EIR, a rendszerelem vagy a rendszerszolgáltatás preprodukciós környezetének védelmét az abban kezelt adatok védelmi igényének megfelelően.	-	-	-

7.	16.6. A rendszer fejlesztési életciklusa – Technológiaváltás	16.6. A szervezet megtervezi és végrehajtja az EIR technológiaváltási ütemtervét a rendszer teljes életciklusa során.	-	-	-
8.	16.7. Beszerzések	16.7. A szervezet a beszerzési folyamat során - beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is - a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat: 16.7.1. A funkcionális biztonsági követelményeket. 16.7.2. A mechanizmusok erősségére vonatkozó követelményeket. 16.7.3. A biztonság garanciális követelményeit. 16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket. 16.7.5. A biztonsággal kapcsolatos dokumentációs követelményeket. 16.7.6. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket. 16.7.7. Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat. 16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását. 16.7.9. A teljesítési kritériumokat.	X	X	X
9.	16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai	16.8. A szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását.	X	X	X
10.	16.9. Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez	16.9. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási információkat a védelmi intézkedésekhez. Ezek az információk tartalmazzák a biztonsági szempontból releváns külső rendszerinterfészeket, a magas szintű rendszertervet, az alacsony szintű rendszertervet, a forráskódot vagy a hardversémákat, valamint a szervezet által meghatározott részletes tervezési és megvalósítási információkat.	-	X	X
11.	16.10. Beszerzések – Fejlesztési módszerek, technikák és gyakorlatok	16.10. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője bemutassa a rendszerfejlesztési életciklus folyamatának alkalmazását. Ez magában foglalja: 16.10.1. a szervezet által meghatározott rendszertervezési módszereket; 16.10.2. a szervezet által meghatározott rendszerbiztonsági módszereket; 16.10.3. a szervezet által meghatározott szoftverfejlesztési, tesztelési, értékelési, ellenőrzési és érvényesítési módszereket, valamint a minőségellenőrzési eljárásokat.	-	-	-
12.	16.11. Beszerzések - Rendszer, rendszerelem és szolgáltatás konfigurációk – Rendszer, rendszerelem és szolgáltatás konfigurációk	16.11. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.11.1. Az EIR, rendszerelem vagy szolgáltatás szállítása a meghatározott biztonsági konfigurációk alkalmazásával történjen. 16.11.2. Minden EIR, rendszerelem vagy szolgáltatás későbbi újratelepítése vagy frissítése során az alapkonfigurációkat használják.	-	-	X
13.	16.12. Beszerzések – Monitorozási terv a biztonsági követelmények teljesülése érdekében	16.12. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervet készítsen, amely a szervezet által meghatározott monitorozási programmal összhangban van, és amely a védelmi intézkedések hatékonyságának monitorozását szolgálja.	-	-	-
14.	16.13. Beszerzések – Használatban lévő funkciók, portok, protokollok és szolgáltatások	16.13. A szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy határozza meg a használatra tervezett funkciókat, portokat, protokollokat és szolgáltatásokat.	-	X	X

15.	16.14. Beszerzések – Adatgazda szerepkör	16.14. A szervezet: 16.14.1. A szervezet adatkezelési követelményeit beépíti a beszerzési szerződésekbe. 16.14.2. Megköveteli, hogy minden adatot távolítsanak el a vállalkozó EIR-éből, és szolgáltassanak vissza a szervezetnek a szervezet által meghatározott időn belül	-	-	-
16.	16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció	16.15. A szervezet: 16.15.1. Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza: 16.15.1.1. az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését; 16.15.1.2. a biztonsági funkciók hatékony használatát és karbantartását; valamint 16.15.1.3. az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban. 16.15.2. Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza: 16.15.2.1. a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját; 16.15.2.2. a felhasználói interakció biztonságos módját; 16.15.2.3. a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában. 16.15.3. Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és 16.15.4. a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.	X	X	X
17.	16.16. Biztonságtervezési elvek	16.16. A szervezet az általa meghatározott biztonságtervezési elveket alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során.	X	X	X
18.	16.17. Biztonságtervezési elvek – Világos fogalomrendszer	16.17. A szervezet kialakítja a biztonságtervezési elveit, amelyek világos absztrakciókra épülnek.	-	-	-
19.	16.18. Biztonságtervezési elvek – Korlátozott közös működés	16.18. A szervezet a korlátozott közös működés (Least Common Mechanism) biztonságtervezési elvét alkalmazza a meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
20.	16.19. Biztonságtervezési elvek – Modularitás és rétegezés	16.19. A szervezet a moduláris és rétegezett felépítés biztonságtervezési elvét alkalmazza a meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
21.	16.20. Biztonságtervezési elvek – Részben rendezett függőségek	16.20. A szervezet a részben rendezett függőségek (Partially Ordered Dependencies) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
22.	16.21. Biztonságtervezési elvek – Hatékony erőforráshozzáférés közvetítés	16.21. A szervezet a hatékonyan közvetített erőforráshozzáférés (Efficiently Mediated Access) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
23.	16.22. Biztonságtervezési elvek – Minimalizált megosztás	16.22. A szervezet a minimalizált megosztás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
24.	16.23. Biztonságtervezési elvek – Minimalizált komplexitás	16.23. A szervezet a minimalizált komplexitás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
25.	16.24. Biztonságtervezési elvek – Biztonságos továbbfejlődés	16.24. A szervezet a biztonságos továbbfejlődés (Secure Evolvability) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-

26.	16.25. Biztonságtervezési elvek – Megbízható rendszerelemek	16.25. A szervezet a megbízható rendszerelemek biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
27.	16.26. Biztonságtervezési elvek – Hierarchikus bizalom	16.26. A szervezet a hierarchikus bizalom biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
28.	16.27. Biztonságtervezési elvek – Inverz módosítási küszöb	16.27. A szervezet az inverz módosítási küszöb (Inverse Modification Threshold) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
29.	16.28. Biztonságtervezési elvek – Hierarchikus védelem	16.28. A szervezet a hierarchikus védelem biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
30.	16.29. Biztonságtervezési elvek – Biztonsági elemek minimalizálása	16.29. A szervezet a biztonsági elemek minimalizálásának biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
31.	16.30. Biztonságtervezési elvek – Legkisebb jogosultság	16.30. A szervezet a legkisebb jogosultság biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
32.	16.31. Biztonságtervezési elvek – Feltételhez kötött engedélyezés	16.31. A szervezet a feltételhez kötött engedélyezés (Predicate Permission) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
33.	16.32. Biztonságtervezési elvek – Önfenntartó megbízhatóság	16.32. A szervezet az önfenntartó megbízhatóság (Self-reliant Trustworthiness) biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
34.	16.33. Biztonságtervezési elvek – Biztonságosan elosztott felépítés	16.33. A szervezet a biztonságosan elosztott felépítés (Secure Distributed Composition) tervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
35.	16.34. Biztonságtervezési elvek – Biztonságos kommunikációs csatornák	16.34. A szervezet a biztonságos kommunikációs csatornák biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
36.	16.35. Biztonságtervezési elvek – Folyamatos védelem	16.35. A szervezet a folyamatos védelem biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
37.	16.36. Biztonságtervezési elvek – Biztonságos metaadatkezelés	16.36. A szervezet a biztonságos metaadatkezelés biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
38.	16.37. Biztonságtervezési elvek – Önellenőrzés	16.37. A szervezet az önellenőrzés biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
39.	16.38. Biztonságtervezési elvek – Elszámoltathatóság és nyomonkövethetőség	16.38. A szervezet az elszámoltathatóság és nyomonkövethetőség biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
40.	16.39. Biztonságtervezési elvek – Biztonságos alapbeállítások	16.39. A szervezet a biztonságos alapbeállítások biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
41.	16.40. Biztonságtervezési elvek – Biztonságos hibakezelés és helyreállítás	16.40. A szervezet a biztonságos hibakezelés és helyreállítás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
42.	16.41. Biztonságtervezési elvek – Költséghatékony biztonság	16.41. A szervezet a költséghatékony biztonság biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
43.	16.42. Biztonságtervezési elvek – Teljesítménybiztonság	16.42. A szervezet a teljesítménybiztonság tervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
44.	16.43. Biztonságtervezési elvek – Emberi tényezőn alapuló biztonság	16.43. A szervezet az emberi tényezőn alapuló biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
45.	16.44. Biztonságtervezési elvek – Elfogadható biztonsági szint	16.44. A szervezet az elfogadható biztonsági szint biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-

46.	16.45. Biztonságtervezési elvek – Megismételhető és dokumentált eljárások	16.45. A szervezet a megismételhető és dokumentált eljárások biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
47.	16.46. Biztonságtervezési elvek – Eljárási szigor	16.46. A szervezet a szigorú eljárási rend biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
48.	16.47. Biztonságtervezési elvek – Biztonságos rendszermódosítás	16.47. A szervezet a biztonságos rendszermódosítás biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
49.	16.48. Biztonságtervezési elvek – Megfelelő dokumentáció	16.48. A szervezet a megfelelő dokumentáció biztonságtervezési elvét alkalmazza a szervezet által meghatározott EIR-ekben vagy rendszerelemekben.	-	-	-
50.	16.49. Külső elektronikus információs rendszerek szolgáltatásai	16.49. A szervezet: 16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák. 16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban. 16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek.	X	X	X
51.	16.50. Külső információs rendszerek szolgáltatásai – Kockázatelemzések és szervezeti jóváhagyások	16.50. A szervezet: 16.50.1. Elvégzi a szervezeti kockázatelemzést az információbiztonsági szolgáltatások beszerzése vagy kiszervezése előtt. 16.50.2. Meghatározott személyek vagy szerepkörök jóváhagyásához köti az információbiztonsági célú szolgáltatások beszerzését vagy kiszervezését.	-	-	-
52.	16.51. Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása	16.51. A szervezet megköveteli a szolgáltatóktól, hogy azonosítsák az általuk nyújtott rendszerszolgáltatásokhoz szükséges funkciókat, portokat, protokollokat és szolgáltatásokat.	-	X	X
53.	16.52. Külső információs rendszerek szolgáltatásai – Megbízható kapcsolat kialakítása és fenntartása a szolgáltatókkal	16.52. A szervezet megbízható kapcsolatokat épít ki és tart fenn külső szolgáltatókkal, a meghatározott biztonsági követelmények alapján.	-	-	-
54.	16.53. Külső információs rendszerek szolgáltatásai – Összhangban lévő érdekek	16.53. A szervezet meghatározott intézkedéseket hajt végre annak érdekében, hogy ellenőrizze, hogy a külső szolgáltatók érdekei sértik-e szervezeti érdeket.	-	-	-
55.	16.54. Külső információs rendszerek szolgáltatásai – Feldolgozás, tárolás és szolgáltatási helyszín	16.54. A szervezet a meghatározott helyszínekre korlátozza az információ feldolgozásának helyét, valamint az információk vagy adatok elhelyezését, a szervezet által meghatározott követelmények és feltételek alapján.	-	-	-
56.	16.55. Külső információs rendszerek szolgáltatásai – Felügyelt kriptográfiai kulcsok	16.55. A szervezet kizárólagos ellenőrzést gyakorol a külső rendszerekben tárolt, vagy külső rendszerekbe továbbított titkos adatokhoz tartozó kriptográfiai kulcsok felett.	-	-	-
57.	16.56. Külső információs rendszerek szolgáltatásai – Sértetlenség felügyelete	16.56. Az EIR képes arra, hogy ellenőrizze a külső rendszerben található információ sértetlenségét.	-	-	-
58.	16.57. Külső információs rendszerek szolgáltatásai – Feldolgozási és tárolási helyszín – Magyarország joghatósága	16.57. A szervezet az információfeldolgozást és az adattárolást olyan helyszínekre korlátozza, amelyek Magyarország határain belül találhatók.	-	-	-

59.	16.58. Fejlesztői változáskövetés	16.58. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.58.1. Alkalmazzon konfigurációkezelési folyamatokat az EIR, rendszerelem vagy szolgáltatás tervezése, fejlesztése, bevezetése, üzemeltetése vagy kivonása (teljes életciklusa) során. 16.58.2. Dokumentálja, kezelje és ellenőrizze a szervezet által a konfigurációkezelés keretében meghatározott konfigurációs elemek változtatásait, és biztosítsa ezek sértetlenségét. 16.58.3. Csak a szervezet által jóváhagyott változtatásokat hajtsa végre az EIR-en, rendszerelemen vagy rendszerszolgáltatáson. 16.58.4. Dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait. 16.58.5. Kövesse nyomon az EIR, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit a szervezet által meghatározott személyeknek.	-	X	X
60.	16.59. Fejlesztői konfigurációkezelés – Szoftver és firmware sértetlenségének ellenőrzése	16.59. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a szervezet részére tegye lehetővé a szoftver- és firmware-elemek sértetlenségének ellenőrzését.	-	-	-
61.	16.60. Fejlesztői konfigurációkezelés – Alternatív konfigurációkezelési folyamatok	16.60. A szervezet alternatív konfigurációkezelési folyamatot biztosít a szervezeti munkavállalók bevonásával, amennyiben a szervezet nem rendelkezik dedikált fejlesztői konfigurációkezelő csoporttal.	-	-	-
62.	16.61. Fejlesztői konfigurációkezelés – Hardver sértetlenségének ellenőrzése	16.61. A szervezet megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője lehetővé tegye a hardverelemek sértetlenségének ellenőrzését.	-	-	-
63.	16.62. Fejlesztői konfigurációkezelés – Megbízható generálás	16.62. A szervezet megköveteli az EIR, rendszerelem és rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon eszközöket a biztonság szempontjából fontos hardver specifikációk, forráskódok és objektumkódok újonnan generált verzióinak korábbi verziókkal való összehasonlítására.	-	-	-
64.	16.63. Fejlesztői konfigurációkezelés – Verziókezelési sértetlenség feltérképezése	16.63. A szervezet biztosítja a biztonság szempontjából releváns hardver, szoftver és firmware aktuális verzióját leíró törzsadatok és az aktuális verzió adatainak helyszíni másolata közötti összefüggés sértetlenségét.	-	-	-
65.	16.64. Fejlesztői konfigurációkezelés – Megbízható terjesztés	16.64. A szervezet előírja az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjének, hogy olyan eljárásokat hajtson végre, amelyek biztosítják, hogy a szervezet számára szétosztott biztonsági szempontból releváns hardver-, szoftver- és firmware-frissítések pontosan megegyeznek a mesterpéldányok által meghatározottakkal.	-	-	-
66.	16.65. Fejlesztői konfigurációkezelés – Biztonsági felelősök	16.65. A szervezet biztosítja a szervezet által meghatározott biztonsági felelősök bevonását a meghatározott konfigurációs változások kezelési és ellenőrzési folyamatába.	-	-	-
67.	16.66. Fejlesztői biztonsági tesztelés	16.66. A szervezet az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől megköveteli, hogy: 16.66.1. Készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat. 16.66.2. Meghatározott gyakorisággal hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, illetve regressziós tesztelést, és értékelje ki a szervezet által meghatározottak szerint. 16.66.3. Dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit. 16.66.4. Vezessen be egy ellenőrizhető hibajavítási folyamatot.	-	X	X

		16.66.5. Javítsa ki a tesztelés és értékelés során azonosított hibákat.			
68.	16.67. Fejlesztői biztonsági tesztelés és értékelés – Statikus kódelemzés	16.67. A szervezet statikus kódelemző eszközöket alkalmaz a gyakori hibák azonosítására, valamint az elemzés eredményeinek dokumentálására.	-	-	-
69.	16.68. Fejlesztői biztonsági tesztelés és értékelés – Fenyegetésmodellezés és sérülékenységelemzések	16.68. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy fenyegetésmodellezést és sérülékenységelemzéseket hajtson végre az EIR-en, rendszerelemen vagy szolgáltatáson a fejlesztés, a tesztelés és az értékelés során, amelyek: 16.68.1. a szervezet által a várható hatásra, a működési környezetre, az ismert vagy feltételezett fenyegetésekre és az elfogadható kockázati szintekre meghatározott környezeti információkat használják; 16.68.2. a szervezet által meghatározott eszközöket és módszereket használják; 16.68.3. a modellezéseket és elemzéseket a szervezet által előírt szigorúsági kritériumok (hatókör és mélység) szerint hajtják végre; 16.68.4. olyan bizonyítékot szolgáltatnak, amelyek megfelelnek a szervezet által meghatározott elfogadási kritériumoknak.	-	-	-
70.	16.69. Fejlesztői biztonsági tesztelés és értékelés – Független ellenőrzés az értékelési tervek és bizonyítékok tekintetében	16.69. A szervezet: 16.69.1. A meghatározott kritériumoknak megfelelő független személyt alkalmaz, aki ellenőrzi a fejlesztői biztonsági-értékelési tervek helyes végrehajtását, valamint a tesztelés és értékelés során előállított bizonyítékokat. 16.69.2. Ellenőrzi, hogy a független megbízott elegendő információt kap-e az ellenőrzési folyamat elvégzéséhez, és fel van-e hatalmazva az ilyen információk megszerzésére	-	-	-
71.	16.70. Fejlesztői biztonsági tesztelés és értékelés – Manuális kódellenőrzés	16.70. A szervezet előírja, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője köteles manuális kódellenőrzést végrehajtani a szervezet által meghatározott konkrét kódrészleten, a meghatározott folyamatok, eljárások vagy technikák segítségével.	-	-	-
72.	16.71. Fejlesztői biztonsági tesztelés és értékelés – Behatolásvizsgálat	16.71. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.71.1. A szervezet meghatározza a vizsgálat terjedelmét és mélységét. 16.71.2. A vizsgálatot a szervezet által meghatározott korlátozások mellett kell elvégezni.	-	-	-
73.	16.72. Fejlesztői biztonsági tesztelés és értékelés – Támadási felület értékelések	16.72. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezze el az EIR támadási felületeire vonatkozó felülvizsgálatokat és értékeléseket.	-	-	-
74.	16.73. Fejlesztői biztonsági tesztelés és értékelés – Tesztelés és értékelés hatáskörének ellenőrzése	16.73. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy ellenőrizze a tesztelés és értékelés terjedelmét annak érdekében, hogy teljes körű lefedettséget biztosítson a szükséges biztonsági követelményekre, amelyeket a szervezet határoz meg a tesztelési és értékelési hatókör és mélység alapján.	-	-	-

75.	16.74. Fejlesztői biztonsági tesztelés és értékelés – Dinamikus kódelemzés	16.74. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy alkalmazzon dinamikus kódelemző eszközöket, és az eszközök segítségével azonosítsa a gyakori hibákat, valamint dokumentálja az elemzés eredményeit.	-	-	-
76.	16.75. Fejlesztői biztonsági tesztelés és értékelés – Interaktív alkalmazásbiztonsági tesztelés	16.75. A szervezet megköveteli a rendszerfejlesztőtől, hogy alkalmazzon manuális és automatizált alkalmazásbiztonsági tesztelő eszközöket a hibák azonosítására és a tesztelési eredmények dokumentálására.	-	-	-
77.	16.76. Fejlesztési folyamat, szabványok és eszközök	16.76.1. A szervezet: 16.76.2. Megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen. 16.76.2.1. Kiemelten kezelje a biztonsági követelményeket. 16.76.2.2. Határozza meg a fejlesztés során alkalmazott szabványokat és eszközöket. 16.76.2.3. Dokumentálja a fejlesztés során alkalmazott speciális eszköz konfigurációkat és opciókat. 16.76.2.4. Tartsa nyilván a változtatásokat, és biztosítsa ezek jogosulatlan változtatás elleni védelmét; továbbá 16.76.3. Előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat	-	X	X
78.	16.77. Fejlesztési folyamat, szabványok és eszközök – Minőség mérőszámai	16.77. A szervezet megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.77.1. A fejlesztési folyamat kezdetén határozzon meg minőségi mérőszámokat. 16.77.2. Rendszeresen, meghatározott időközönként és a mérföldkövek elérésekor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan. 16.77.3. A fejlesztett szolgáltatás átadásakor számoljon be a minőségi mutatók teljesítéséről és nyújtson be bizonyítékot erre vonatkozóan.	-	-	-
79.	16.78. Fejlesztési folyamat, szabványok és eszközök – Biztonsági szempontokat nyomonkövető eszközök	16.78. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy válasszon ki és alkalmazzon olyan eszközöket a fejlesztési folyamat során, amelyek alkalmasak a biztonsági szempontok nyomonkövetésére.	-	-	-
80.	16.79. Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés	16.79. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen kritikussági elemzést: 16.79.1. A rendszerfejlesztési életciklus alatt, a szervezet által meghatározott döntési pontokon. 16.79.2. A szervezet által meghatározott szigorúsággal.	-	X	X
81.	16.80. Fejlesztési folyamat, szabványok és eszközök – Támadási felület csökkentése	16.80. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a szervezet által meghatározott mértékben csökkentse az EIR támadási felületeit.	-	-	-
82.	16.81. Fejlesztési folyamat, szabványok és eszközök – Folyamatos továbbfejlesztés	16.81. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy egy folyamatot vezessen be a fejlesztési folyamat folyamatos javítására.	-	-	-

83.	16.82. Fejlesztési folyamat, szabványok és eszközök – Automatizált sérülékenységelemzés	16.82. A szervezet megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat során, a szervezet által elvárt gyakorisággal: 16.82.1. végezze el az automatizált sérülékenységelemzést a szervezet által meghatározott eszközökkel; 16.82.2. határozza meg a felfedezett sérülékenységek kihasználásának módjait és potenciálját; 16.82.3. határozza meg a sérülékenységekre vonatkozó javasolt kockázatcsökkentő lehetőségeket; valamint 16.82.4. adja át a vizsgálat és elemzés eredményeit a szervezet által meghatározott személyeknek vagy szerepköröknek.	-	-	-
84.	16.83. Fejlesztési folyamat, szabványok és eszközök – Fenyegetési- és sérülékenységi információk felhasználása	16.83. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat támogatása érdekében vegye figyelembe a hasonló rendszerekből, rendszerelemekből vagy rendszerszolgáltatásokból származó fenyegetésmodellezést és sérülékenységelemzéseket.	-	-	-
85.	16.84. Fejlesztési folyamat, szabványok és eszközök – Biztonsági eseménykezelési terv	16.84. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy a fejlesztési folyamat részeként készítse el, vezesse be és tesztelje a rendszer biztonsági eseménykezelési tervét.	-	-	-
86.	16.85. Fejlesztési folyamat, szabványok és eszközök – Rendszer vagy rendszerelem archiválása	16.85. A szervezet megköveteli az EIR vagy rendszerelem fejlesztőjétől, hogy archiválja a kiadásra vagy szállításra kerülő rendszert vagy rendszerelemet a végső biztonsági felülvizsgálatot alátámasztó bizonyítékokkal együtt.	-	-	-
87.	16.86. Szoftverfejlesztők oktatása	16.86. A szervezet kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről.	-	-	X
88.	16.87. Fejlesztői biztonsági architektúra és tervezés	16.87. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervezési specifikációt és biztonsági architektúrát hozzon létre, amely: 16.87.1. Illeszkedik a szervezet biztonsági architektúrájához és támogatja azt. 16.87.2. Leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között. 16.87.3. Bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.	-	-	X
89.	16.88. Fejlesztői biztonsági architektúra és tervezés – Formális szabályzati modell	16.88. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.88.1. a fejlesztési folyamat szerves részeként hozzon létre egy formális szabályzati modellt, amely tartalmazza az érvényesítendő szervezeti biztonsági elemeket; és 16.88.2. gondoskodjon a formális szabályzati modell belső konzisztenciájának biztosításáról olyan módon, hogy az megfeleljen az előírt szervezeti biztonsági szabályoknak.	-	-	-
90.	16.89. Fejlesztői biztonsági architektúra és tervezés – Biztonsági szempontból kiemelt rendszerelemek	16.89. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.89.1. határozza meg a biztonsági szempontból releváns hardvert, szoftvert és firmware-t; és 16.89.2. szolgáltasson indoklást arra vonatkozóan, hogy a biztonsági szempontból releváns hardver, szoftver és firmware meghatározás miért tekinthető teljesnek.	-	-	-

91.	16.90. Fejlesztői biztonsági architektúra és tervezés – Formalizált specifikáció	16.90. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.90.1. Hozzon létre a fejlesztési folyamat szerves részeként egy formális, magasszintű specifikációt, amely meghatározza a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket, kivételeket, hibaüzeneteket és hatásokat. 16.90.2. Mutassa be és szükség esetén bizonyítékokkal támassza alá, hogy a formális magasszintű specifikáció megfelel a szabályzati modellben meghatározott követelményeknek és elvárásoknak. 16.90.3. Mutassa be és bizonyítékokkal támassza alá, hogy a formális magasszintű specifikáció megfelel a szabályzati modellben meghatározott követelményeknek és elvárásoknak. 16.90.4. Mutassa be, hogy a formális magasszintű specifikáció teljesen lefedi a biztonsági szempontból releváns hardver, szoftver és firmware interfészeket. 16.90.5. Írja le azokat a biztonsági szempontból releváns hardver, szoftver és firmware mechanizmusokat, amelyeket a formális magasszintű specifikáció nem kezel, de a biztonsági szempontból releváns hardveren, szoftveren vagy firmware-en belül működnek.	-	-	-
92.	16.91. Fejlesztői biztonsági architektúra és tervezés – Nem formalizált specifikáció	16.91. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.91.1. A fejlesztési folyamat szerves részeként hozzon létre egy informális, leíró jellegű magasszintű specifikációt, amely meghatározza a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit, kivételeket, hibajelzéseket és hatásokat. 16.91.2. Mutassa be és megfelelő érvekkel támassza alá, hogy a leíró jellegű magasszintű specifikáció megfelel a szervezet szoftverfejlesztésre vonatkozó elvárásainak. 16.91.3. Mutassa be informális bemutatóval, hogy a leíró jellegű magasszintű specifikáció teljes körűen lefedi a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit. 16.91.4. Bizonyítsa, hogy a leíró jellegű magasszintű specifikáció pontosan leírja a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek interfészeit; és 16.91.5. írja le azokat a mechanizmusokat, amelyeket nem vesz figyelembe a leíró jellegű magasszintű specifikáció, de a biztonsági szempontból releváns hardveren, szoftveren vagy firmware-en belül működnek.	-	-	-
93.	16.92. Fejlesztői biztonsági architektúra és tervezés – Egyszerű tervezési koncepció	16.92. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.92.1. úgy tervezze és strukturálja a biztonsági szempontból releváns hardvereket, szoftvereket és firmware-eket, hogy azok teljes, koncepcionálisan egyszerű védelmi mechanizmusokat alkalmazzanak, és amelyeknek a szemantikája pontosan meghatározott; és 16.92.2. a biztonsági szempontból releváns hardverek, szoftverek és firmware-ek belső struktúráját ezen védelmi mechanizmus figyelembevételével alakítsa ki.	-	-	-
94.	16.93. Fejlesztői biztonsági architektúra és tervezés – Tesztelési struktúra	16.93. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan módon strukturálja a rendszereket és rendszerelemeket, hogy azok könnyen tesztelhetők legyenek a biztonsági hibák és sérülékenységek szempontjából.	-	-	-
95.	16.94. Fejlesztői biztonsági architektúra és tervezés – Struktúra a legkisebb jogosultság elvéhez	16.94. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy úgy strukturálja a biztonsági szempontból releváns hardvert, szoftvert és firmware-t, hogy könnyen megvalósítható legyen a legkisebb jogosultság elvén alapuló hozzáférési szabályozás.	-	-	-

96.	16.95. Fejlesztői biztonsági architektúra és tervezés – Összehangolás	16.95. A szervezet meghatározza és megtervezi azokat a szervezet működése szempontjából kritikus EIR-eket, vagy rendszerelemeket, amelyek összehangoltan működnek a szervezet által meghatározott képességek végrehajtása érdekében.	-	-	-
97.	16.96. Fejlesztői biztonsági architektúra és tervezés – Tervezési modellek diverzifikálása	16.96. A szervezet különböző tervezési modelleket alkalmaz az általa meghatározott és a szervezet működése szempontjából kritikus EIR-ek, vagy rendszerelemek esetében, hogy kielégítsen egy közös követelménykészletet vagy, hogy egyenértékű funkcionalitást biztosítson.	-	-	-
98.	16.97. Kritikus rendszerelemek egyedi fejlesztése	16.97. A szervezet újratervezi vagy egyedileg továbbfejleszti az általa meghatározott és a szervezet működése szempontjából kritikus rendszerelemeket.	-	-	-
99.	16.98. Külső fejlesztők háttérellenőrzése	16.98. A szervezet megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy: 16.98.1. rendelkezzen a hivatalos feladatok alapján meghatározott megfelelő hozzáférési jogosultságokkal; és 16.98.2. teljesítse a szervezet által meghatározott további átvilágítási kritériumokat.	-	-	X
100.	16.99. Támogatással nem rendelkező rendszerelemek	16.99. A szervezet: 16.99.1. lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve 16.99.2. a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.	X	X	X
101.	16.100. Speciális követelmények	16.100. A szervezet tervezési, módosítási, bővítési vagy újrakonfigurálási eljárásokat alkalmaz azon rendszereken vagy rendszerelemeken, amelyek a szervezet számára nélkülözhetetlen szolgáltatásokat vagy funkciókat támogatnak.	-	-	-

17. Rendszer- és kommunikációvédelem

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	17.1. Szabályzat és eljárásrendek	17.1. A szervezet: 17.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 17.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és kommunikációvédelmi szabályzatot, amely 17.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 17.1.1.1.2. összhangban van a szervezetre vonatkozó hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 17.1.1.2. a rendszer- és kommunikációvédelmi eljárásrendet, amely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 17.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 17.1.3. Felülvizsgálja és frissíti az aktuális rendszer- és kommunikációvédelmi szabályzatot és a rendszer- és kommunikációvédelmi eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	17.2. Rendszer és felhasználói funkciók szétválasztása	17.2. Az EIR szétválasztja a felhasználók által elérhető funkciókat - beleértve a felhasználói interfész szolgáltatásait - a rendszer üzemeltetési funkcióktól.	-	X	X
4.	17.3. Rendszer és felhasználói funkciók szétválasztása – Nem privilegizált felhasználók interfészei	17.3. Az EIR megakadályozza a rendszerüzemeltetési funkciók megjelenítését a felhasználói interfészeken a nem privilegizált felhasználók számára.	-	-	-
5.	17.4. Biztonsági funkciók elkülönítése	17.4. Az EIR elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.	-	-	X
6.	17.5. Biztonsági funkciók elkülönítése – Hardver szintű	17.5. Az EIR hardver szintű mechanizmusokat alkalmaz a biztonsági funkciók elkülönítésére.	-	-	-
7.	17.6. Biztonsági funkciók elkülönítése – Hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő biztonsági funkciók	17.6. Az EIR elkülöníti a hozzáférés-felügyeleti és információáramlási szabályokat érvényesítő biztonsági funkciókat a nem biztonsági funkcióktól, valamint az egyéb biztonsági funkcióktól.	-	-	-
8.	17.7. Biztonsági funkciók elkülönítése – Nem biztonsági funkciók számának minimalizálása	17.7. Az EIR minimalizálja a biztonsági funkciókat tartalmazó izolációs határon belüli nem biztonsági funkciók számát.	-	-	-
9.	17.8. Biztonsági funkciók elkülönítése – Modulok összekapcsolása és összetartása	17.8. Az EIR a biztonsági funkciókat nagymértékben független modulokként valósítja meg, amelyek maximalizálják a modulokon belüli belső összhangot, és minimalizálják a modulok közötti összekapcsoltságot.	-	-	-
10.	17.9. Biztonsági funkciók elkülönítése – Réteges szerkezetek	17.9. A szervezet a biztonsági funkciókat többrétegű struktúraként valósítja meg, minimalizálva a tervezés rétegei közötti kölcsönhatásokat, és elkerülve, hogy az alsóbb rétegek függjenek a magasabb rétegek funkcionalitásától vagy helyességétől.	-	-	-

11.	17.10. Információk az osztott használatú rendszererőforrásokban	17.10. Az EIR meggátolja a megosztott erőforrásokon keresztül történő jogosulatlan vagy véletlen információátvitelt.	-	X	X
12.	17.11. Információk az osztott használatú rendszererőforrásokban – Többszintű vagy időszakos feldolgozás	17.11. Az EIR megakadályozza az engedély nélküli információátvitelt a megosztott erőforrásokon keresztül, a szervezet által meghatározott eljárásokat követve a különböző biztonsági besorolású információk vagy biztonsági osztályok között.	-	-	-
13.	17.12. Szolgáltatásmegtagadással járó támadások elleni védelem	17.12. A szervezet: 17.12.1. védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait; és 17.12.2. alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját.	X	X	X
14.	17.13. Szolgáltatásmegtagadással járó támadások elleni védelem – Más rendszerek megtámadásának korlátozása	17.13. A szervezet korlátozza az egyének képességét, hogy meghatározott szolgáltatásmegtagadással járó támadásokat indíthassanak más rendszerek ellen.	-	-	-
15.	17.14. Szolgáltatásmegtagadással járó támadások elleni védelem – Kapacitás, sávszélesség, redundancia	17.14. A szervezet kezeli a kapacitásokat, sávszélességeket, egyéb redundanciákat, hogy korlátozza az információs elárasztás által okozott szolgáltatásmegtagadással járó támadások hatásait.	-	-	-
16.	17.15. Szolgáltatásmegtagadással járó támadások elleni védelem – Észlelés és felügyelet	17.15. A szervezet: 17.15.1. Olyan, a szervezet által meghatározott felügyeleti eszközöket alkalmaz, amelyek képesek észlelni az EIR ellen vagy az EIR-ből kezdeményezett szolgáltatásmegtagadással járó támadások jeleit. 17.15.2. Figyelemmel kíséri a meghatározott EIR erőforrásait annak megállapítása érdekében, hogy megbizonyosodjon arról, hogy elegendő erőforrás áll-e rendelkezésre a hatékony szolgáltatásmegtagadással járó támadások megakadályozásához.	-	-	-
17.	17.16. Erőforrások rendelkezésre állása	17.16. A szervezet úgy védi erőforrásainak rendelkezésre állását, hogy a szervezet által meghatározott erőforrásokat prioritás, kvóta vagy a szervezet által meghatározott egyéb követelmények alapján osztja szét.	-	-	-
18.	17.17. A határok védelme	17.17. A szervezet: 17.17.1. Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein. 17.17.2. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól. 17.17.3. Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez.	X	X	X
19.	17.18. A határok védelme – Hozzáférési pontok	17.18. A szervezet korlátozza az EIR külső hálózati kapcsolatainak számát.	-	X	X

20.	17.19. A határok védelme – Külső infokommunikációs szolgáltatások	17.19. A szervezet: 17.19.1. Menedzselt interfészt alkalmaz minden külső infokommunikációs szolgáltatáshoz. 17.19.2. Minden menedzselt interfészhez forgalomáramlási szabályokat alakít ki. 17.19.3. Védi az egyes interfészeken átvitelre kerülő információk bizalmasságát és sértetlenségét. 17.19.4. Dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó működési céllal vagy üzleti igénnyel, valamint az igényelt kivétel időtartamával együtt. 17.19.5. Meghatározott gyakorisággal felülvizsgálja a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket nem támogat valamilyen működési cél vagy üzleti igény. 17.19.6. Megakadályozza a nem engedélyezett vezérlőadat-forgalom (control plane traffic) cseréjét a külső hálózatokkal. 17.19.7. Közzéteszi azokat az információkat, amelyek lehetővé teszik a távoli hálózatok számára a nem engedélyezett vezérlőadat-forgalom (control plane traffic) észlelését a belső hálózatokból. 17.19.8. Szűri a nem engedélyezett vezérlőadat-forgalmat a külső hálózatokból.	-	X	X
21.	17.20. A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés	17.20. Az EIR alapértelmezés szerint elutasítja a hálózati kommunikációs forgalmat, és csak kivételként engedélyezi azt a menedzselt interfészeknél.	-	X	X
22.	17.21. A határok védelme – Megosztott csatornahasználat távoli eszközök esetén	17.21. Az EIR megakadályozza a megosztott csatornahasználatot az EIR-ekhez csatlakozó távoli eszközök számára, kivéve, ha a megosztott csatornát biztonságosan konfigurálják a szervezet által meghatározott védelmi intézkedések használatával.	-	X	X
23.	17.22. A határok védelme – A forgalom átirányítása hitelesített proxykiszolgálókra	17.22. Az EIR a meghatározott belső kommunikációs forgalmat a meghatározott külső hálózatok felé a menedzselt interfészeken lévő hitelesített proxykiszolgálókon keresztül irányítja.	-	X	X
24.	17.23. A határok védelme – Korlátozza a fenyegető kimenő kommunikációs forgalmat	17.23. Az EIR: 17.23.1. észleli és megtagadja a kimenő kommunikációs forgalmat, amely fenyegetést jelent a külső rendszerek számára; és 17.23.2. ellenőrzi a megtagadott kommunikációval kapcsolatos belső felhasználók személyazonosságát.	-	-	-
25.	17.24. A határok védelme – Információ kiszivárgásának megakadályozása	17.24. A szervezet: 17.24.1. megakadályozza az információk kiszivárgását, és 17.24.2. meghatározott gyakorisággal információszivárgási teszteket hajt végre.	-	-	-
26.	17.25. A határok védelme – A bejövő kommunikációs forgalom korlátozása	17.25. Az EIR csak a szervezet által meghatározott, engedélyezett forrásokból származó bejövő adatforgalmat továbbítja a szervezet által meghatározott, engedélyezett célpontok felé.	-	-	-
27.	17.26. A határok védelme – Hosztalapú védelem	17.26. A szervezet az általa meghatározott hosztalapú határvédelmi mechanizmusokat megvalósítja a meghatározott rendszerelemeken.	-	-	-
28.	17.27. A határok védelme – A biztonsági eszközök, mechanizmusok és támogató rendszerelemek elkülönítése	17.27. A szervezet az általa meghatározott információbiztonsági eszközöket, mechanizmusokat és támogató rendszerelemeket fizikailag különálló alhálózatok létrehozásával és menedzselt interfészek alkalmazásával különíti el az EIR többi belső rendszerelemétől.	-	-	-
29.	17.28. A határok védelme – Védelem az engedély nélküli fizikai kapcsolatok kialakítása ellen	17.28. A szervezet védekezik a jogosulatlan fizikai csatlakozások ellen a szervezet által meghatározott menedzselt interfészeknél.	-	-	-
30.	17.29. A határok védelme – Hálózati privilegizált hozzáférések	17.29. Az EIR a privilegizált hálózati hozzáféréseket a hozzáférés-felügyelete és átvizsgálása céljából egy erre a célra dedikált, menedzselt interfészen keresztül irányítja.	-	-	-

31.	17.30. A határok védelme – Rendszerelemek felfedezésének megakadályozása	17.30. Az EIR megakadályozza a menedzselt interfészekkel rendelkező konkrét rendszerelemek felderítését.	-	-	-
32.	17.31. A határok védelme – A protokoll formátumok betartása	17.31. Az EIR kikényszeríti a protokoll formátumok betartását.	-	-	-
33.	17.32. A határok védelme – Biztonságos állapot fenntartása	17.32. A szervezet megakadályozza, hogy az EIR nem biztonságos állapotba kerüljön egy határvédelmi berendezés működési hibája esetén.	-	-	X
34.	17.33. A határok védelme – Kommunikáció blokkolása nem szervezeti konfigurációval rendelkező gépekről	17.33. Az EIR blokkolja a bejövő és a kimenő kommunikációs forgalmat azok között a kliensek között, amelyeket a végfelhasználók és a külső szolgáltatók a szervezettől függetlenül konfigurálnak.	-	-	-
35.	17.34. A határok védelme – Dinamikus elszigetelés és elkülönítés	17.34. Az EIR képes dinamikusan elkülöníteni a szervezet által meghatározott rendszerelemeket a többi rendszerelemtől.	-	-	-
36.	17.35. A határok védelme – Rendszerelemek elkülönítése	17.35. A szervezet határvédelmi mechanizmusokat alkalmaz a szervezet által meghatározott rendszerelemek elkülönítésére, amelyek a szervezet által meghatározott célokat és üzleti funkciókat támogatják.	-	-	X
37.	17.36. A határok védelme – Különálló alhálózatok a különböző biztonsági tartományokhoz való csatlakozáshoz	17.36. A szervezet különböző hálózati címeket hoz létre a különböző biztonsági tartományokban elhelyezett rendszerekhez való csatlakozáshoz.	-	-	-
38.	17.37. A határok védelme – Visszajelzés küldésének letiltása a protokoll ellenőrzési hiba esetén	17.37. Az EIR letiltja a visszajelzés küldését a feladónak, amennyiben protokollformátum-ellenőrzési hiba lép fel.	-	-	-
39.	17.38. A határok védelme – Nyilvános hálózathoz történő csatlakozás tiltása	17.38. A szervezet tiltja a meghatározott EIR nyilvános hálózathoz történő közvetlen csatlakozását.	-	-	-
40.	17.39. A határok védelme – Különálló alhálózatok a funkciók elkülönítéséhez	17.39. A szervezet fizikailag vagy logikailag elkülönített alhálózatokat alakít ki a szervezet működése szempontjából kritikus rendszerelemek és funkciók elkülönítése érdekében.	-	-	-
41.	17.40. Az adatátvitel bizalmassága és sértetlensége	17.40. Az EIR megvédi a továbbított információk bizalmasságát és sértetlenségét.	-	X	X
42.	17.41. Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem	17.41. Az EIR kriptográfiai mechanizmusokat alkalmaz az adatátvitel során, hogy megelőzze az információk jogosulatlan felfedését, illetve kimutassa az információk módosításait.	-	X	X
43.	17.42. Az adatátvitel bizalmassága és sértetlensége – Az adatok átvitel előtti és utáni kezelése	17.42. Az EIR fenntartja az információ bizalmasságát és sértetlenségét a továbbítás előkészítése és a fogadás során.	-	-	-
44.	17.43. Az adatátvitel bizalmassága és sértetlensége – Üzenetek kriptográfiai védelme külső fogadó fél esetén	17.43. A szervezet kriptográfiai mechanizmusokat alkalmaz az üzenetek külső adatainak (például: fejléc) védelmére, kivéve, ha azokat a szervezet által kijelölt alternatív fizikai védelmi mechanizmusok védik.	-	-	-
45.	17.44. Az adatátvitel bizalmassága és sértetlensége – Kommunikáció elrejtése vagy randomizálása	17.44. A szervezet kriptográfiai mechanizmusokat alkalmaz a kommunikációs mintázatok elrejtésére vagy randomizálására, ha azokat nem védi más, a szervezet által meghatározott alternatív fizikai intézkedés.	-	-	-
46.	17.45. Az adatátvitel bizalmassága és sértetlensége – Védett elosztórendszer	17.45. A szervezet egy, a szervezet által meghatározott védett elosztórendszert alkalmaz, melynek célja az információ jogosulatlan nyilvánosságra hozatalának megakadályozása, valamint az információban bekövetkező változások észlelése a továbbítás során.	-	-	-
47.	17.46. A hálózati kapcsolat megszakítása	17.46. Az EIR megszakítja a hálózati kapcsolatot a kommunikációs munkaszakasz befejezésekor vagy meghatározott időtartamú inaktivitás után.	-	X	X

48.	17.47. Megbízható útvonal	17.47. Az EIR: 17.47.1. Egy fizikailag vagy logikailag elkülönített, megbízható kommunikációs útvonalat biztosít a felhasználók és az EIR megbízható elemei közötti kommunikációhoz. 17.47.2. Lehetővé teszi a felhasználók számára, hogy ezt a megbízható kommunikációs útvonalat használják a felhasználók és a rendszer biztonsági funkciói közötti kommunikációra, beleértve a hitelesítést és az újrahitelesítést, valamint további, a szervezet által meghatározott biztonsági funkciókat.	-	-	-
49.	17.48. Megbízható útvonal – Megmásíthatatlan útvonal	17.48. Az EIR: 17.48.1. egy olyan megbízható kommunikációs útvonalat biztosít, amely egyértelműen megkülönböztethető más kommunikációs útvonalaktól; 17.48.2. kezdeményezi a megbízható kommunikációs útvonalat a rendszer meghatározott biztonsági funkciói és a felhasználó közötti kommunikációhoz.	-	-	-
50.	17.49. Kriptográfiai kulcs előállítása és kezelése	17.49. A szervezet előállítja és kezeli a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.	X	X	X
51.	17.50. Kriptográfiai kulcs előállítása és kezelése – Rendelkezésre állás	17.50. A szervezet biztosítja az információk rendelkezésre állását abban az esetben is, amikor a felhasználók elveszítik a kriptográfiai kulcsaikat.	-	-	X
52.	17.51. Kriptográfiai kulcs előállítása és kezelése – Aszimmetrikus kulcsok	17.51. A szervezet előállítja, felügyeli és terjeszti az aszimmetrikus kriptográfiai kulcsokat a legjobb iparági gyakorlatnak megfelelő kulcskezelési technológia és kulcskezelési folyamatok alkalmazásával.	-	-	-
53.	17.52. Kriptográfiai kulcs előállítása és kezelése – Kulcsok fizikai felügyelete	17.52. A szervezet megőrzi a kriptográfiai kulcsok fizikai felügyeletét, ha a tárolt információkat külső szolgáltatók titkosítják.	-	-	-
54.	17.53. Kriptográfiai védelem	17.53. A szervezet: 17.53.1. meghatározza a kriptográfia szervezeten belüli felhasználási területeit; és 17.53.2. megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.	X	X	X
55.	17.54. Együttműködésen alapuló informatikai eszközök	17.54. A szervezet: 17.54.1. tiltja az együttműködésen alapuló számítástechnikai eszközök (például: kamerák, mikrofonok) és alkalmazások távoli aktiválását, a szervezet által meghatározott kivételekkel; és 17.54.2. egyértelmű visszajelzést ad a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.	X	X	X
56.	17.55. Együttműködésen alapuló informatikai eszközök – Fizikai vagy logikai szétkapcsolás	17.55. A szervezet biztosítja az együttműködésen alapuló számítástechnikai eszközök egyszerű és könnyű fizikai vagy logikai szétkapcsolását.	-	-	-
57.	17.56. Együttműködésen alapuló informatikai eszközök – Biztonságos munkaterületek	17.56. A szervezet letiltja vagy eltávolítja a meghatározott biztonságos munkaterületeken található együttműködésen alapuló számítástechnikai eszközöket és alkalmazásokat a meghatározott EIR-ekből, vagy rendszerelemekből.	-	-	-
58.	17.57. Együttműködésen alapuló informatikai eszközök – Résztvevők egyértelmű felsorolása	17.57. A szervezet biztosítja az általa meghatározott online megbeszéléseken és telefonkonferenciákon a résztvevők egyértelmű felsorolását.	-	-	-
59.	17.58. Biztonsági tulajdonságok átvitele	17.58. A szervezet meghatározott biztonsági tulajdonságokat rendel a rendszerek és rendszerelemek között kicserélt információkhoz.	-	-	-
60.	17.59. Biztonsági tulajdonságok átvitele – Sértetlenség ellenőrzése	17.59. Az EIR ellenőrzi a továbbított biztonsági tulajdonságok sértetlenségét.	-	-	-
61.	17.60. Biztonsági tulajdonságok átvitele – Megtévesztés elleni mechanizmusok	17.60. Az EIR hamisítás elleni mechanizmusok alkalmaz annak megakadályozására, hogy a rosszindulatú személyek meghamisítsák a biztonsági eljárás sikeres alkalmazását jelző biztonsági tulajdonságokat.	-	-	-

62.	17.61. Biztonsági tulajdonságok átvitele – Kriptográfiai kötés	17.61. A szervezet meghatározott mechanizmusokat vagy technikákat alkalmaz, hogy a biztonsági tulajdonságokat az átvitt információhoz kösse.	-	-	-
63.	17.62. Nyilvános kulcsú infrastruktúra tanúsítványok	17.62. A szervezet: 17.62.1. nyilvános kulcsú tanúsítványokat állít ki a szervezet által meghatározott tanúsítványkiadási szabályok szerint, vagy nyilvános kulcsú tanúsítványokat szerez be egy bizalmi szolgáltatótól; és 17.62.2. a szervezet által kezelt tanúsítványtárolókban, csak jóváhagyott, hitelesített tanúsítvány vehető fel.	-	X	X
64.	17.63. Mobilkód korlátozása	17.63. A szervezet: 17.63.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat, valamint a mobilkód technológiákat; valamint 17.63.2. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az EIR-en belül.	-	X	X
65.	17.64. Mobilkód korlátozása – Nem elfogadható kód azonosítása és korrektív intézkedések	17.64. A szervezet azonosítja a meghatározott nem elfogadható mobilkódot, majd meghatározott korrekciós intézkedéseket hajt végre.	-	-	-
66.	17.65. Mobilkód korlátozása – Beszerzés, fejlesztés és használat	17.65. A szervezet ellenőrzi, hogy a rendszerben telepítendő mobilkód beszerzése, fejlesztése és használata megfelel-e a szervezet által meghatározott mobilkódokra vonatkozó követelményeknek.	-	-	-
67.	17.66. Mobilkód korlátozása – Letöltés és kódvégrehajtás megakadályozása	17.66. A szervezet megakadályozza az általa meghatározott nem elfogadható mobilkód letöltését és végrehajtását.	-	-	-
68.	17.67. Mobilkód korlátozása – Automatikus kódvégrehajtás megakadályozása	17.67. A szervezet megakadályozza a mobilkódok automatikus végrehajtását a meghatározott szoftverekben, valamint kikényszeríti a meghatározott intézkedések végrehajtását a mobilkódok futtatása előtt.	-	-	-
69.	17.68. Mobilkód korlátozása – Csak zárt környezetekben való kódvégrehajtás	17.68. A szervezet a jóváhagyott mobilkód futtatását kizárólag zárt, virtualizált környezetben engedélyezi.	-	-	-
70.	17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)	17.69. Az EIR: 17.69.1. A név- és címfeloldási kérésekre a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosít. 17.69.2. Amennyiben egy elosztott, hierarchikus névtér részeként működik, jelzi a gyermektartományok biztonsági állapotát is, és ha azok támogatják a biztonságos névfeloldási szolgáltatásokat, lehetővé teszi a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.	X	X	X
71.	17.70. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) – Adat forrása és bizalmassága	17.70. Az EIR biztosítja az adatok eredetiségének és sértetlenségének a védelmét a belső név- és címfeloldási lekérdezések során.	-	-	-
72.	17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	17.71. Az EIR eredet-hitelesítést és adatsértetlenség-ellenőrzést kér és hajt végre a hiteles forrásból származó név- és címfeloldó válaszokon.	X	X	X
73.	17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	17.72. A szervezet számára név- és címfeloldási szolgáltatást együttesen biztosító EIR-ek hibatűrő képességgel rendelkeznek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.	X	X	X
74.	17.73. Munkaszakasz hitelessége	17.73. Az EIR védi a kommunikációs munkaszakaszok hitelességét.	-	X	X
75.	17.74. Munkaszakasz hitelessége – Munkaszakasz-azonosítók érvénytelenítése kijelentkezéskor	17.74. Az EIR érvényteleníti a felhasználói munkaszakasz azonosítóját, amikor a felhasználó kijelentkezik, vagy a munkaszakasz más módon befejeződik.	-	-	-
76.	17.75. Munkaszakasz hitelessége – A rendszer által generált egyedi munkaszakasz-azonosítók	17.75. Az EIR minden munkaszakaszhoz egyedi munkaszakasz-azonosítót hoz létre a szervezet által meghatározott véletlenszerűségi követelményeknek megfelelően, és csak a rendszer által generált munkaszakasz-azonosítókat fogadja el.	-	-	-

77.	17.76. Munkaszakasz hitelessége – Engedélyezett tanúsítvány kibocsájtók	17.76. A szervezet a védett munkaszakasz létrehozásának ellenőrzésére csak a szervezet által meghatározott tanúsítványkibocsátók tanúsítványainak használatát engedélyezi.	-	-	-
78.	17.77. Ismert állapotba való visszatérés	17.77. A rendszer meghatározott rendszerelemei a meghatározott hibák bekövetkezése estén megőrzik a hiba bekövetkezése előtti ismert rendszerállapotukat.	-	-	X
79.	17.78. Funkcionalitás és információtárolás minimalizálása	17.78. A szervezet minimális funkcionalitást és információtárolást alkalmaz a meghatározott rendszerelemeken.	-	-	-
80.	17.79. Csapdák alkalmazása	17.79. A szervezet kifejezetten rosszindulatú támadások célpontjául szolgáló elemeket épít be a szervezeti EIR-ekbe, hogy az ilyen támadásokat észlelni, elhárítani és elemezni tudja.	-	-	-
81.	17.80. Platform-független alkalmazások	17.80. A platformfüggetlen alkalmazásokat a szervezet az EIR-ek közé sorolja.	-	-	-
82.	17.81. Tárolt (at rest) adatok védelme	17.81. A szervezet megóvja a meghatározott tárolt, illetve archivált (at rest) adatok bizalmasságát és sértetlenségét a feldolgozás vagy továbbítás alatt álló adatokkal megegyező szinten.	-	X	X
83.	17.82. Tárolt (at rest) adatok védelme – Kriptográfiai védelem	17.82. A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz a szervezet által meghatározott tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére.	-	X	X
84.	17.83. Tárolt (at rest) adatok védelme – Offline tárhely	17.83. A szervezet eltávolítja a meghatározott információkat az online tárhelyekről, és biztonságos offline tárhelyeken tárolja azokat.	-	-	-
85.	17.84. Tárolt (at rest) adatok védelme – Kriptográfiai kulcsok	17.84. A szervezet meghatározott óvintézkedések és hardveres kulcstároló alkalmazásával biztosítja a kriptográfiai kulcsok védett tárolását.	-	-	-
86.	17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák	17.85. A szervezet EIR-ének meghatározott rendszereleimben különböző technológián alapú összetevőket alkalmaz.	-	-	-
87.	17.86. Heterogenitás – Virtualizációs technikák	17.86. A szervezet meghatározott gyakorisággal frissített virtualizációs technológiákat alkalmaz a különböző operációs rendszerek és alkalmazások telepítésének támogatására.	-	-	-
88.	17.87. Elfedés és megtévesztés	17.87. A szervezet meghatározott elrejtési és félrevezetési technikákat alkalmaz a meghatározott EIR-ekben és időszakokban, annak érdekében, hogy összezavarja és félrevezesse az ellenséges szándékú felhasználókat.	-	-	-
89.	17.88. Elfedés és megtévesztés – Véletlenszerűség	17.88. A szervezet meghatározott technikákat alkalmaz a véletlenszerűség bevezetésére a szervezeti működésbe és eszközökbe.	-	-	-
90.	17.89. Elfedés és megtévesztés – Feldolgozási és tárolási helyek megváltoztatása	17.89. A szervezet meghatározott gyakorisággal vagy eseti jelleggel módosítja az információk feldolgozási, vagy tárolási helyét.	-	-	-
91.	17.90. Elfedés és megtévesztés – Félrevezető információ	17.90. A szervezet valósághű, de félrevezető információkat alkalmaz a meghatározott rendszerelemekben azok biztonsági állapotáról vagy helyzetéről.	-	-	-
92.	17.91. Elfedés és megtévesztés – Rendszerelemek elrejtése	17.91. A szervezet meghatározott technikákat alkalmaz a meghatározott rendszerelemek elrejtésére vagy álcázására.	-	-	-
93.	17.92. Rejtett csatornák elemzése	17.92. A szervezet: 17.92.1. Elemzi a rejtett csatornákat a rendszeren belüli kommunikáció azon aspektusainak azonosítása érdekében, amelyek potenciális útvonalak lehetnek a rejtett tároló vagy időzítő csatornák számára. 17.92.2. Megbecsüli a rejtett csatornák maximális sávszélességét.	-	-	-
94.	17.93. Rejtett csatornák elemzése – Rejtett csatornák tesztelése a kihasználhatóság szempontjából	17.93. A szervezet az azonosított rejtett csatornák egy részén tesztelést hajt végre kihasználhatóságuk megállapítása érdekében.	-	-	-
95.	17.94. Rejtett csatornák elemzése – Maximális sávszélesség	17.94. A szervezet csökkenti az azonosított rejtett (tárolási és időzítési) csatornák maximális sávszélességét.	-	-	-

96.	17.95. Rejtett csatornák elemzése – Sávszélesség mérése éles környezetben	17.95. A szervezet megméri a meghatározott és azonosított rejtett csatornák sávszélességét a rendszer működési környezetében.	-	-	-
97.	17.96. Rendszer felosztása	17.96. A szervezet az EIR-t meghatározott rendszerelemekre osztja fel, amelyek külön fizikai vagy logikai tartományokban vagy környezetekben helyezkednek el, a szervezet által meghatározott elkülönítési körülményeknek megfelelően.	-	-	-
98.	17.97. Rendszer felosztása – Fizikai tartományok különválasztása a privilegizált funkciókhoz	17.97. A szervezet a privilegizált funkciókat külön fizikai tartományokba osztja szét.	-	-	-
99.	17.98. Végrehajtható, de nem módosítható programok	17.98. A szervezet meghatározott rendszerelemek esetében: 17.98.1. a működési környezet betöltését és futtatását csak hardveresen kikényszerített, csak olvasható adathordozóról engedélyezi; 17.98.2. az alkalmazások betöltését és futtatását csak hardveresen kikényszerített, csak olvasható adathordozóról engedélyezi.	-	-	-
100.	17.99. Végrehajtható, de nem módosítható programok – Nem írható tárolóeszköz	17.99. A szervezet meghatározott rendszerelemek esetében olyan nem írható tárolóeszközöket alkalmaz, amelyek a rendszerelemek újraindítása vagy be- és kikapcsolása után is folyamatosan fennmaradnak.	-	-	-
101.	17.100. Végrehajtható, de nem módosítható programok – Sértetlenség védelme az írásvédett adathordozón	17.100. A szervezet gondoskodik az információ sértetlenségének védelméről még az írásvédett adathordozón történő rögzítés előtt, és ellenőrzi az adathordozót, miután adatokat rögzített rá.	-	-	-
102.	17.101. Külső kártékony kódok azonosítása	17.101. Az EIR olyan rendszerelemeket tartalmaz, amelyek proaktívan keresik és azonosítják a hálózat alapú kártékony kódokat vagy kártékony weboldalakat.	-	-	-
103.	17.102. Elosztott feldolgozás és tárolás	17.102. A szervezet a meghatározott adatfeldolgozó és tároló rendszerelemeket több fizikai helyszínen és több logikai tartomány között osztja szét.	-	-	-
104.	17.103. Elosztott feldolgozás és tárolás – Mérési technikák	17.103. A szervezet: 17.103.1. Tesztelési technikákat alkalmaz az elosztott feldolgozó és tároló rendszerelemek lehetséges zavarainak, hibáinak vagy kompromittálódásának azonosítására. 17.103.2. Zavarok, hibák vagy kompromittálódások azonosítása esetén a szervezet által meghatározott válaszintézkedéseket foganatosítja.	-	-	-
105.	17.104. Elosztott feldolgozás és tárolás – Szinkronizáció	17.104. A szervezet szinkronizálja az általa meghatározott redundáns rendszereket vagy rendszerelemeket.	-	-	-
106.	17.105. Sávon kívüli csatornák	17.105. A szervezet meghatározott sávon kívüli (out-of-band) csatornákat alkalmaz a kijelölt információk, rendszerelemek vagy eszközök fizikai szállításához vagy elektronikus továbbításához a kijelölt személyek vagy rendszerek számára.	-	-	-
107.	17.106. Sávon kívüli csatornák – Átvitel és továbbítás biztosítása	17.106. A szervezet kontrollmechanizmusokat alkalmaz annak biztosítására, hogy csak a feljogosított személyek vagy rendszerek férhessenek hozzá bizonyos, a szervezet által meghatározott információkhoz, rendszerelemekhez és eszközökhöz.	-	-	-
108.	17.107. Működésbiztonság	17.107. A szervezet meghatározott működésbiztonsági követelményeket alkalmaz a szervezet működése szempontjából kritikus információk védelme érdekében a rendszerfejlesztési életciklus során.	-	-	-
109.	17.108. A folyamatok elkülönítése	17.108. Az EIR elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.	X	X	X
110.	17.109. Folyamatok elkülönítése – Hardveres elkülönítés	17.109. A szervezet a folyamatok elkülönítését elősegítő hardver szintű mechanizmusokat alkalmaz.	-	-	-

111.	17.110. A folyamatok elkülönítése – Külön végrehajtási tartomány szálanként	17.110. Az EIR külön végrehajtási tartományt tart fenn minden szálon belül a többszálú feldolgozás esetén.	-	-	-
112.	17.111. Vezeték nélküli kapcsolat védelme	17.111. A szervezet védelmet biztosít a meghatározott vezeték nélküli kapcsolatok számára a meghatározott jelparaméter-támadásokkal, valamint az ilyen támadások forrásaira történő hivatkozásokkal szemben.	-	-	-
113.	17.112. Vezeték nélküli kapcsolat védelme – Elektromágneses interferencia	17.112. A szervezet olyan kriptográfiai mechanizmusokat valósít meg, amelyek a meghatározott védelmi szint elérését szolgálják a szándékosan előidézett elektromágneses interferencia hatásaival szemben.	-	-	-
114.	17.113. Vezeték nélküli kapcsolat védelme – Felderítés lehetőségének csökkentése	17.113. A szervezet kriptográfiai módszereket alkalmaz annak érdekében, hogy a szervezet által meghatározott szintre csökkentse a vezeték nélküli kapcsolatok észlelési lehetőségét.	-	-	-
115.	17.114. Vezeték nélküli kapcsolat védelme – Utánzó vagy manipulatív megtévesztés	17.114. A szervezet olyan kriptográfiai mechanizmusokat alkalmaz, amelyek azonosítják és visszautasítják azokat a vezeték nélküli adatátviteleket, amelyek jelparaméterek figyelembevételével történő elemzés alapján szándékos utánzó vagy manipulatív kommunikációs csalásra utalnak.	-	-	-
116.	17.115. Vezeték nélküli kapcsolat védelme – Jelparaméterek azonosítása	17.115. A szervezet kriptográfiai mechanizmusokat alkalmaz a meghatározott vezeték nélküli adók jelparamétereinek felhasználásával történő nem kívánt hozzáférés megakadályozására.	-	-	-
117.	17.116. Portok, illetve ki- és bemeneti eszközök hozzáférése	17.116. A szervezet fizikailag vagy logikailag letiltja vagy eltávolítja a meghatározott csatlakozókat, vagy be- és kimeneti eszközöket a meghatározott EIR-eken vagy rendszerelemeken.	-	-	-
118.	17.117. Érzékelő képességei és kapcsolódó adatok	17.117. A szervezet: 17.117.1. megtiltja a meghatározott környezeti érzékelő képességekkel rendelkező eszközök használatát a meghatározott létesítményekben, területeken vagy rendszerekben, továbbá a környezeti érzékelési képességek távoli aktiválását a meghatározott szervezeti EIR-ekben vagy rendszerelemekben, kivéve a szervezet által meghatározott kivételeket; és 17.117.2. egyértelmű jelzést biztosít a szenzor használatáról a meghatározott felhasználói csoport számára.	-	-	-
119.	17.118. Érzékelő képesség és adatok – Jelentés a kijelölt személyeknek vagy szerepköröknek	17.118. A szervezet úgy konfigurálja az EIR-t, hogy az csak a jogosult személyek vagy szerepkörök számára továbbítsa a meghatározott érzékelők által gyűjtött adatokat vagy információkat.	-	-	-
120.	17.119. Érzékelő képesség és adatok – Engedélyezett felhasználás	17.119. A szervezet meghatározott intézkedéseket alkalmaz annak érdekében, hogy a meghatározott érzékelők által gyűjtött adatokat vagy információkat csak engedélyezett célokra lehessen felhasználni.	-	-	-
121.	17.120. Érzékelő képesség és adatok – Adatgyűjtés minimalizálása	17.120. A szervezet olyan érzékelőket alkalmaz, amelyek úgy vannak beállítva, hogy minimalizálják az egyénekről történő szükségtelen információgyűjtést.	-	-	-
122.	17.121. Használati korlátozások	17.121. A szervezet: 17.121.1. kidolgozza a használati korlátozásokat és az alkalmazási irányelveket a szervezet által meghatározott rendszerelemekre; és 17.121.2. engedélyezi, ellenőrzi és szabályozza az ilyen rendszerelemek használatát a rendszeren belül.	-	-	-
123.	17.122. Izolált futtatási környezetek	17.122. A szervezet elszigetelt programfuttatási környezetet alkalmaz a meghatározott rendszerben, rendszerelemben vagy helyszínen.	-	-	-
124.	17.123. Rendszeridő szinkronizálása	17.123. A szervezet szinkronizálja a rendszerórákat a rendszereken belül, valamint a rendszerelemek között.	-	-	-

125.	17.124. Rendszeridő szinkronizálása – Szinkronizálás a hiteles időforrással	17.124.1. A szervezet meghatározott időközönként összehasonlítja a belső rendszerórákat a szervezet által meghatározott hiteles időforrással, és 17.124.2. ha az időkülönbség meghaladja a szervezet által meghatározott időintervallumot, szinkronizálja a belső rendszerórákat a hiteles időforrással.	-	-	-
126.	17.125. Rendszeridő szinkronizálása – Másodlagos hiteles időforrás	17.125.1. A szervezet meghatároz egy olyan másodlagos hiteles időforrást, amely az elsődleges hiteles időforrástól eltérő földrajzi régióban található; és 17.125.2. ha az elsődleges hiteles időforrás nem áll rendelkezésre a belső rendszerórákat a másodlagos hiteles időforráshoz szinkronizálja.	-	-	-
127.	17.126. Tartományok közötti szabályok érvényesítése	17.126. A szervezet fizikai vagy logikai módon érvényesíti a biztonsági szabályzatokat az összekapcsolt biztonsági tartományok fizikai és hálózati interfészei között.	-	-	-
128.	17.127. Alternatív kommunikációs utak	17.127. A szervezet alternatív kommunikációs útvonalakat alakít ki a rendszer működésének szervezeti irányításához és ellenőrzéséhez.	-	-	-
129.	17.128. Érzékelő áthelyezése	17.128. A szervezet a meghatározott érzékelőket és felügyeleti eszközöket a meghatározott helyekre, a meghatározott feltételek és körülmények között dinamikusan helyezi át.	-	-	-
130.	17.129. Érzékelő áthelyezése – Érzékelők vagy felügyeleti képességek dinamikus áthelyezése	17.129. A szervezet a meghatározott érzékelőket és felügyeleti eszközöket a meghatározott helyekre, a meghatározott feltételek és körülmények között dinamikusan helyezi át.	-	-	-
131.	17.130. Hardver szintű szétválasztás és szabályérvényesítés	17.130. A szervezet hardverrel kikényszerített szétválasztási és szabály-kikényszerítési mechanizmusokat alkalmaz a szervezet által meghatározott biztonsági tartományok között.	-	-	-
132.	17.131. Szoftver szintű szétválasztás és szabályérvényesítés	17.131. A szervezet szoftverrel kikényszerített szétválasztási és szabály-kikényszerítési mechanizmusokat alkalmaz a szervezet által meghatározott biztonsági tartományok között.	-	-	-
133.	17.132. Hardver szintű védelem	17.132. A szervezet: 17.132.1. Hardver szintű írásvédelmet alkalmaz a meghatározott rendszer firmware-elemeken. 17.132.2. Egyedi eljárásokat alkalmaz a jogosult személyek számára a hardveres írásvédelem manuális kikapcsolásához, a firmware módosításaihoz, majd az írásvédelem újbóli bekapcsolásához az üzemi állapotba való visszatérés előtt.	-	-	-

18. Rendszer- és információsértetlenség

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	18.1. Szabályzat és eljárásrendek	18.1. A szervezet: 18.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 18.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és információsértetlenségi szabályzatot, amely 18.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 18.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 18.1.1.2. a rendszer- és információsértetlenségi eljárásrendet, amely a rendszer- és információsértetlenségi szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 18.1.2. Kijelöl egy meghatározott személyt, aki a rendszer- és információsértetlenségi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 18.1.3. Felülvizsgálja és frissíti az aktuális rendszer- és információsértetlenségi szabályzatot és a rendszer- és információsértetlenségi eljárásokat a meghatározott gyakorisággal és a meghatározott események bekövetkezését követően.	X	X	X
3.	18.2. Hibajavítás	18.2. A szervezet: 18.2.1. Azonosítja, jelenti és kijavítja az EIR hibáit. 18.2.2. A hibajavítással kapcsolatos szoftverfrissítéseket telepítés előtt teszteli a hatékonyság és a potenciális mellékhatások szempontjából. 18.2.3. A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti. 18.2.4. A hibajavítást beépíti a szervezet konfigurációkezelési folyamatába.	X	X	X
4.	18.3. Hibajavítás – Automatizált hibaelhárítás állapota	18.3. A szervezet meghatározott gyakorisággal a szervezet által meghatározott automatizált mechanizmusokat alkalmaz annak ellenőrzésére, hogy a rendszerelemek rendelkeznek-e a biztonsági szempontból releváns szoftver- és firmware-frissítésekkel.	-	X	X
5.	18.4. Hibajavítás – A hibák kijavításának ideje és a korrekciós intézkedésekre vonatkozó referenciaértékek	18.4. A szervezet: 18.4.1. Megállapítja a hiba azonosítása és a hiba javítása között eltelt időt. 18.4.2. Referenciaértékeket határoz meg a korrekciós intézkedések megtételéhez.	-	-	-
6.	18.5. Hibajavítás – Automatizált patch-menedzsment eszközök	18.5. A szervezet a meghatározott rendszerelemeken automatizált patch-menedzsment eszközöket alkalmaz a hibajavítás megkönnyítése érdekében.	-	-	-
7.	18.6. Hibajavítás – Automatikus szoftver - és firmware frissítés	18.6. A szervezet automatikusan telepíti a meghatározott rendszerelemekre a szervezet által meghatározott biztonsági szempontból releváns szoftver- és firmware-frissítéseket.	-	-	-
8.	18.7. Hibajavítás – Korábbi szoftver- és firmware-verziók eltávolítása	18.7. A szervezet eltávolítja a szoftver- és firmware-elemek korábbi verzióit, miután azok frissített változatait telepítették.	-	-	-

9.	18.8. Kártékony kódok elleni védelem	18.8. A szervezet: 18.8.1. Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat. 18.8.2. A védelmi mechanizmusokat automatikusan frissíti minden olyan esetben, amikor új verziók jelennek meg összhangban a szervezet konfigurációkezelési szabályaival. 18.8.3. A kártékony kódok elleni védelmi mechanizmusokat úgy konfigurálja, hogy: 18.8.3.1. Meghatározott időközönként átvizsgálja a rendszert, és valós időben ellenőrzi a külső forrásokból származó fájlokat a végpontokon, a hálózati belépési vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amint a fájlokat letöltik, megnyitják vagy futtatják. 18.8.3.2. Kártékony kód észlelésekor blokkolja vagy karanténba helyezi a kártékony kódokat, vagy a szervezet által meghatározott egyéb intézkedéseket hajt végre; továbbá riasztást küld a szervezet által meghatározott személyeknek vagy szerepköröknek. 18.8.4. Ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az EIR rendelkezésre állására.	X	X	X
10.	18.9. Kártékony kódok elleni védelem – Frissítések privilegizált felhasználók által	18.9. A szervezet kizárólag privilegizált felhasználó által frissíti a kártékony kódok elleni védelmi mechanizmusokat.	-	-	-
11.	18.10. Rosszindulatú kód elleni védelem – Tesztelés és ellenőrzés	18.10. A szervezet: 18.10.1. meghatározott gyakorisággal teszteli a rosszindulatú kódok elleni védelmi mechanizmusait úgy, hogy ártalmatlan kódot juttat be a rendszerbe; és 18.10.2. ellenőrzi, hogy a kód észlelése és a kapcsolódó biztonsági események jelentése megtörténik-e.	-	-	-
12.	18.11. Kártékony kódok elleni védelem – Jogosulatlan parancsok észlelése	18.11. Az EIR: 18.11.1. felismeri a meghatározott hardverelemeken a nem engedélyezett operációsrendszer parancsokat a rendszermag (kernel) alkalmazásprogramozási interfészen (API) keresztül; és 18.11.2. figyelmeztetést ad ki, naplózza a végrehajtási kísérletet, és megakadályozza a parancs végrehajtását.	-	-	-
13.	18.12. Kártékony kódok elleni védelem – Kártékony kódok elemzése	18.12. A szervezet: 18.12.1. meghatározott eszközöket és technikákat alkalmaz a kártékony kódok jellemzőinek és viselkedésének elemzésére; és 18.12.2. a kártékony kódok elemzéséből származó eredményeket beépíti a szervezet hibajavítási eljárásaiba és a biztonsági események kezelésére vonatkozó eljárásokba.	-	-	-

14.	18.13. Az EIR monitorozása	18.13. A szervezet: 18.13.1. Monitorozza a rendszert, hogy észlelje: 18.13.1.1. A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal; 18.13.1.2. Az engedély nélküli helyi, hálózati és távoli kapcsolatokat. 18.13.2. Azonosítja a rendszer jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával. 18.13.3. Aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket: 18.13.3.1. az egész rendszerre kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetve 18.13.3.2. a rendszeren belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében. 18.13.4. Elemzi az észlelt eseményeket és rendellenességeket. 18.13.5. Módosítja a rendszerfelügyeleti tevékenység szintjét, amikor változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szint. 18.13.6. Jogi állásfoglalást kér a rendszerfelügyeleti tevékenységekről. 18.13.7. Biztosítja a szervezet által meghatározott rendszerfelügyeleti információkat a meghatározott személyeknek vagy szerepköröknek a szervezet által meghatározott gyakorisággal.	X	X	X
15.	18.14. Az EIR monitorozása – Behatolásérzékelő rendszer	18.14. A szervezet az egyedi behatolásérzékelő eszközöket egy rendszerszintű behatolásérzékelő rendszerbe konfigurálja és csatlakoztatja.	-	-	-
16.	18.15. Az EIR monitorozása – Automatizált eszközök és mechanizmusok valós idejű elemzéshez	18.15. Az EIR automatizált eszközöket és mechanizmusokat alkalmaz, amelyek támogatják az események majdnem valós idejű elemzését.	-	X	X
17.	18.16. Az EIR monitorozása – Automatizált eszközök és mechanizmusok integrációja	18.16. A szervezet automatizált eszközök és mechanizmusok segítségével integrálja a behatolásellenőrző berendezéseket a hozzáférés- és áramlásszabályozási mechanizmusokba.	-	-	-
18.	18.17. Az EIR monitorozása – Bejövő és kimenő kommunikációs forgalom	18.17. A szervezet: 18.17.1. A bejövő és kimenő kommunikációs forgalomra vonatkozóan kritériumokat állít fel a szokatlan vagy nem engedélyezett tevékenységek és körülmények azonosítására. 18.17.2. Meghatározott időközönként ellenőrzi a bejövő és kimenő kommunikációs forgalmat a szokatlan vagy jogosulatlan tevékenységek vagy körülmények tekintetében.	-	X	X
19.	18.18. Az EIR monitorozása – Rendszer által generált riasztások	18.18. Az EIR riasztást küld a meghatározott személyeknek vagy szerepköröknek, amikor a rendszer által generált meghatározott indikátorok a rendszer potenciális kompromittálódására utaló jeleket mutatnak.	-	X	X
20.	18.19. Az EIR monitorozása – Automatikus válasz gyanús eseményekre	18.19. A szervezet: 18.19.1. tájékoztatja a felmerült gyanús eseményekről a biztonsági események kijelölt kezelőit, akiket névvel vagy munkakörükkel azonosítanak; és 18.19.2. előre meghatározott és a rendszer működését csak minimálisan befolyásoló intézkedéseket hajt végre a gyanús események megszüntetése érdekében.	-	-	-
21.	18.20. Az EIR monitorozása – A felügyeleti eszközök és mechanizmusok tesztelése	18.20. A szervezet meghatározott gyakorisággal teszteli a behatolásfelügyeleti eszközöket és mechanizmusokat.	-	-	-
22.	18.21. Az EIR monitorozása – Az titkosított kommunikáció láthatósága	18.21. A szervezet intézkedéseket tesz arra, hogy a meghatározott titkosított kommunikációs forgalom átlátható legyen a meghatározott rendszerfelügyeleti eszközök és mechanizmusok számára.	-	-	X

23.	18.22. Az EIR monitorozása – Kommunikációs forgalom eltéréseinek elemzése	18.22. A szervezet elemzi a kimenő kommunikációs adatforgalmat a rendszer külső csatlakozási pontjain és a rendszer kijelölt belső pontjain, hogy felfedezze a rendellenességeket.	-	-	-
24.	18.23. Az EIR monitorozása – Automatikusan generált szervezeti riasztások	18.23. A rendszer a meghatározott automatizált mechanizmusok használatával riasztást küld a kijelölt személyeknek vagy munkaköröknek, ha olyan meghatározott, nem megfelelő vagy szokatlan tevékenységek történnek, amelyek biztonsági következményekkel járó tevékenységekre utalnak.	-	-	X
25.	18.24. Az EIR monitorozása – Forgalmi és eseményminták elemzése	18.24. A szervezet: 18.24.1. elemzi a rendszer kommunikációs forgalmát és az eseménymintákat; 18.24.2. a jellemző forgalmi és eseménymintákat megjelenítő profilokat dolgoz ki; és 18.24.3. ezeket a forgalmi és eseményprofilokat használja fel a rendszerfelügyeleti eszközök hangolásához.	-	-	-
26.	18.25. Az EIR monitorozása – Vezeték nélküli behatolást érzékelő rendszer	18.25. A szervezet egy vezeték nélküli behatolást érzékelő rendszert használ, amely képes felismerni a nem engedélyezett vezeték nélküli eszközöket, valamint észlelni a támadási kísérleteket és a rendszer potenciális kompromittálását vagy sérülését.	-	-	X
27.	18.26. Az EIR monitorozása – Vezeték nélküli és vezetékes kommunikáció	18.26. A szervezet egy behatolásérzékelő rendszert alkalmaz a vezeték nélküli kommunikációs forgalom megfigyelésére, amint az áthalad a vezeték nélküli hálózatból a vezetékes hálózatba.	-	-	-
28.	18.27. Az EIR monitorozása – Felügyeleti információk összehangolása	18.27. A szervezet összekapcsolja a rendszerben alkalmazott felügyeleti eszközökből és mechanizmusokból származó információkat.	-	-	-
29.	18.28. Az EIR monitorozása – Integrált helyzetfelismerés	18.28. A szervezet összekapcsolja a fizikai, ellátási lánc és kiberbiztonsági tevékenységek megfigyelése során gyűjtött információkat az integrált, a teljes szervezetre kiterjedő átfogóbb helyzetfelismerés érdekében.	-	-	-
30.	18.29. Az EIR monitorozása – Kimenő forgalom elemzése	18.29. A szervezet elemzi a kimenő kommunikációs forgalmat a rendszer külső interfészeinél, valamint a meghatározott belső rendszerpontokon, hogy észlelje az információ rejtett kiszivárogtatását.	-	-	-
31.	18.30. Az EIR monitorozása – Az egyének kockázatának felügyelete	18.30. A szervezet meghatározott kiegészítő felügyeletet alkalmaz azokra az egyénekre, akiket a meghatározott források alapján nagyobb kockázatot jelentő személyekként azonosítottak.	-	-	-
32.	18.31. Az EIR monitorozása – Privilegizált felhasználók	18.31. A szervezet meghatározott kiegészítő felügyeletet alkalmaz a privilegizált felhasználók esetében.	-	-	X
33.	18.32. Az EIR monitorozása – Próbaidőszakok	18.32. A szervezet meghatározott kiegészítő felügyeletet alkalmaz az egyénekkel szemben a szervezet által meghatározott próbaidőszakuk alatt.	-	-	-
34.	18.33. Az EIR monitorozása – Engedély nélküli hálózati szolgáltatások	18.33. A szervezet: 18.33.1. észleli azokat a hálózati szolgáltatásokat, amelyeket a szervezet által meghatározott engedélyezési és jóváhagyási folyamatok alapján nem engedélyeztek vagy nem hagytak jóvá; és 18.33.2. naplózza a nem engedélyezett hálózati szolgáltatások észlelését, és egyben riasztást küld a szervezet által kijelölt személyeknek vagy szerepköröknek, annak észlelésekor.	-	-	X
35.	18.34. Az EIR monitorozása – Hosztalapú eszközök	18.34. A szervezet meghatározott hosztalapú felügyeleti mechanizmusokat alkalmaz a szervezet által meghatározott rendszerelemeken.	-	-	-
36.	18.35. Az EIR monitorozása – Kompromittálódás jelei	18.35. A szervezet felismeri, összegyűjti és a kijelölt személyeknek vagy szerepköröknek továbbítja a meghatározott forrásokból származó kompromittálódásra utaló jeleket.	-	-	-

37.	18.36. Az EIR monitorozása – Hálózati forgalom elemzésének optimalizálása	18.36. Az EIR biztosítja a hálózati forgalom átláthatóságát mind a külső, mind a szervezet működése szempontjából kritikus belső rendszerinterfészeken, a felügyeleti eszközök hatékonyságának optimalizálása érdekében.	-	-	-
38.	18.37. Biztonsági riasztások és tájékoztatások	18.37. A szervezet: 18.37.1. Folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat. 18.37.2. Szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat készít. 18.37.3. Biztonsági riasztásokat, tanácsokat és iránymutatásokat ad ki a meghatározott személyeknek vagy szerepkörökben dolgozóknak, a kijelölt szervezeti egységeknek és a kijelölt külső szervezeteknek. 18.37.4. A biztonsági iránymutatásokat az azokban foglaltak szerint alkalmazza.	X	X	X
39.	18.38. Biztonsági riasztások és tájékoztatások – Automatizált figyelmeztetések és tanácsok	18.38. A szervezet biztonsági riasztásokat és tanácsokat tesz közzé az egész szervezeten belül a meghatározott, automatizált mechanizmusok segítségével.	-	-	X
40.	18.39. Biztonsági funkciók ellenőrzése	18.39. Az EIR: 18.39.1. Ellenőrzi a meghatározott biztonsági funkciók helyes működését. 18.39.2. Az előírt gyakorisággal a megfelelő jogosultsággal rendelkező felhasználók utasítására végrehajtja a meghatározott rendszerállapot-változásokat kezelő funkciók (például: indítás, újraindítás, leállítás) ellenőrzését. 18.39.3. Figyelmezteti a meghatározott személyeket vagy szerepköröket a fentiek sikertelensége esetén. 18.39.4. Amennyiben rendellenességeket észlel, leállítja vagy újraindítja a rendszert, illetve a szervezet által meghatározott alternatív intézkedéseket hajt végre	-	-	X
41.	18.40. A biztonsági funkciók ellenőrzése – Automatizálási támogatás elosztott teszteléshez	18.40. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági funkciók elosztott tesztelésének támogatására.	-	-	-
42.	18.41. Biztonsági funkciók ellenőrzése – Jelentés az ellenőrzés eredményéről	18.41. A szervezet jelentést készít a biztonsági funkciók ellenőrzésének eredményeiről a szervezet által meghatározott személyeknek vagy szerepköröknek.	-	-	-
43.	18.42. Szoftver- és információsértetlenség	18.42. A szervezet: 18.42.1. sértetlenségellenőrző eszközöket alkalmaz, hogy észlelje a jogosulatlan változtatásokat a meghatározott szoftverekben, firmware-ekben és információkban; és 18.42.2. meghatározott intézkedéseket hajt végre, amikor engedély nélküli változásokat észlel a szoftverekben, firmware-ekben vagy az információkban.	-	X	X
44.	18.43. Szoftver-, firmware- és információsértetlenség – Sértetlenség ellenőrzése	18.43. Az EIR meghatározott gyakorisággal sértetlenségellenőrzést végez a meghatározott szoftvereken, firmware-eken és információkon, a rendszer indításakor, az átmeneti rendszerállapotokban vagy a biztonsági szempontból releváns események esetén.	-	X	X
45.	18.44. Szoftver-, firmware- és információsértetlenség – Automatikus értesítések az sértetlenség megszűnéséről	18.44. A szervezet olyan automatizált eszközöket alkalmaz, amelyek értesítik a kijelölt személyeket vagy szerepköröket, amennyiben a sértetlenségellenőrzés során eltéréseket észlelnek.	-	-	X
46.	18.45. Szoftver-, firmware- és információsértetlenség – Központilag kezelt sértetlenségellenőrző eszközök	18.45. A szervezet központilag menedzselt sértetlenségellenőrző eszközöket használ.	-	-	-
47.	18.46. Szoftver- és információsértetlenség – Automatikus reagálás	18.46. Az EIR automatikusan leáll, vagy újraindul, vagy végrehajtja a szervezet által meghatározott intézkedéseket, amennyiben a sértetlenségellenőrzés során rendellenességet észlel.	-	-	X
48.	18.47. Szoftver- és információsértetlenség – Kriptográfiai védelem	18.47. Az EIR kriptográfiai mechanizmusokat alkalmaz a szoftverek, firmware-ek és az információk jogosulatlan módosításainak észlelésére.	-	-	-

49.	18.48. Szoftver- és információsértetlenség – Észlelés és a válaszadás integrálása	18.48. A szervezet a rendszer biztonsága szempontjából releváns jogosulatlan változtatások észlelését integrálja a szervezet biztonsági eseményeket kezelő rendszerébe.	-	X	X
50.	18.49. Szoftver- és információsértetlenség – Naplózás és riasztás	18.49. A sértetlenség potenciális sérülésének észlelésekor az EIR a következő lépéseket hajtja végre: esemény naplózása, riasztás küldése a felhasználóknak, meghatározott személyek vagy szerepkörök értesítése, további műveletek végrehajtása.	-	-	-
51.	18.50. Szoftver-, firmware- és információsértetlenség – Boot folyamat ellenőrzése	18.50. Az EIR ellenőrzi a meghatározott rendszerelemek rendszerindítási folyamatának (boot) sértetlenségét.	-	-	-
52.	18.51. Szoftver-, firmware- és információsértetlenség – Boot firmware védelme	18.51. A szervezet meghatározott mechanizmusokat alkalmaz a rendszerindító (boot) firmware sértetlenségének védelme érdekében a meghatározott rendszerelemekben.	-	-	-
53.	18.52. Szoftver-, firmware- és információsértetlenség – Felhasználó által telepített szoftver	18.52. A szervezet megköveteli a sértetlenségellenőrzés elvégzését a meghatározott felhasználók által telepíthető szoftvereken a végrehajtás előtt.	-	-	-
54.	18.53. Szoftver-, firmware- és információsértetlenség – Kódok hitelesítése	18.53. A szervezet kriptográfiai mechanizmusokat alkalmaz a meghatározott szoftver- vagy firmware-elemek hitelesítésére a telepítés előtt.	-	-	X
55.	18.54. Szoftver-, firmware- és információsértetlenség – Időkorlát a folyamat végrehajtására	18.54. A szervezet tiltja a meghatározott időnél hosszabb folyamatok felügyelet nélküli végrehajtását.	-	-	-
56.	18.55. Szoftver-, firmware- és információsértetlenség – Beépített védelem	18.55. A szervezet meghatározott követelményeket alkalmaz az alkalmazások beépített védelmének (RASP) biztosítására, azok futása közben.	-	-	-
57.	18.56. Kéretlen üzenetek elleni védelem	18.56. A szervezet: 18.56.1. olyan levélszemét elleni védelmet valósít meg az EIR belépési és kilépési pontjain, amelyek felismerik és kezelik az ilyen üzeneteket; és 18.56.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat a konfigurációkezelési szabályokkal összhangban.	-	X	X
58.	18.57. Kéretlen üzenetek elleni védelem – Automatikus frissítések	18.57. A szervezet meghatározott gyakorisággal automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat.	-	X	X
59.	18.58. Kéretlen üzenetek elleni védelem – Folyamatos tanulási képesség	18.58. A szervezet tanulási képességgel ellátott levélszemét elleni védelmi mechanizmusokat alkalmaz, hogy hatékonyabban tudja azonosítani a jogos kommunikációs forgalmat.	-	-	-
60.	18.59. Bemeneti információ ellenőrzés	18.59. A szervezet ellenőrzi a meghatározott beviteli információk érvényességét.	-	X	X
61.	18.60. Bemeneti információ ellenőrzés – Manuális felülírási képesség	18.60. A szervezet: 18.60.1. a meghatározott beviteli információk ellenőrzésénél biztosítja az alapkövetelmények manuális felülbírálati lehetőségét; 18.60.2. a meghatározott jogosult személyekre korlátozza a manuális felülbírálati lehetőség használatát; és 18.60.3. ellenőrzi a manuális felülbírálat lehetőségének használatát.	-	-	-
62.	18.61. Bemeneti információ ellenőrzés – Hibák felülvizsgálata és megoldása	18.61. A szervezet meghatározott időn belül felülvizsgálja és kezeli az adatbevitel érvényesítési hibáit.	-	-	-
63.	18.62. Bemeneti információ ellenőrzés – Rendszer kiszámítható működése	18.62. A szervezet ellenőrzi, hogy a rendszer előrelátható és dokumentált módon viselkedik-e, amikor érvénytelen bemenő adatot kap.	-	-	-
64.	18.63. Bemeneti információ ellenőrzés – Időzítési interakciók	18.63. Az EIR az érvénytelen bemeneti adatokra adott megfelelő válaszok meghatározásakor, figyelembe veszi a rendszerelemek közötti időzítési interakciókat.	-	-	-
65.	18.64. Bemeneti információ ellenőrzés – Bemeneteket megbízható forrásokra és jóváhagyott formátumokra korlátozása	18.64. A szervezet az információbevitelt a meghatározott, megbízható forrásokra és a meghatározott formátumokra korlátozza.	-	-	-

66.	18.65. Bemeneti információ ellenőrzés – Az adatok injektálásának megakadályozása	18.65. Az EIR megakadályozza az adatok injektálását.	-	-	-
67.	18.66. Hibakezelés	18.66. Az EIR: 18.66.1. olyan hibajelzéseket állít elő, amelyek a hibák kijavításához szükséges információkat szolgáltatnak anélkül, hogy kihasználható információkat tárnának fel; és 18.66.2. a hibaüzeneteket csak a meghatározott személyeknek vagy szerepköröknek teszi elérhetővé.	-	X	X
68.	18.67. Információ kezelése és megőrzése	18.67. A szervezet az EIR-ben lévő és az onnan kikerülő információk kezelése és megőrzése során a szervezetre vonatkozó, hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások és működési követelmények szerint jár el.	X	X	X
69.	18.68. Előreláthatható meghibásodás megelőzése	18.68. A szervezet: 18.68.1. meghatározza a meghibásodásig eltelt átlagos időt (MTTF) a meghatározott rendszerelemekre a meghatározott működési környezetekben; és 18.68.2. helyettesítő rendszerelemeket biztosít, valamint az aktív és készenléti rendszerelemek cseréjének módját a meghatározott helyettesítési kritériumoknak megfelelően végzi.	-	-	-
70.	18.69. Előreláthatható meghibásodás megelőzése - Helyettesítő rendszerelemek használata	18.69. A szervezet a rendszerelemeket úgy helyezi üzemen kívül, hogy a rendszerelemek feladatai a helyettesítő rendszerelemekre helyeződnek át, legkésőbb a meghibásodásig eltelt átlagos idő (MTTF) szervezet által meghatározott hányadának vagy százalékának leteltét követően.	-	-	-
71.	18.70. Előre látható meghibásodás megelőzése – Manuális átvitel rendszerelemek között	18.70. A szervezet manuálisan kezdeményezi az aktív és készenléti rendszerelemek közötti átállást, amikor az aktív rendszerelem használati ideje eléri a meghibásodásig eltelt átlagos idő (MTTF) szervezet által meghatározott hányadát vagy százalékát.	-	-	-
72.	18.71. Előre látható meghibásodás megelőzése – Készenléti tartalék rendszerelemek telepítése és értesítés	18.71. A szervezet a rendszerelemek hibáinak észlelésekor: 18.71.1. gondoskodik arról, hogy a készenléti rendszerelemek sikeresen és átlátható módon telepítésre kerüljenek a szervezet által meghatározott időablakon belül, és 18.71.2. aktiválja a meghatározott riasztást, valamint automatikusan leállítja az EIR-t és egyéb meghatározott műveleteket hajt végre.	-	-	-
73.	18.72. Előre látható meghibásodás megelőzése – biztonsági mentőkapacitás	18.72. A szervezet valós idejű vagy közel valós idejű átállási képességet biztosít az EIR számára, a szervezet által meghatározott módon.	-	-	-
74.	18.73. Nem állandó rendszerelemek és szolgáltatások	18.73. A szervezet olyan nem állandó rendszerelemeket és szolgáltatásokat alkalmaz, amelyeket ismert állapotban indít el, és a munkaszakasz végén vagy meghatározott gyakorisággal leállít.	-	-	-
75.	18.74. Nem állandó rendszerelemek és szolgáltatások – Megbízható forrásokból történő frissítés	18.74. A szervezet a rendszerelemek és szolgáltatások frissítése során felhasznált szoftvereket és adatokat a szervezet által meghatározott megbízható forrásokból szerzi be.	-	-	-
76.	18.75. Nem állandó információk kezelése	18.75. A szervezet: 18.75.1. meghatározott gyakorisággal frissíti a meghatározott információkat, igény szerint létrehozza a meghatározott információkat; és 18.75.2. törli az információkat, amennyiben már nincs rájuk szükség.	-	-	-
77.	18.76. Nem állandó kapcsolatok létrehozása	18.76. A szervezet igény szerint rendszerkapcsolatokat hoz létre és megszakítja a kapcsolatokat, ha egy kérést teljesíteni kell, vagy ha adott ideig nem használták a kapcsolatokat.	-	-	-

78.	18.77. A kimeneti információ kezelése és megőrzése	18.77. A szervezet bizonyos szoftverek és alkalmazások esetén ellenőrzi a kimeneti információkat annak biztosítása érdekében, hogy azok összhangban legyenek az elvárt tartalommal.	-	-	-
79.	18.78. Memóriavédelem	18.78. A szervezet meghatározott védelmi intézkedéseket alkalmaz annak érdekében, hogy megvédje a rendszermemóriát a jogosulatlan kódok végrehajtásától.	-	X	X
80.	18.79. Hiba esetén alkalmazandó biztonsági eljárások	18.79. A szervezet meghatározott meghibásodások bekövetkezésekor a szervezet által meghatározott hibaelhárító eljárásokat hajt végre.	-	-	-
81.	18.80. Adatszivárgás észlelésének támogatása	18.80. A szervezet adatokat vagy funkciókat ágyaz be a meghatározott EIR-ekbe vagy rendszerelemekbe, annak megállapítására, hogy a szervezeti adatokat kiszivárogtatták-e vagy jogosulatlanul eltávolították-e azokat a szervezetből.	-	-	-
82.	18.81. Információfrissítés	18.81. A szervezet adott gyakorisággal frissíti a meghatározott információkat vagy előállítja a szükséges információkat és eltávolítja azokat, amennyiben már nincs rájuk szükség.	-	-	-
83.	18.82. Információ diverzitás	18.82. A szervezet: 18.82.1. meghatározza és azonosítja az alternatív információforrásokat a szervezet működése szempontjából kritikus funkciók és szolgáltatások számára; és 18.82.2. egy alternatív információforrást használ a szervezet működése szempontjából kritikus funkciók vagy szolgáltatások végrehajtásához a meghatározott EIR-ek vagy rendszerelemek esetén, amikor az elsődleges információforrás sérült vagy nem elérhető.	-	-	-
84.	18.83. Fragmentált információ	18.83. A szervezet meghatározott körülmények esetén: 18.83.1. a meghatározott információt fragmentálja; és 18.83.2. a fragmentált információt szétosztja a meghatározott EIR-ek és rendszerelemek között.	-	-	-

19. Ellátási lánc kockázatkezelése

	A	B	C	D	E
1.	Követelménycsoport megnevezése	Követelmény szövege	Biztonsági osztály		
			Alap	Jelentős	Magas
2.	19.1. Szabályzat és eljárásrendek	19.1. A szervezet: 19.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 19.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó ellátási láncra vonatkozó kockázatmenedzsment szabályzatot, amely 19.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 19.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 19.1.1.2. az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrendet, amely az ellátási láncra vonatkozó kockázatkezeléséhez kapcsolódó szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 19.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 19.1.3. Felülvizsgálja és frissíti az aktuális ellátási láncra vonatkozó kockázatmenedzsment szabályzatot és az ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	X	X	X
3.	19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	19.2. A szervezet: 19.2.1. A meghatározott EIR-ek, rendszerelemek vagy rendszerszolgáltatások tekintetében szabályzatot dolgoz ki a kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, kivezetés valamint a selejtezés során felmerülő ellátási lánccal kapcsolatos kockázatok kezelésére. 19.2.2. Meghatározott gyakorisággal felülvizsgálja és frissíti az ellátási lánc kockázatmenedzsment szabályzatát, illetve szükség szerint annak érdekében, hogy kezelje a fenyegetéseket, valamint a szervezeti és környezeti változásokat. 19.2.3. Védi az ellátási lánc kockázatmenedzsment szabályzatát a jogosulatlan közzétételtől és módosítástól.	X	X	X
4.	19.3. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat – Ellátási lánc kockázatkezeléséért felelős csoport létrehozása	19.3. A szervezet létrehoz egy, az ellátási lánc kockázatait kezelő csapatot, amely a meghatározott személyekből, szerepkörökből és felelősségi körökből áll.	-	-	-

5.	19.4. Ellátási láncra vonatkozó követelmények és folyamatok	19.4. A szervezet: 19.4.1. Folyamatot vagy folyamatokat alakít ki annak érdekében, hogy azonosítsa és kezelje a gyengeségeket vagy hiányosságokat a meghatározott EIR ellátási láncának elemeiben és folyamataiban, a szervezet által meghatározott ellátási láncért felelős személyekkel együttműködve. 19.4.2. Alkalmazza a szervezet által meghatározott ellátási lánccal kapcsolatos kontrollokat annak érdekében, hogy védje az EIR-t, rendszerelemet vagy rendszer szolgáltatást az ellátási lánccal kapcsolatos kockázatokkal szemben és csökkentse az ellátási lánccal kapcsolatos eseményekből eredő károkat és következményeket. 19.4.3. Dokumentálja a meghatározott és bevezetett ellátási láncot érintő folyamatokat és kontrollokat a biztonsági szabályzatokban, az ellátási lánc kockázatmenedzsment szabályzatában és egyéb, a szervezet által meghatározott dokumentumban.	X	X	X
6.	19.5. Ellátási lánc ellenőrzések és folyamatok – Diverzifikált beszállítói bázis	19.5. A szervezet többféle beszállítót vesz igénybe a meghatározott rendszerelemek és szolgáltatások vonatkozásában.	-	-	-
7.	19.6. Ellátási lánc ellenőrzések és folyamatok – Károk csökkentése	19.6. A szervezet meghatározott ellenintézkedéseket alkalmaz a szervezeti ellátási láncot azonosító és célba vevő potenciális ellenérdekű felek által okozott kár csökkentése érdekében.	-	-	-
8.	19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók	19.7. A szervezet gondoskodik arról, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.	X	X	X
9.	19.8. Rendszerelemek és kapcsolódó adatok eredetisége	19.8. A szervezet dokumentálja, monitorozza és megőrzi a meghatározott EIR-ekhez, rendszerelemekhez kapcsolódó, azok eredetiségét igazoló adatokat.	-	-	-
10.	19.9. Rendszerelemek és kapcsolódó adatok eredetisége - Azonosítás	19.9. A szervezet az EIR, valamint a szervezet működése szempontjából kritikus rendszerelemek ellátási láncának meghatározott elemeire folyamataira és a hozzájuk köthető személyzetre azonosítási folyamatot alakít ki és tart fenn.	-	-	-
11.	19.10. Rendszerelemek és kapcsolódó adatok eredetisége – Ellátási láncon keresztül történő nyomon követés	19.10. A szervezet az EIR-eket, valamint a szervezet működése szempontjából kritikus rendszerelemeket egyedileg azonosítja az ellátási láncon keresztül történő nyomon követés céljából.	-	-	-
12.	19.11. Eredet – Valódiság és módosítatlanság hitelesítése	19.11. A szervezet meghatározott védelmi intézkedéseket alkalmaz annak ellenőrzésére, hogy az EIR vagy rendszerelem eredeti és nem módosított.	-	-	-
13.	19.12. Eredet – Ellátási lánc sértetlensége – Jóhírnév	19.12. A szervezet meghatározott védelmi intézkedéseket alkalmaz, és meghatározott elemzéseket végez az EIR és rendszerelemek sértetlenségének biztosítása érdekében, a szervezet működése szempontjából kritikus technológiák, termékek és szolgáltatások belső összetételének és eredetének ellenőrzésével.	-	-	-
14.	19.13. Beszerzési stratégiák, eszközök és módszerek	19.13. A szervezet meghatározott beszerzési stratégiákat, szerződéses eszközöket és beszerzési módszereket alkalmaz annak érdekében, hogy kivédje, azonosítsa és csökkentse az ellátási láncból eredő kockázatokat.	X	X	X
15.	19.14. Beszerzési stratégiák, eszközök és módszerek – Megfelelő utánpótlás	19.14. A szervezet meghatározott követelményeket alkalmaz annak érdekében, hogy a meghatározott és a szervezet működése szempontjából kritikus rendszerelemek ellátása és utánpótlása megfelelő legyen.	-	-	-
16.	19.15. Beszerzési stratégiák, eszközök és módszerek – Kiválasztás, elfogadás, módosítás vagy frissítés előtti értékelések	19.15. A szervezet értékeli az EIR-t, rendszerelemet vagy rendszerszolgáltatást a kiválasztást, az elfogadást, a módosítást vagy a frissítést megelőzően.	-	-	-
17.	19.16. Beszállítók értékelése és felülvizsgálata	19.16. A szervezet meghatározott gyakorisággal értékeli és felülvizsgálja a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat.	-	X	X

18.	19.17. Beszállító értékelések és felülvizsgálatok – Tesztelés és elemzés	19.17. A szervezet az EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz kapcsolódó, szervezet által meghatározott ellátási lánc-elemekkel, folyamatokkal és szereplőkkel kapcsolatosan szervezeti és független harmadik fél által végzett elemzéseket és teszteket alkalmaz.	-	-	-
19.	19.18. Ellátási lánc működésbiztonsága (OPSEC)	19.18. A szervezet meghatározott működésbiztonsági (OPSEC) kontrollokat alkalmaz annak érdekében, hogy védje az EIR-hez, rendszerelemhez vagy rendszerszolgáltatáshoz köthető, ellátási lánchoz kapcsolódó információkat.	-	-	-
20.	19.19. Értesítési megállapodások	19.19. A szervezet megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel.	X	X	X
21.	19.20. Hamisítás elleni védelem	19.20. A szervezet hamisítás elleni védelmi programot vezet be a rendszer, rendszerelem vagy rendszerszolgáltatás védelmére.	-	-	X
22.	19.21. Hamisítás elleni védelem - Rendszerfejlesztési életciklus	19.21. A szervezet hamisítás elleni technológiákat, eszközöket és technikákat alkalmaz a teljes rendszerfejlesztési életciklus során.	-	-	X
23.	19.22. Rendszerek vagy rendszerelemek vizsgálata	19.22. A szervezet eseti jelleggel vagy meghatározott gyakorisággal és meghatározott esetekben ellenőrzi A EIR-eket vagy rendszerelemeket az esetleges hamisítás felderítése érdekében.	X	X	X
24.	19.23. Rendszerelem hitelessége	19.23. A szervezet: 19.23.1. kialakítja és bevezeti a hamisítás elleni szabályokat és eljárásokat, amelyek magukban foglalják a hamisított rendszerelemek észlelését és annak megelőzését, hogy ezek bejussanak az EIR-be; valamint 19.23.2. jelenti a hamisított rendszerelemeket és azok forrását a szervezet által meghatározott külső szervezeteknek, illetve a szervezet által meghatározott személyeknek vagy szerepköröknek.	X	X	X
25.	19.24. Rendszerelem hitelessége – Hamisítás elleni képzés	19.24. A szervezet a meghatározott személyeknek vagy szerepköröknek képzést biztosít a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.	X	X	X
26.	19.25. Rendszerelem hitelessége – Konfigurációfelügyelet	19.25. A szervezet fenntartja a konfiguráció felügyeletét a meghatározott szervizelésre vagy javításra váró vagy olyan rendszerelemek esetén, amelyeket szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.	X	X	X
27.	19.26. Rendszerelem hitelessége – Hamisítás elleni intézkedések	19.26. A szervezet meghatározott gyakorisággal ellenőrzi rendszerét a hamisított rendszerelemek után kutatva.	-	-	-
28.	19.27. Rendszerelem selejtezése, megsemmisítése	19.27. A szervezet meghatározott technikákkal és módszerekkel selejtezi a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.	X	X	X

20. Alkalmazási útmutató

20.1. Az 1-19. pontban foglalt táblázat „A” oszlopa a követelménycsoportok megnevezését és számkódját tartalmazza.

20.2. Az 1-19. pontban foglalt táblázat „B” oszlopa az adott követelménycsoporthoz tartozó védelmi intézkedések leírását és számkódját tartalmazza.

20.3. Az 1-19. pontban foglalt táblázat „A” és „B” oszlopokban alkalmazott számkódok 1. szintje a követelménycsaládot, 2. szintje a követelménycsoportot, míg a 3-5. szintek a védelmi intézkedés leírásának különböző mélységű részleteit jelzik.

20.4. Az 1-19. pontban foglalt táblázat „C”, „D” és „E” oszlopok jelölik az adott követelmény használhatóságát, az ”Alap”, „Jelentős” és „Magas” biztonsági osztályok esetében. „X” jelöli, ha a védelmi intézkedés használata az adott biztonsági osztálynál elvárt, és „-” jelöli, ha a védelmi intézkedés használata az adott biztonsági osztálynál nem elvárás. Azon védelmi intézkedések, amelyek esetében a „C” „D” és „E” oszlopok egyaránt „-” jelölést tartalmaznak, kiegészítő védelmi intézkedések. Ezen kiegészítő védelmi intézkedéseket egyik biztonsági osztály esetében sem kötelező alkalmazni, a szervezetek azonban felhasználhatják ezeket a rájuk vonatkozó egyéb – különösen rendszerspecifikus sajátosságokból eredő – követelmények teljesítése érdekében.

20.5. Az 1-19. pontban foglalt táblázat „B” oszlopban elvárt, meghatározandó tevékenységeket, paramétereket az adott követelménycsaládhoz és követelménycsoporthoz tartozó stratégiában, szabályzatban, eljárásrendben, eljárásban vagy munkautasításban szükséges meghatározni. Ez a tevékenység a szervezet, személy vagy szerepkör feladata.

20.6. Az 1-19. pontban foglalt táblázat „B” oszlopban található követelmények szövege a követelménycsoport megnevezésével együtt értelmezendő.

3. melléklet a 7/2024. (VI. 24.) MK rendelethez

1. Fenyegetések katalógusa

	A	B
1.	Fenyegetés	Érintett információbiztonsági alapelvek
2.	Tűz	R
3.	Kedvezőtlen környezeti feltételek	S, R
4.	Víz	S, R
5.	Szennyeződés, por, korrózió	S, R
6.	Természeti katasztrófák	R
7.	Katasztrófák a környezetben	R
8.	Jelentős környezeti események	B, S, R
9.	Áramellátás megszakadása, vagy hibája	S, R
10.	Kommunikációs hálózatok megszakadása, vagy zavara	S, R
11.	Beszállítói láncok megszakadása, vagy zavara	R
12.	Külső szolgáltatók hibája, vagy működési zavara	B, S, R
13.	Elektromágneses interferencia	S, R
14.	Kompromittáló elektromágneses kisugárzás	B
15.	Kémkedés	B
16.	Lehallgatás	B
17.	Eszközök, adathordozók, dokumentumok eltulajdonítása	B, R
18.	Eszközök, adathordozók, dokumentumok elvesztése	B, R
19.	Rossz tervezés vagy az alkalmazkodás hiánya	B, S, R
20.	Védett információ nyilvánosságra kerülése	B
21.	Nem megbízható forrásból származó információk	B, S, R
22.	Hardver vagy szoftver hamisítása (manipulációja)	B, S, R
23.	Információmanipuláció	S
24.	Elektronikus információs rendszerbe történő illetéktelen belépés	B, S
25.	Eszközök vagy adathordozók megsemmisülése	R
26.	Eszközök vagy az elektronikus információs rendszer működésének megszakadása	R
27.	Eszközök vagy az elektronikus információs rendszer hibás működése	B, S, R
28.	Erőforrások hiánya	R
29.	Szoftverek sérülékenységei vagy hibái	B, S, R
30.	Jogszabályok vagy szerződések megszegése	B, S, R
31.	Eszközök vagy az elektronikus információs rendszer engedély nélküli kezelése vagy használata	B, S, R
32.	Eszközök vagy az elektronikus információs rendszer hibás kezelése vagy használata	B, S, R
33.	Engedélyekkel való visszaélés	B, S, R
34.	Személyi állomány elvesztése	R
35.	Támadás	B, S, R
36.	Kényszerítés, zsarolás vagy korrupció	B, S, R
37.	Eltulajdonított személyazonossággal történő visszaélés	B, S, R
38.	Cselekmények letagadása	B, S
39.	Személyes adatokkal történő visszaélés	B
40.	Rosszindulatú szoftverek (malware)	B, S, R

41.	Szolgáltatásmegtagadással járó támadás (DOS)	R
42.	Szabotázs	R
43.	Pszichológiai manipuláció (social engineering)	B, S
44.	Manipulált hálózati adatforgalom	B, S
45.	Helyiségekbe történő engedély nélküli behatolás	B, S, R
46.	Adatvesztés	R
47.	Védendő információk sértetlenségének elvesztése	S
48.	Kártékony mellékhatások	B, S, R

2. Alkalmazási útmutató

2.1. Az 1. pontban foglalt táblázat „A" oszlopa a fenyegetések megnevezését tartalmazza.

2.2. Az 1. pontban foglalt táblázat „B" oszlopa az adott fenyegetések által potenciálisan érintett információbiztonsági alapelvek betűjeleit tartalmazza, az alábbiak szerint:

2.2.1. Bizalmasság: B

2.2.2. Sértetlenség: S

2.2.3. Rendelkezésre állás: R

A nemzetgazdasági miniszter 20/2024. (VI. 24.) NGM rendelete a fejezeti és központi kezelésű előirányzatok kezeléséről és felhasználásáról

Az államháztartásról szóló 2011. évi CXCV. törvény 109. § (5) bekezdésében kapott felhatalmazás alapján, az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet 1. melléklet I. pont 22. alpontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 148. § (1) bekezdés 2. pontjában meghatározott feladatkörében eljáró pénzügyminiszterrel egyetértésben – a következőket rendelem el:

I. FEJEZET
ÁLTALÁNOS RENDELKEZÉSEK

1. A rendelet hatálya

1. § E rendelet hatálya

a) a központi költségvetésről szóló törvény 1. melléklet XXIII. Nemzetgazdasági Minisztérium fejezetében előirányzatként megállapított fejezeti kezelésű előirányzatokra és központi kezelésű előirányzatokra, amelyek vonatkozásában az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet (a továbbiakban: Ávr.) 1. melléklete szerint a fejezetet irányító szerv és annak vezetője a Nemzetgazdasági Minisztérium és a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 103. § (1) bekezdése szerinti tagja (a továbbiakban: miniszter),

b) a költségvetési évet megelőző évek központi költségvetéséről szóló törvényeiben az a) pont szerinti fejezetet irányító szerv vezetője által vezetett minisztérium és annak jogelődjei költségvetési fejezetében megállapított fejezeti kezelésű előirányzatok költségvetési maradványára, tekintet nélkül annak eredeti előirányzathoz való kapcsolódására vagy annak hiányára, és

c) a tárgyév során megállapított új fejezeti kezelésű előirányzatok és központi kezelésű előirányzatok kiadási előirányzataira

[az a)–c) pont szerinti előirányzatok a továbbiakban együtt: előirányzatok] terjed ki.

2. Értelmező rendelkezések

2. § E rendelet alkalmazásában

1. *acélipar:* a 651/2014/EU bizottsági rendelet 2. cikk 43. pontja szerinti tevékenység,
2. *alapkutatás:* a 651/2014/EU bizottsági rendelet 2. cikk 84. pontja szerinti kísérleti vagy elméleti munka,
3. *azonos vagy hasonló tevékenység:* a 651/2014/EU bizottsági rendelet 2. cikk 50. pontja szerinti tevékenység,
4. *állami támogatás:* az európai uniós versenyjogi értelemben vett állami támogatásokkal kapcsolatos eljárásról és a regionális támogatási térképről szóló 37/2011. (III. 22.) Korm. rendelet (a továbbiakban: Atr.) 2. § 1. pontja szerinti támogatás,
5. *átlagos éves utasforgalom:* a 651/2014/EU bizottsági rendelet 2. cikk 148. pontja szerinti utasforgalom,
6. *átlátható formában nyújtott támogatás:* olyan támogatás, amelynél előzetesen, kockázatértékelés nélkül kiszámítható a bruttó támogatástartalom,
7. *átmeneti támogatás:* az Európai Unió működéséről szóló szerződés (a továbbiakban: EUMSz) 107. cikk (1) bekezdése szerinti állami támogatásnak minősülő és az „Állami támogatási intézkedésekre vonatkozó ideiglenes keret a gazdaságnak a jelenlegi COVID-19-járvánnyal összefüggésben való támogatása céljából" című, 2020. március 19-i, 2020/C 91 I/01 számú európai bizottsági közlemény (a továbbiakban: közlemény) 3.1. pontja szerint nyújtott támogatás,
8. *áttelepítés:* ha
   a) a kérelmet benyújtó beruházó vagy a kérelmet benyújtó beruházóval egy vállalatcsoportba tartozó beruházó azonos vagy hasonló tevékenységet vagy annak egy részét az EGT megállapodás egyik szerződő felének területén található létesítményből az EGT megállapodás egy másik szerződő felének területén található azon létesítménybe helyezi át, ahol a támogatott beruházásra sor kerül,
   b) az eredeti, valamint a támogatott létesítményben előállított termék vagy nyújtott szolgáltatás legalább részben ugyanazokat a célokat szolgálja, és ugyanazon fogyasztói típus keresletét vagy igényeit elégíti ki, és
   c) a kérelmet benyújtó beruházó vagy a kérelmet benyújtó beruházóval egy vállalatcsoportba tartozó vállalkozás valamely, az EGT-n belüli eredeti létesítményében folytatott azonos vagy hasonló tevékenység körében munkahelyek szűnnek meg,
9. *belvízi hajó:* a 651/2014/EU bizottsági rendelet 2. cikk 164. pontja szerinti jármű,
10. *belvízi kikötő:* a 651/2014/EU bizottsági rendelet 2. cikk 156. pontja szerinti kikötő,
11. *bérköltség:* a 651/2014/EU bizottsági rendelet 2. cikk 31. pontja szerinti költség,
12. *biogáz:* a 651/2014/EU bizottsági rendelet 2. cikk 117b. pontja szerinti biogáz,
13. *biomassza:* a 651/2014/EU bizottsági rendelet 2. cikk 117. pontja szerinti anyag,
14. *biomasszából előállított üzemanyagok:* a 651/2014/EU bizottsági rendelet 2. cikk 117d. pontja szerint előállított üzemanyagok,
15. *bioüzemanyagok:* a 651/2014/EU bizottsági rendelet 2. cikk 117a. pontja szerinti üzemanyagok,
16. *bruttó támogatási egyenérték:* a 651/2014/EU bizottsági rendelet 2. cikk 22. pontja szerinti összeg,
17. *csekély összegű támogatás:*
   a) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a csekély összegű támogatásokra való alkalmazásáról szóló, 2023. december 13-i (EU) 2023/2831 bizottsági rendelet szerinti támogatás,
   b) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a mezőgazdasági ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról szóló, 2013. december 18-i 1408/2013/EU bizottsági rendelet szerinti támogatás,
   c) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a halászati és akvakultúra-ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról szóló, 2014. június 27-i 717/2014/EU bizottsági rendelet (a továbbiakban: 717/2014/EU bizottsági rendelet) hatálya alá tartozó támogatás, valamint
   d) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a mezőgazdasági ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról szóló, 2013. december 18-i 1408/2013/EU bizottsági rendelet szerinti támogatás,
18. *csoportmentességi rendeletek:* a 651/2014/EU bizottsági rendelet, az (EU) 2022/2472 bizottsági rendelet, az (EU) 2022/2473 bizottsági rendelet és az 1407/2013/EU bizottsági rendelet,

19. *dedikált infrastruktúra:* az előzetesen azonosítható vállalkozás számára épített és az ő igényeihez szabott infrastruktúra,
20. *digitalizáció:* a 651/2014/EU bizottsági rendelet 2. cikk 103c. pontja szerinti fejlesztés,
21. *diszkont kamatláb:* az Atr. 2. § 3. pontja szerinti kamatláb,
22. *egy és ugyanazon vállalkozás:* az (EU) 2023/2831 bizottsági rendelet 2. cikk (2) bekezdése, az 1408/2013/EU bizottsági rendelet 2. cikk 2. pontja, valamint a 717/2014/EU bizottsági rendelet 2. cikk 2. pontja szerinti feltételeknek megfelelő vállalkozás,
23. *eljárási innováció:* a 651/2014/EU bizottsági rendelet 2. cikk 97. pontja szerinti módszer alkalmazása,
24. *elsődleges mezőgazdasági termelés:* az EUMSz I. mellékletében felsorolt növények vagy állati eredetű termék előállítása, ide nem értve bármely, azok lényegi tulajdonságát megváltoztató tevékenységet,
25. *elszámolható költség:* az Atr. 2. § 6. pontja szerinti költség,
26. *energetikai célú infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 130. pontja szerinti fizikai berendezés vagy létesítmény,
27. *energiahatékonyság:* a 651/2014/EU bizottsági rendelet 2. cikk 103. pontja szerint megtakarított energiamennyiség,
28. *energiahatékony távfűtés és távhűtés:* a 651/2014/EU bizottsági rendelet 2. cikk 124. pontja szerinti távfűtés és távhűtés,
29. *energiatárolás:* a villamos energia végső felhasználásának elhalasztása a termelésnél későbbi időpontra, vagy a villamos energia átalakítása tárolható formájú energiává, az ilyen energia tárolása, valamint az ilyen energia ezt követő villamos energiává való visszaalakítása,
30. *észszerű nyereség:* a 651/2014/EU bizottsági rendelet 2. cikk 142. pontja szerinti nyereség,
31. *élelmiszer-feldolgozás:* a mezőgazdasági termék feldolgozás és forgalmazás tevékenység, illetve a 10 „Élelmiszergyártás" és 11 „Italgyártás" Tevékenységek egységes ágazati osztályozási rendszere (TEÁOR'08) kód alá tartozó tevékenység,
32. *finanszírozási hiány:* a 651/2014/EU bizottsági rendelet 2. cikk 118. pontja szerinti hiány,
33. *folyékony bio-energiahordozó:* a 651/2014/EU bizottsági rendelet 2. cikk 117c. pontja szerinti bio-energiahordozó,
34. *foglalkoztatottak számának nettó növekedése:* a 651/2014/EU bizottsági rendelet 2. cikk 32. pontja szerinti növekedés,
35. *független harmadik fél:* olyan vállalkozás, amely nem minősül egy másik meghatározott vállalkozás vonatkozásában a 651/2014/EU bizottsági rendelet I. melléklet 3. cikk (2) bekezdése szerinti partnervállalkozásnak vagy (3) bekezdése szerinti kapcsolt vállalkozásnak,
36. *halászati és akvakultúra-termékek:* az 1379/2013/EU európai parlamenti és tanácsi rendelet I. melléklete szerinti termékek,
37. *hatékony együttműködés:* a 651/2014/EU bizottsági rendelet 2. cikk 90. pontja szerinti együttműködés,
38. *hátrányos helyzetű munkavállaló:* a 651/2014/EU bizottsági rendelet 2. cikk 4. pontja szerinti munkavállaló,
39. *helyi infrastruktúra:* olyan infrastruktúra, amely helyi szinten járul hozzá az üzleti és fogyasztói környezet korszerűsítéséhez és ipari bázisok fejlesztéséhez,
40. *hitelszerződés:* a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 6:382. §-a szerinti szerződés,
41. *hozzáférési infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 159. pontja szerinti infrastruktúra,
42. *hidrogéntöltő infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 102b. pontja szerinti infrastruktúra,
43. *hivatásos csapat:* az a sportvállalkozás, amely hivatásos sportolót alkalmaz,
44. *hivatásos sport:* a 651/2014/EU bizottsági rendelet 2. cikk 143. pontja szerinti sporttevékenység,
45. *hivatásos sportoló:* az a sportoló, aki jövedelemszerzési céllal, foglalkozásszerűen vagy más módon, ellenszolgáltatás fejében folytat sporttevékenységet. A sporttevékenységért nyújtott ellenszolgáltatásnak meg kell haladnia a részvételi költségeket, és a sportoló jövedelmének jelentős részét kell kitennie, függetlenül attól, hogy a sportoló és az érintett sportvállalkozás kötött-e munka- vagy más, munkavégzésre irányuló szerződést. Nem minősül ellenszolgáltatásnak a sportrendezvényen való részvételhez kapcsolódó utazási és szállásköltségek megtérítése,
46. *hőszivattyú:* a 651/2014/EU bizottsági rendelet 2. cikk 108b. pontja szerinti gép, készülék vagy berendezés,
47. *immateriális javak:* a 651/2014/EU bizottsági rendelet 2. cikk 30. pontja szerinti javak,
48. *induló beruházás:* a 651/2014/EU bizottsági rendelet 2. cikk 49. pontja szerinti beruházás,

49. *innovációs tanácsadás:* a 651/2014/EU bizottsági rendelet 2. cikk 94. pontjában meghatározott feltételeknek megfelelő tanácsadás, segítségnyújtás és képzés,
50. *innovációs támogató szolgáltatás:* a 651/2014/EU bizottsági rendelet 2. cikk 95. pontja szerinti szolgáltatás,
51. *ipari kutatás:* a 651/2014/EU bizottsági rendelet 2. cikk 85. pontja szerinti tervezett kutatás vagy kritikus vizsgálat,
52. *kapcsolt energiatermelés vagy kapcsolt hő- és villamosenergia-termelés:* a 651/2014/EU bizottsági rendelet 2. cikk 108. pontja szerinti energiatermelés,
53. *kapcsolt vállalkozás:* a 651/2014/EU bizottsági rendelet I. melléklet 3. cikk (3) bekezdése szerinti vállalkozás továbbá az Európai Unió működéséről szóló szerződés 107. és 108. cikkének alkalmazásában a mezőgazdasági és az erdészeti ágazatban, valamint a vidéki térségekben nyújtott támogatások bizonyos kategóriáinak a belső piaccal összeegyeztethetőnek nyilvánításáról szóló, 2014. június 25-i 702/2014/EU bizottsági rendelet (a továbbiakban: 702/2014/EU bizottsági rendelet) I. melléklet 3. cikk (3) bekezdése szerinti vállalkozás,
54. *kérelmet benyújtó beruházóval egy vállalatcsoportba tartozó beruházó:* az a beruházó, amely a kérelmet benyújtó beruházóval a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Sztv.) szerinti anya- vagy leányvállalati kapcsolatban áll,
55. *kikötői felépítmény:* a 651/2014/EU bizottsági rendelet 2. cikk 158. pontja szerinti felépítmény,
56. *kikötői infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 157. pontja szerinti infrastruktúra,
57. *kísérleti fejlesztés:* a 651/2014/EU bizottsági rendelet 2. cikk 86. pontja szerinti fejlesztés,
58. *kis- és középvállalkozás:* a 651/2014/EU bizottsági rendelet I. melléklete szerinti vállalkozás,
59. *kockázatfinanszírozási célú intézkedés:* a végső kedvezményezett kis- és középvállalkozásnak nyújtott sajáttőke- és kvázi sajáttőke-befektetés, hitel, kezességvállalás, valamint ezek kombinációja,
60. *kotrás:* a 651/2014/EU bizottsági rendelet 2. cikk 160. pontja szerinti tevékenység,
61. *közvetlenül a beruházási projekt által létrehozott munkahely:* a 651/2014/EU bizottsági rendelet 2. cikk 62. pontja szerinti munkahely,
62. *kutatási infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 91. pontja szerinti infrastruktúra,
63. *kutató-tudásközvetítő szervezet:* a 651/2014/EU bizottsági rendelet 2. cikk 83. pontja szerinti szervezet,
64. *kvázi sajáttőke-befektetés:* a 651/2014/EU bizottsági rendelet 2. cikk 66. pontja szerinti finanszírozási forma,
65. *légitársaság:* az (EU) 2017/1084 bizottsági rendelettel módosított 651/2014/EU bizottsági rendelet 2. cikk 145. pontja szerinti légitársaság,
66. *létesítmény:* funkcionálisan megbonthatatlan egészet képező termelő vagy szolgáltató egység,
67. *létesítmény felvásárlása:* egy létesítményhez közvetlenül kapcsolódó tárgyi eszközök és immateriális javak piaci feltételek mellett történő megvásárlása, ha a létesítmény bezárásra került, vagy – ha nem vásárolják meg – bezárásra került volna, és – kivéve, ha egy kisvállalkozást az eladónak a Ptk. szerinti közeli hozzátartozója vagy korábbi munkavállalója vásárol meg – a felvásárló beruházó a létesítmény tulajdonosától független harmadik fél,
68. *lignit:* a 651/2014/EU bizottsági rendelet 2. cikk 43a. pontja szerinti anyag,
69. *magasan képzett munkaerő:* a 651/2014/EU bizottsági rendelet 2. cikk 93. pontja szerinti munkaerő,
70. *megújuló energia vagy megújuló energiaforrásból előállított energia:* a 651/2014/EU bizottsági rendelet 2. cikk 109. pontja szerinti energia,
71. *megújuló hidrogén:* a 651/2014/EU bizottsági rendelet 2. cikk 102c. pontja szerint előállított hidrogén,
72. *megújuló energiaforrásokon alapuló kapcsolt energiatermelés:* a 651/2014/EU bizottsági rendelet 2. cikk 108a. pontja szerinti energiatermelés,
73. *megújuló villamos energia:* a 651/2014/EU bizottsági rendelet 2. cikk 102d. pontja szerinti villamos energia,
74. *megvalósíthatósági tanulmány:* a 651/2014/EU bizottsági rendelet 2. cikk 87. pontja szerinti tanulmány,
75. *megváltozott munkaképességű munkavállaló:* a 651/2014/EU bizottsági rendelet 2. cikk 3. pontja szerinti munkavállaló,
76. *mezőgazdasági ágazat:* a mezőgazdasági termékek elsődleges termelésével, feldolgozásával és forgalmazásával foglalkozó vállalkozások összessége,
77. *mezőgazdasági termék:* a 651/2014/EU bizottsági rendelet 2. cikk 11. pontja szerinti termék,
78. *mezőgazdasági termék feldolgozása:* a 651/2014/EU bizottsági rendelet 2. cikk 10. pontja szerinti tevékenység,
79. *mezőgazdasági termék forgalmazása:* a 651/2014/EU bizottsági rendelet 2. cikk 8. pontja szerinti tevékenység,
80. *mezőgazdasági üzem:* az (EU) 2022/2472 bizottsági rendelet 2. cikk 6. pontja szerinti üzem,

81. *multifunkcionális szabadidős létesítmény:* a 651/2014/EU bizottsági rendelet 55. cikk (3) bekezdése szerinti létesítmény,
82. *működési eredmény:* a beruházásnak az Sztv. 3. § (4) bekezdés 5. pontja szerinti hasznos élettartama alatt elért – a projektkockázat és a tőkeköltség alapján a támogatást nyújtó által jóváhagyott diszkonttényezővel diszkontált – bevételei, csökkentve az ugyanezen diszkonttényezővel diszkontált működési költségekkel, így különösen a személyi jellegű ráfordítással, anyagköltséggel, a szerződéses szolgáltatással, a távközléssel, az energiával és a karbantartással, a bérleti díjjal, az adminisztrációval összefüggő költséggel, kivéve az olyan értékcsökkenési és a finanszírozási költséget, amelyet beruházási támogatásból már fedeztek, azzal, hogy amennyiben a számítás eredménye negatív, a működési eredmény értéke nulla,
83. *nagyberuházás:* az az induló beruházás, amelyhez kapcsolódóan az elszámolható költségek összege az összeszámítási szabályt figyelembe véve jelenértéken meghaladja az 50 millió eurónak megfelelő forintösszeget,
84. *nagy hatásfokú kapcsolt energiatermelés:* a 651/2014/EU bizottsági rendelet 2. cikk 107. pontja szerinti energiatermelés,
85. *nagyvállalkozás:* a 651/2014/EU bizottsági rendelet 2. cikk 24. pontja szerinti vállalkozás,
86. *nehéz helyzetben lévő vállalkozás:* az Atr. 6. §-ában meghatározott vállalkozás,
87. *okosfunkció-fogadási alkalmasság:* a 651/2014/EU bizottsági rendelet 2. cikk 103d. pontja szerinti jellemző,
88. *összeszámítási szabály:* a nagyberuházás elszámolható költségei kiszámításakor egyetlen beruházásnak kell tekinteni a kérelemben szereplő beruházást és a kérelmet benyújtó beruházó, valamint a kérelmet benyújtó beruházóval egy vállalatcsoportba tartozó beruházó által a kérelemben szereplő beruházás megkezdésétől számított háromszor háromszázhatvanöt napos időszakon belül a kérelemben szereplő beruházással azonos vármegyében megkezdett, ugyanazon vagy hasonló tevékenységhez kapcsolódó, regionális beruházási támogatásban részesülő beruházást,
89. *pályázat:* támogatási program végrehajtása érdekében megjelentetett pályázati felhívás, pályázati útmutató vagy pályázati kiírás a támogatási programban való részvételre,
90. *pénzügyi közvetítő:* a 651/2014/EU bizottsági rendelet 2. cikk 34. pontja szerinti pénzügyi intézmény,
91. *primerenergia:* a 651/2014/EU bizottsági rendelet 2. cikk 103a. pontja szerinti energia,
92. *projekt vagy beruházás megkezdése:*
    a) építési munka esetén az építési naplóba történő első bejegyzés vagy az építésre vonatkozó első visszavonhatatlan kötelezettségvállalás időpontja,
    b) tárgyi eszköz és immateriális javak beszerzése esetén
        ba) a vállalkozás általi első jogilag kötelező érvényűnek tekintett megrendelés napja,
        bb) – a ba) pont szerinti megrendelés hiányában – az arra vonatkozóan megkötött, jogilag kötelező érvényűnek tekintett szerződés létrejöttének a napja,
        bc) – a ba) pont szerinti megrendelés és a bb) pont szerinti szerződés hiányában – a beruházó által aláírással igazolt átvételi nap az első beszerzett gép, berendezés, anyag vagy termék szállítását igazoló okmányon,
    c) létesítmény felvásárlása esetén a felvásárlás időpontja,
    d) az a)–c) alpont közül több alpont együttes megvalósulása esetén a legkorábbi időpont, azzal, hogy nem tekinthető a projekt vagy beruházás megkezdésének a földterület megvásárlása, ha az nem képezi a projekt vagy beruházás elszámolható költségét, valamint az előkészítő munka költségének felmerülése,
93. *regionális beruházási támogatás:* a 651/2014/EU bizottsági rendelet 2. cikk 41. pontja szerinti támogatás,
94. *regionális repülőtér:* repülőtéri szolgáltatásokat magában foglaló tevékenységet végző olyan repülőtér, amelynek átlagos éves utasforgalma nem haladja meg a hárommillió főt,
95. *repülőtér:* a 651/2014/EU bizottsági rendelet 2. cikk 146. pontja szerinti repülőtér,
96. *repülőtéri infrastruktúra:* a 651/2014/EU bizottsági rendelet 2. cikk 144. pontja szerinti infrastruktúra,
97. *repülőtéri szolgáltatások:* a 651/2014/EU bizottsági rendelet 2. cikk 147. pontja szerinti szolgáltatások,
98. *saját forrás:* a kedvezményezett által a projekthez igénybe vett állami támogatást, valamint az Európai Unió intézményei, ügynökségei, közös vállalkozásai vagy más szervei által központilag kezelt, a tagállam ellenőrzése alá közvetlenül vagy közvetve nem tartozó uniós finanszírozást nem tartalmazó forrás,
99. *sajáttőke-befektetés:* a 651/2014/EU bizottsági rendelet 2. cikk 74. pontja szerinti befektetés,
100. *sertés:* az ex 0103921900 vámtarifaszámú, legalább 70 kg élősúlyú vágósertés vagy az élelmiszerlánc-felügyeleti információs rendszer szerinti tenyészsertés,

101. *szállítás:* a 651/2014/EU bizottsági rendelet 2. cikk 5. pontja szerinti személyszállítás vagy szolgáltatás,
102. *személyi jellegű ráfordítás:* a 651/2014/EU bizottsági rendelet 2. cikk 88. pontja szerinti ráfordítás,
103. *szénipar:* a 651/2014/EU bizottsági rendelet 2. cikk 13. pontja szerinti szén kitermelésével kapcsolatos tevékenység,
104. *szinten tartást szolgáló eszköz:* olyan eszköz, amely a kedvezményezett által már használt tárgyi eszközt, immateriális javakat váltja ki anélkül, hogy a kiváltás az előállított termék, a nyújtott szolgáltatás, a termelési, valamint a szolgáltatási folyamat alapvető változását vagy bővülését eredményezné,
105. *szokásos piaci feltételek:* a 651/2014/EU bizottsági rendelet 2. cikk 39a. pontja szerinti feltétel,
106. *támogatási intenzitás:* az Atr. 2. § 15. pontja szerinti intenzitás,
107. *támogatási program:* a 651/2014/EU bizottsági rendelet 2. cikk 16. pontja szerinti program,
108. *támogatást nyújtó:* az egyedi támogatás odaítéléséről döntő vagy a támogatási program, valamint a pályázat elkészítéséért felelős szerv vagy személy,
109. *támogatott létesítmény:* áttelepítés esetén az Európai Gazdasági Térségről szóló megállapodás egy másik szerződő felének területén található azon létesítmény, ahol a támogatott beruházásra sor kerül, azaz amely létesítménybe a kérelmet benyújtó beruházó vagy a kérelmet benyújtó beruházóval egy vállalatcsoportba tartozó beruházó áthelyezi az azonos vagy hasonló tevékenységet vagy annak egy részét,
110. *támogatástartalom:* az Atr. 2. § 19. pontjában meghatározott támogatási egyenérték,
111. *tárgyi eszköz:* a 651/2014/EU bizottsági rendelet 2. cikk 29. pontja szerinti eszköz,
112. *távfűtés és távhűtés:* a 651/2014/EU bizottsági rendelet 2. cikk 124a. pontja szerinti távfűtés vagy távhűtés,
113. *teljes finanszírozás:* a 651/2014/EU bizottsági rendelet 2. cikk 37. pontja szerinti finanszírozás,
114. *termékágazat:* a mezőgazdasági termékpiacok közös szervezésének létrehozásáról és a 922/72/EGK, a 234/79/EGK, az 1037/2001/EK és az 1234/2007/EK tanácsi rendelet hatályon kívül helyezéséről szóló, 2013. december 20-i 1308/2013/EU európai parlamenti és tanácsi rendelet 1. cikk (2) bekezdés a)–w) pontjában szereplő ágazat,
115. *természetes személy:* a 651/2014/EU bizottsági rendelet 2. cikk 73. pontja szerinti személy,
116. *természeti katasztrófához hasonlító kedvezőtlen éghajlati jelenség:* az (EU) 2022/2472 bizottsági rendelet 2. cikk 2. pontja szerinti éghajlati jelenség,
117. *tőkejuttatás:* a 651/2014/EU bizottsági rendelet 2. cikk 70. pontja szerinti juttatás,
118. *tőzsdén nem jegyzett kis- és középvállalkozás:* a 651/2014/EU bizottsági rendelet 2. cikk 76. pontja szerinti kis- és középvállalkozás,
119. *turisztikai tevékenység:* a 651/2014/EU bizottsági rendelet 2. cikk 47. pontja szerinti tevékenység,
120. *uniós szabvány:* a 651/2014/EU bizottsági rendelet 2. cikk 102. pontja szerinti szabvány,
121. *válságtámogatás:* az „Az állami támogatásokra vonatkozó, az Ukrajna elleni orosz agresszióval összefüggésben a gazdaság támogatását célzó ideiglenes válság- és átállási keret” című, 2023. március 17-i, 2023/C 101/03. számú európai bizottsági közlemény 2.1. szakasza szerinti támogatás,
122. *vállalkozás:* agrárvállalkozás vagy élelmiszer-feldolgozást végző vállalkozás,
123. *versenyeztetéses ajánlattételi eljárás:* a 651/2014/EU bizottsági rendelet 2. cikk 38. pontja szerinti eljárás.

II. FEJEZET
AZ ELŐIRÁNYZATOK FELHASZNÁLÁSÁNAK ÁLTALÁNOS SZABÁLYAI

3. § (1) A Nemzetgazdasági Minisztérium fejezetben előirányzatként megállapított fejezeti kezelésű előirányzatok részletes felhasználási szabályait az 1. melléklet, a központi kezelésű előirányzatok részletes felhasználási szabályait a 2. melléklet tartalmazza. Az 1. és 2. mellékletben meghatározott felhasználási szabályokat az egyes előirányzatokhoz rendelt megfelelő államháztartási egyedi azonosító számmal azonosított előirányzatra kell alkalmazni, annak a fejezeten belüli címrendi besorolásától függetlenül.

(2) Az e rendelet alapján
a) kijelölt kezelő szerv, valamint
b) – ha e rendelet a hatálya alá tartozó előirányzat esetében lebonyolító szerv igénybevételét lehetővé teszi – az Ávr. szerinti megállapodás keretében kijelölt lebonyolító szerv

(a kezelő szerv és a lebonyolító szerv a továbbiakban együtt: szerv) által az e rendelet hatálya alá tartozó előirányzatok vonatkozásában az e rendelet hatálybalépését megelőzően tett kötelezettségvállalást és teljesített kifizetést az arra jogosult szerv által tett kötelezettségvállalásnak és teljesített kifizetésnek kell tekinteni.

4. § (1) A támogató – a 4. alcímben meghatározott kivételekkel – az állami támogatás odaítélésekor tájékoztatja a kedvezményezettet a nyújtott támogatás támogatástartalmáról, a támogatásra vonatkozó, 9. § szerinti támogatási kategóriáról és annak szabályairól.

(2) A kedvezményezett köteles a támogatással kapcsolatos okiratokat és dokumentumokat a támogatási döntés meghozatala napjától számított tíz évig megőrizni.

5. § (1) A 651/2014/EU bizottsági rendelet, az (EU) 2022/2472 bizottsági rendelet, az (EU) 2023/2831 bizottsági rendelet, az 1408/2013/EU bizottsági rendelet és a 717/2014/EU bizottsági rendelet hatálya alá tartozó támogatás kizárólag átlátható formában nyújtható.

(2) Nem ítélhető meg támogatás

a) – a 22–24. alcím szerinti támogatás kivételével – azon szervezet részére, amely a támogatás odaítélésekor még nem tett eleget valamennyi, az Európai Bizottság európai uniós versenyjogi értelemben vett állami támogatás visszafizettetésére kötelező, Magyarországnak címzett határozata alapján fennálló visszafizetési kötelezettségének,

b) – a 22–24. alcím szerinti támogatás kivételével – nehéz helyzetben lévő vállalkozás részére,

c) – a 9., 10., 12., 14. és 24. alcím szerinti támogatás kivételével – halászati és akvakultúra-termékek termeléséhez,

d) – a 9., 10., 12., 14. és 24. alcím, valamint – ha a támogatás összegét nem a piacon vásárolt vagy forgalomba hozott termékek ára vagy mennyisége alapján határozzák meg – a 23. és 29. alcím szerinti támogatás kivételével – támogatás halászati és akvakultúra-termékek feldolgozásához és forgalmazásához,

e) – a 8., 10., 12., 14–18., 23., 25. és 26. alcím szerinti támogatás kivételével – elsődleges mezőgazdasági termeléshez,

f) mezőgazdasági termék feldolgozásához és mezőgazdasági termék forgalmazásához az 5–24., valamint a 26–29. alcím szerinti támogatás, ha

fa) a támogatás összege az elsődleges termelőktől beszerzett vagy érintett vállalkozások által forgalmazott ilyen termékek ára vagy mennyisége alapján kerül rögzítésre, vagy

fb) a támogatás az elsődleges termelőknek történő teljes vagy részleges továbbítástól függ,

g) a 25. alcím szerinti támogatás mezőgazdasági termék feldolgozásához és mezőgazdasági termék forgalmazásához,

h) exporttal kapcsolatos tevékenységhez, ha a támogatás az exportált mennyiségekhez, értékesítési hálózat kialakításához és működtetéséhez vagy az exporttevékenységgel összefüggésben felmerülő egyéb folyó kiadásokhoz közvetlenül kapcsolódik,

i) abban az esetben, ha azt import áru helyett hazai áru használatától teszik függővé,

j) olyan feltétellel, amely az európai uniós jog megsértését eredményezi,

k) – a 22–24. alcím szerinti támogatás kivételével – a versenyképtelen szénbányák bezárását elősegítő állami támogatásról szóló, 2010. december 10-i 2010/787/EU tanácsi határozat hatálya alá tartozó versenyképtelen szénbányák részére,

l) – a 22–24. alcím szerinti támogatás kivételével – atomenergia termeléshez.

(3) Nem ítélhető meg a 24. alcím szerinti támogatás

a) amennyiben annak összegét a piacon beszerzett vagy forgalomba hozott termékek ára vagy mennyisége alapján állapították meg;

b) exporttal kapcsolatos tevékenységhez, ha a támogatás az exportált mennyiségekhez, értékesítési hálózat kialakításához és működtetéséhez vagy az exporttevékenységgel összefüggésben felmerülő egyéb folyó kiadásokhoz közvetlenül kapcsolódik;

c) abban az esetben, ha azt import áru helyett hazai áru használatától teszik függővé;

d) halászhajók vásárlásához;

e) halászhajók főhajtóműveinek vagy kiegészítő hajtóműveinek korszerűsítéséhez vagy cseréjéhez;

f) a halászhajó halászati kapacitásának növelését célzó műveletekre vagy halfelderítési képességének növelését célzó berendezésekre;

g) új halászhajók építéséhez vagy halászhajók behozatalához;

h) a halászati tevékenységek végleges vagy ideiglenes szüneteltetésére, kivéve az (EU) 2021/1139 európai parlamenti és tanácsi rendelet 20. és 21. cikkében rögzített feltételeket teljesítő támogatást;
i) a felderítő halászatra;
j) vállalkozás tulajdonjogának átadására;
k) közvetlen újratelepítésre, kivéve abban az esetben, ha azt valamely uniós jogi aktus állományvédelmi intézkedésként kifejezetten előírja, illetve kísérleti újratelepítés esetén.

(4) Amennyiben a kedvezményezett a (2) bekezdés c)–f) pontjában kizárt ágazatok bármelyikében és ezektől eltérő egy vagy több ágazatban egyaránt végez tevékenységet, a 22. alcím szerinti támogatás akkor nyújtható a kedvezményezett részére ez utóbbi egyéb tevékenységhez, ha a kedvezményezett megfelelő eszközökkel – úgymint a tevékenységek szétválasztásával vagy számviteli elkülönítéssel – biztosítja, hogy a (2) bekezdés c)–f) pontja szerinti kizárt ágazatokban végzett tevékenységek ne részesüljenek a 22. alcím szerinti támogatásban.

(5) Nem minősül exporttámogatásnak az olyan támogatás, amellyel a kereskedelmi vásárokon való részvétel költségeihez vagy olyan tanulmányok vagy tanácsadói szolgáltatások költségeihez járulnak hozzá, amelyek valamely új vagy már meglévő terméknek egy új piacra történő bevezetéséhez szükségesek.

(6) A 651/2014/EU bizottsági rendelet vagy az (EU) 2022/2472 bizottsági rendelet alapján támogatás – az induló vállalkozásnak nyújtott támogatás és a kultúrát és a kulturális örökség megőrzését előmozdító támogatás kivételével – csak akkor ítélhető meg, ha a kedvezményezett a 651/2014/EU bizottsági rendelet 6. cikk (2) bekezdésében vagy az (EU) 2022/2472 bizottsági rendelet 6. cikk (2) bekezdésében meghatározott kötelező tartalmi elemeket tartalmazó támogatási kérelmét a projekt megkezdése előtt írásban benyújtotta.

(7) A (6) bekezdés szerinti támogatási kérelem benyújtása előtt felmerült költségekre kizárólag az (EU) 2023/2831 bizottsági rendelet, az 1408/2013/EU bizottsági rendelet vagy a 717/2014/EU bizottsági rendelet szerinti csekély összegű támogatás nyújtható.

6. § (1) Azonos vagy részben azonos azonosítható elszámolható költségek esetén az e rendelet szerinti támogatás abban az esetben halmozható más, helyi, regionális, hazai vagy uniós forrásból származó állami támogatással, ha az nem vezet a csoportmentességi rendeletekben vagy az Európai Bizottság jóváhagyó határozatában meghatározott legmagasabb támogatási intenzitás túllépéséhez.

(2) Az e rendelet szerinti támogatás különböző azonosítható elszámolható költségek esetén halmozható más, helyi, regionális, hazai vagy uniós forrásból származó állami támogatással.

(3) Az egy projekthez igénybe vett összes támogatás – függetlenül attól, hogy annak finanszírozása uniós, országos, regionális vagy helyi forrásból történik – támogatási intenzitása nem haladhatja meg az irányadó uniós állami támogatási szabályokban meghatározott támogatási intenzitást vagy támogatási összeget.

(4) Amennyiben a 4. és 9., valamint a 22–24. alcím szerinti támogatás nem rendelkezik azonosítható elszámolható költségekkel, a támogatás bármely egyéb, azonosítható elszámolható költségekkel rendelkező állami támogatással halmozható. Az azonosítható elszámolható költségekkel nem rendelkező támogatás a csoportmentességi rendeletekben és az Európai Bizottság jóváhagyó határozatában meghatározott legmagasabb teljes finanszírozási határértékig bármilyen más, azonosítható elszámolható költségekkel nem rendelkező állami támogatással halmozható.

(5) A 23., 25. és 26. alcím szerinti támogatás ugyanazon elszámolható költségek vonatkozásában nem halmozható az (EU) 2021/2115 európai parlamenti és tanácsi rendelet 145. cikk (2) bekezdése és 146. cikke szerinti kifizetésekkel, ha az ilyen halmozódás eredményeként a támogatási intenzitás vagy a támogatási összeg meghaladná a 23., 25. és 26. alcím szerinti értékeket.

7. § (1) A támogatási intenzitás kiszámítása során valamennyi felhasznált számadatot az adók és illetékek levonása előtt kell figyelembe venni. Ha a támogatást visszatérítendő formában nyújtják, a támogatás összegének a támogatástartalmat kell tekinteni.

(2) A több részletben kifizetett támogatást a támogatási döntés időpontja szerinti értékre kell diszkontálni a diszkont kamatláb alkalmazásával.

(3) Ha a támogatás nyújtása az uniós állami támogatási szabályok értelmében az Európai Bizottság előzetes jóváhagyásától függ, a támogatás az Európai Bizottság jóváhagyó határozatának meghozatalát követően fizethető ki.

(4) Az általános forgalmi adó (a továbbiakban: ÁFA) nem támogatható, kivéve, ha az ÁFA-ra vonatkozó jogszabályok értelmében nem igényelhető vissza.

(5) Az Atr. 18. § (2) bekezdés a) és c) pontja szerint előzetesen be kell jelenteni az Európai Bizottság részére az egyedi támogatást, ha a támogatás összege

1. regionális beruházási támogatás esetén a beruházáshoz igényelt összes állami támogatással együtt – figyelembe véve a nagyberuházásokra vonatkozó rendelkezéseket – egy legalább 110 millió euró elszámolható költségű beruházási támogatás esetében vállalkozásonként és projektenként meghaladja
   a) a 24,75 millió eurónak megfelelő forintösszeget, ha a maximális regionális támogatási intenzitás 30%,
   b) a 41,25 millió eurónak megfelelő forintösszeget, ha a maximális regionális támogatási intenzitás 50%,
   c) a 49,5 millió eurónak megfelelő forintösszeget, ha a maximális regionális támogatási intenzitás 60%,
2. a kis- és középvállalkozásnak nyújtott beruházási támogatás esetén vállalkozásonként és beruházási projektenként meghaladja a 8,25 millió eurónak megfelelő forintösszeget,
3. a kis- és középvállalkozás részére tanácsadáshoz nyújtott támogatás esetén vállalkozásonként és beruházási projektenként meghaladja a 2,2 millió eurónak megfelelő forintösszeget,
4. a kis- és középvállalkozás vásáron való részvételéhez nyújtott támogatás esetén vállalkozásonként meghaladja a 2,2 millió eurónak megfelelő forintösszeget,
5. induló vállalkozásnak nyújtott támogatás esetén meghaladja a támogatási kategóriára vonatkozó szabályokban meghatározott mértéket,
6. kutatásfejlesztési projekthez nyújtott támogatás esetén
   a) vállalkozásonként és projektenként meghaladja az 55 millió eurónak megfelelő forintösszeget, ha a projekt elszámolható költségeinek több mint fele az alapkutatás kategóriájába tartozó tevékenységgel kapcsolatban merül fel,
   b) vállalkozásonként és projektenként meghaladja a 35 millió eurónak megfelelő forintösszeget, ha a projekt elszámolható költségeinek több mint fele az ipari kutatás kategóriájába vagy együttesen véve az ipari kutatás és az alapkutatás kategóriájába tartozó tevékenységgel kapcsolatban merül fel,
   c) vállalkozásonként és projektenként meghaladja a 25 millió eurónak megfelelő forintösszeget, ha a projekt elszámolható költségeinek több mint fele a kísérleti fejlesztés kategóriájába tartozó tevékenységgel kapcsolatban merül fel,
   d) meghaladja a 2. pont a)–c) alpont szerinti összeg kétszeresét EUREKA-projekt vagy az EUMSz 185. vagy 187. cikke alapján létrehozott közös vállalkozás által megvalósított projekt, vagy a 28. § (5) bekezdés b) pontjában előírt feltételeknek megfelelő projekt esetén,
   e) meghaladja a 6. pont a)–d) alpont szerinti összeg 150%-át, ha a kutatásfejlesztési projekthez a támogatást visszafizetendő előleg formájában nyújtják – amelyet a bruttó támogatási egyenérték kiszámításához használt módszertan hiánya esetén az elszámolható költségek százalékában kell kifejezni –, és ha az intézkedés biztosítja, hogy a projekt észszerű és prudenciális megfontolások alapján megállapított, sikeres befejezése esetén az előleg legalább a támogatás odaítélésekor irányadó diszkont kamatláb szerint számított kamattal megnövelve kerül visszafizetésre,
   f) kutatási tevékenységet előkészítő megvalósíthatósági tanulmányhoz nyújtott támogatás esetén tanulmányonként meghaladja a 8,25 millió eurónak megfelelő forintösszeget,
7. a kutatási infrastruktúrához nyújtott beruházási támogatás esetén infrastruktúránként meghaladja a 35 millió eurónak megfelelő forintösszeget,
8. a kis- és középvállalkozásnak nyújtott innovációs támogatás esetén vállalkozásonként és projektenként meghaladja a 10 millió eurónak megfelelő forintösszeget,
9. eljárási és szervezési innováció támogatása esetén vállalkozásonként és projektenként meghaladja a 12,5 millió eurónak megfelelő forintösszeget,
10. képzési támogatás esetén képzési projektenként meghaladja a 3 millió eurónak megfelelő forintösszeget,
11. épületek energiahatékonyságának kivételével az energiahatékonysági intézkedéshez nyújtott beruházási támogatás, épület-energiahatékonysági intézkedéshez nyújtott beruházási támogatás megújuló energia, megújuló hidrogén és nagy hatásfokú kapcsolt energiatermeléshez nyújtott beruházási támogatás esetén vállalkozásonként és beruházásonként meghaladja a 30 millió eurónak megfelelő forintösszeget,
12. energetikai célú infrastruktúrához nyújtott beruházási támogatás esetén vállalkozásonként és beruházásonként meghaladja a 70 millió eurónak megfelelő forintösszeget,
13. kultúrát és a kulturális örökség megőrzését előmozdító
   a) beruházási támogatás esetén meghaladja a projektenként 165 millió eurónak megfelelő forintösszeget,

b) működési támogatás esetén meghaladja a vállalkozásonként évente 82,5 millió eurónak megfelelő forintösszeget,

14. sportlétesítményhez és multifunkcionális szabadidős létesítményhez nyújtott beruházási támogatás esetén meghaladja a 33 millió eurónak megfelelő forintösszeget, vagy a projekt teljes költsége meghaladja a 110 millió eurónak megfelelő forintösszeget,
15. a regionális repülőterekre irányuló támogatás esetében meghaladja a 63. §-ban meghatározott mértéket,
16. helyi infrastruktúra fejlesztéséhez nyújtott beruházási támogatás esetén meghaladja egyazon infrastruktúra esetén a 11 millió eurónak megfelelő forintösszeget vagy a 22 millió eurónak megfelelő forintösszeget meghaladó összköltséget,
17. mezőgazdasági üzemekben végrehajtott, elsődleges mezőgazdasági termeléshez irányuló beruházásokhoz nyújtott támogatás esetén kedvezményezettenként és projektenként meghaladja a 0,6 millió eurónak megfelelő forintösszeget,
18. a mezőgazdasági termékek feldolgozásával vagy forgalmazásával kapcsolatos beruházásokhoz nyújtott támogatás esetén vállalkozásonként és beruházási projektenként meghaladja a 7,5 millió eurónak megfelelő forintösszeget.

(6) Az Atr. 18. § (2) bekezdés a) pontja szerint előzetesen be kell jelenteni az Európai Bizottság részére az egyedi támogatást, ha belvízi kikötő fejlesztéséhez nyújtott beruházási támogatás esetén a projekt elszámolható költsége meghaladja

a) a 44 millió eurónak megfelelő forintösszeget, vagy
b) – a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről szóló, 2013. december 11-i 1315/2013/EU európai parlamenti és tanácsi rendelet 47. cikkében meghatározott munkatervben szereplő belvízi kikötő esetén – az 55 millió eurónak megfelelő forintösszeget, azzal, hogy ha a projekt kotrást is tartalmaz, e pont alkalmazásában az adott belvízi kikötőben egy naptári éven belül végrehajtott összes kotrási tevékenység tekintendő a projekt részének.

(7) E rendelet alapján

a) a 651/2014/EU bizottsági rendelet szerinti támogatás esetén 2027. június 30-ig,
b) az (EU) 2023/2831 bizottsági rendelet szerinti csekély összegű támogatás esetén 2031. június 30-ig,
c) a 717/2014/EU bizottsági rendelet szerinti csekély összegű támogatás esetén 2030. június 30-ig,
d) az 1408/2013/EU bizottsági rendelet szerinti mezőgazdasági csekély összegű támogatás esetén 2028. június 30-ig,
e) az (EU) 2022/2472 bizottsági rendelet szerinti támogatás esetén 2030. június 30-ig,
f) válságtámogatás esetén 2024. június 30-ig,
g) halászati csekély összegű támogatás esetén 2027. december 31-ig

lehet támogatási döntést hozni.

8. § (1) A támogatást nyújtó köteles adatot szolgáltatni a Támogatásokat Vizsgáló Iroda részére a 651/2014/EU bizottsági rendelet 9. cikke és az (EU) 2022/2472 bizottsági rendelet 9. cikke szerinti közzététel céljából a 100 000 eurónak, az elsődleges mezőgazdasági termelés támogatása esetén a 10 000 eurónak megfelelő forintösszeget meghaladó egyedi támogatásokról.

(2) Az (1) bekezdés szerinti adatszolgáltatást az Atr. 18/A–18/D. §-a szerint kell teljesíteni.

III. FEJEZET
AZ EURÓPAI UNIÓS ÁLLAMI TÁMOGATÁSOKRA VONATKOZÓ SZABÁLYOK

3. Az európai uniós támogatásoknak való megfelelés

9. § Az EUMSz 107. cikk (1) bekezdése szerinti állami támogatások esetében az 1. mellékletben foglalt táblázat

1. 4–13. és 15. sora alapján az (EU) 2023/2831 bizottsági rendelet szerinti csekély összegű támogatás;
2. 4., 6., 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 13. és 14. cikke szerinti regionális beruházási támogatás;
3. 4., 6., 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 17. cikke szerinti kis- és középvállalkozásnak nyújtott beruházási támogatás;

4. 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 18. cikke szerinti kis- és középvállalkozás részére tanácsadáshoz nyújtott támogatás;
5. 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 19. cikke szerinti kis- és középvállalkozás vásáron való részvételéhez nyújtott támogatás;
6. 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 22. cikke szerinti induló vállalkozásnak nyújtott támogatás;
7. 6., 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 25. cikke szerinti kutatás-fejlesztési projektekhez nyújtott támogatás;
8. 6., 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 26. cikke szerinti kutatási infrastruktúrához nyújtott beruházási támogatás;
9. 6., 8., 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 28. cikke szerinti kis- és középvállalkozásoknak nyújtott innovációs támogatás;
10. 6., 8. és 9. sora alapján a 651/2014/EU bizottsági rendelet 29. cikke szerinti eljárási és szervezési innováció támogatása;
11. 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 31. cikke szerinti képzési támogatás;
12. 7. és 9. sora alapján a 651/2014/EU bizottsági rendelet 38. cikke szerinti az épületek energiahatékonyságának kivételével az energiahatékonysági intézkedéshez nyújtott beruházási támogatás;
13. 7. és 9. sora alapján a 651/2014/EU bizottsági rendelet 38a. cikke szerinti épület-energiahatékonysági intézkedéshez nyújtott beruházási támogatás;
14. 7. és 9. sora alapján a 651/2014/EU bizottsági rendelet 41. cikke szerinti a megújuló energia, megújuló hidrogén és nagy hatásfokú kapcsolt energiatermeléshez nyújtott beruházási támogatás;
15. 7. sora alapján a 651/2014/EU bizottsági rendelet 48. cikke szerinti energetikai infrastruktúrára irányuló beruházási támogatás;
16. 10. és 15. sora alapján a 651/2014/EU bizottsági rendelet 53. cikke szerinti a kultúrát és a kulturális örökség megőrzését előmozdító támogatás;
17. 11. és 15. sora alapján a 651/2014/EU bizottsági rendelet 55. cikke szerinti sportlétesítményekre és multifunkcionális szabadidős létesítményekre nyújtott támogatás;
18. 9. és 15. sora alapján a 651/2014/EU bizottsági rendelet 56. cikke szerinti helyi infrastruktúrára irányuló támogatás;
19. 15. sora alapján a 651/2014/EU bizottsági rendelet 56a. cikke szerinti regionális repülőterekre irányuló támogatás vagy az Európai Bizottság előzetes jóváhagyását igénylő támogatási intézkedés esetén az Európai Bizottságnak a repülőtereknek és a légitársaságoknak nyújtott állami támogatásról szóló közleménye (2014/C99/03) szerinti támogatás;
20. 15. sora alapján a 651/2014/EU bizottsági rendelet 56c. cikke szerinti belvízi kikötőkre irányuló támogatás;
21. 4. és 15. sora alapján az 1408/2013/EU bizottsági rendelet szerinti mezőgazdasági csekély összegű támogatás;
22. 4. sora alapján a 717/2014/EU bizottsági rendelet szerinti halászati és akvakultúra ágazatban nyújtott csekély összegű támogatás;
23. 4. sora alapján az (EU) 2022/2472 bizottsági rendelet 14. cikke szerinti az elsődleges mezőgazdasági termeléshez kapcsolódó, mezőgazdasági üzemekben végrehajtott, tárgyi eszközökre vagy immateriális javakra irányuló beruházásokhoz nyújtott támogatás;
24. 4. sora alapján az (EU) 2022/2472 bizottsági rendelet 17. cikke szerinti mezőgazdasági termékek feldolgozásával és a mezőgazdasági termékek forgalmazásával kapcsolatos beruházásokhoz nyújtott támogatás;
25. 4–15. sora alapján az SA.106542 (2023/N) számú, valamint az azt módosító európai bizottsági határozatokban foglaltakkal összhangban az „Az állami támogatásokra vonatkozó, az Ukrajna elleni orosz agresszióval összefüggésben a gazdaság támogatását célzó ideiglenes válság- és átállási keret” című, 2023. március 17-i, 2023/C 101/03. számú európai bizottsági közlemény 2.1. szakasza szerinti válságtámogatás;
26. 4. sora alapján az Európai Unió működéséről szóló szerződés 107. cikk (1) bekezdése szerinti állami támogatásnak minősülő, és az „Állami támogatási intézkedésekre vonatkozó ideiglenes keret a gazdaságnak a jelenlegi COVID-19-járvánnyal összefüggésben való támogatása céljából” című, 2020. március 19-i, 2020/C 91 I/01 számú európai bizottsági közlemény 3.1. pontja szerint nyújtott támogatás

nyújtható.

4. Kamattámogatás, kezelési költségtámogatás, egyéb költségtámogatás és kezességi díjtámogatás

10. § (1) Az 1. mellékletben foglalt táblázat 4. sora szerint a Széchenyi Kártya Program Konstrukciók – a 11. §-ban meghatározott Agrár Széchenyi Kártya Konstrukciók kivételével – keretében nyújtott kamattámogatás, kezelési költségtámogatás és egyéb költségtámogatás a támogatott ügylet jellegétől függően a 22. alcímben meghatározott csekély összegű támogatásnak, a 23. alcímben meghatározott mezőgazdasági csekély összegű támogatásnak vagy az Európai Bizottságnak az SA.103089 (2022/N) számú ügyben hozott C(2022) 4303 final számú határozata és ezen bizottsági határozatot érintő módosító határozatai szerinti, a 29. alcímben meghatározott válságtámogatásnak minősül.

(2) Az 1. mellékletben foglalt táblázat 4. sora szerinti intézményi kezességi díjtámogatás és a Széchenyi Kártya Program Konstrukciók keretében nyújtott kezességi díjtámogatás a támogatott ügylet jellegétől függően a 22. alcímben meghatározott csekély összegű támogatásnak, a 23. alcímben meghatározott mezőgazdasági csekély összegű támogatásnak, az Európai Bizottságnak az SA.103315 (2022/N) számú ügyben hozott C(2022) 5019 final számú határozata, vagy az SA.103089 (2022/N) számú ügyben hozott C(2022) 4303 final számú határozata szerinti, a 29. alcímben meghatározott válságtámogatásnak minősül, az érintett bizottsági határozatok mindenkori módosításainak figyelembevételével.

(3) A Széchenyi Kártya Programban, illetve az előirányzat felhasználásában a KAVOSZ Széchenyi Kártya Program Zártkörűen Működő Részvénytársaság (a továbbiakban: KAVOSZ Zrt.) közreműködői feladatokat ellátó és a Széchenyi Kártya Programot működtető szervezet, amelynek keretében ellátja a Széchenyi Kártya Program Konstrukciók lebonyolítása és működtetése során a Támogató jóváhagyásával kiadott, a Konstrukciók részletes szabályait tartalmazó, a KAVOSZ Zrt. honlapján közzétett, mindenkor hatályos Széchenyi Kártya Program Üzletszabályzatában meghatározott és a Támogató által rábízott feladatokat.

(4) A Széchenyi Kártya Program Konstrukciók keretében a vállalkozásoknak csekély összegű támogatás alkalmazása esetén a megítélt támogatás összegébe a hitelkeret támogatott futamidejének időszakára jutó kamattámogatás, kezelési költségtámogatás, egyéb, pénzügyi intézmény által megelőlegezett költségtámogatás és kezességi díjtámogatás, valamint a kezességvállaló intézmény kedvezményes kezességvállalásából adódó támogatástartalom összege számít bele.

(5) Csekély összegű támogatásként nyújtott intézményi kezességi díjtámogatás esetén a Garantiqa Hitelgarancia Zártkörűen Működő Részvénytársaság (a továbbiakban: Garantiqa Zrt.), a Széchenyi Kártya Program Konstrukciók keretében csekély összegű támogatásként nyújtott támogatások esetén – kezességvállaló intézmény kedvezményes kezességvállalásából adódó támogatástartalom kivételével – a KAVOSZ Zrt. tájékoztatja a kedvezményezettet arról, hogy csekély összegű támogatásban részesül. A tájékoztatásnak kifejezetten utalnia kell a csekély összegű támogatásokról szóló bizottsági rendeletre, hivatkozva annak pontos címére és az Európai Unió Hivatalos lapjában való kihirdetésre, valamint meg kell határoznia a támogatás összegét, az Atr. 2. mellékletében foglalt módszertan alapján kiszámolt támogatástartalomban kifejezve.

(6) A Széchenyi Kártya Program Konstrukciók keretében a kedvezményezett számára az (1) bekezdésben meghatározott válságtámogatásként megítélt válságtámogatás összegébe a hitel támogatott futamidejének időszakára eső kamattámogatás, kezelési költségtámogatás és egyéb költségtámogatás a (2) bekezdés szerinti, 29. alcímben meghatározott válságtámogatásnak minősülő kezességi díjtámogatás összege számít bele.

(7) A Széchenyi Kártya Program Konstrukciók keretében lehetőség van egy hitelügylethez kapcsolódóan a 29. alcímben meghatározott válságtámogatási jogcímen biztosított támogatás nyújtására és a kezességvállaló intézmény kezességvállalása tekintetében csekély összegű jogcímen biztosított készfizető kezesség biztosítására. Ez esetben a megítélt támogatás összegébe az (1) és (2) bekezdés szerinti, a 29. alcímben meghatározott válságtámogatásnak minősülő kamattámogatás, kezelési költségtámogatás, kezességi díjtámogatás, valamint a kezességvállaló intézmény csekély összegű jogcímen vállalt kedvezményes kezességvállalásából adódó támogatástartalom együttes összege számít bele.

(8) A Széchenyi Kártya Program Konstrukciók keretében a vállalkozásoknak az (1) és (2) bekezdés szerinti, a 29. alcímben meghatározott válságtámogatásnak minősülő kamattámogatás, kezelési költségtámogatás, kezességi díjtámogatás és egyéb költségtámogatás esetén a KAVOSZ Zrt. írásban tájékoztatja a kedvezményezettet arról, hogy válságtámogatásban részesült a válságközlemény 2.1. szakasza alapján elfogadott bizottsági határozatok szerint. A tájékoztatásban rögzíteni kell a válságtámogatás támogatástartalmát, amely megfelel a teljes odaítélt kamattámogatás, kezelési költségtámogatás, kezességi díjtámogatás és egyéb költségtámogatás összegének, jelenérték számítása nélkül.

(9) A (2) bekezdés szerinti kezességi díjtámogatás esetén – a Széchenyi Kártya Program Konstrukció kivételével – a Garantiqa Zrt. írásban tájékoztatja a kedvezményezettet arról, hogy támogatásban részesült az ügylet jellegétől függően csekély összegű jogcímen vagy a válságközlemény 2.1. szakasza alapján.

(10) A Széchenyi Kártya Program Konstrukciókhoz az (1) és (2) bekezdés szerinti, a 29. alcímben meghatározott válságtámogatásnak minősülő kamattámogatás, kezelési költségtámogatás biztosítása esetén lehetőség van a Garantiqa Zrt. által a válságközlemény 2.2. szakasza szerint vállalt készfizető kezesség biztosítására is, amely készfizető kezességvállalásnak és a hozzá kapcsolódó kezességi díjtámogatásnak nincs a válságközlemény 2.1. szakasza szerinti támogatási keretet terhelő támogatástartalma.

(11) A kamattámogatások, kezelési költségtámogatások, egyéb költségtámogatások és kezességi díjtámogatások kifizetésében részesülők köre azon pénzügyi intézmények, amelyek a vállalkozásnak megítélt támogatás összegét az Ávr. 88. § (1) bekezdés c) pontja alapján megelőlegezik a végső kedvezményezettnek minősülő, támogatásra jogosult mikro-, kis- és középvállalkozások részére.

11. § (1) Az 1. mellékletben foglalt táblázat 4. sora szerint az Agrár Széchenyi Kártya Konstrukciók keretében nyújtott pénzügyi intézmény által megelőlegezett kamattámogatás, kezességi díjtámogatás, kezelési költségtámogatás és a pénzügyi intézmény által nem megelőlegezett egyéb költségtámogatás

a) a 22. alcímben meghatározott általános csekély összegű támogatásnak,

b) a 23. alcímben meghatározott mezőgazdasági csekély összegű támogatásnak,

c) a 24. alcímben meghatározott halászati és akvakultúra ágazatban nyújtott csekély összegű támogatásnak

[az a)–c) pont a továbbiakban együtt: csekély összegű támogatás] vagy

d) a 29. alcímben meghatározott, az Európai Bizottságnak az SA.103089 (2022/N) számú ügyben hozott C(2022) 4303 final számú határozata és ezen bizottsági határozatot érintő módosító határozatai szerinti válságtámogatásnak vagy

e) a 20. alcímben meghatározott, az „Állami támogatási intézkedésekre vonatkozó ideiglenes keret a gazdaságnak a jelenlegi COVID-19-járvánnyal összefüggésben való támogatása céljából” című, 2020. március 19-i, 2020/C 91 I/01 számú európai bizottsági közlemény szerinti átmeneti támogatásnak

[az a)–e) pont a továbbiakban együtt: támogatás] minősül.

(2) Az Agrár Széchenyi Kártya Konstrukciók keretében a vállalkozásoknak csekély összegű támogatás jogcímen nyújtott támogatás alkalmazása esetén a megítélt csekély összegű támogatás összegébe kamattámogatás, kezességi díjtámogatás, kezelési költségtámogatás és egyéb költségtámogatás, valamint az Agrár-Vállalkozási Hitelgarancia Alapítvány (a továbbiakban: AVHGA) kedvezményes kezességvállalásából adódó támogatástartalmának összege számít bele.

(3) Az Agrár Széchenyi Kártya Konstrukciók keretében a kedvezményezett számára az (1) bekezdés d) pontjában meghatározott válságtámogatásként megítélt válságtámogatás összegébe a hitel támogatott futamidejének időszakára eső kamattámogatás, kezességi díjtámogatás, kezelési költségtámogatás számít bele.

(4) Az Agrár Széchenyi Kártya Konstrukciók keretében lehetőség van egy hitelügylethez kapcsolódóan a 29. alcímben meghatározott válságtámogatási jogcímen biztosított támogatás nyújtására és az AVHGA kedvezményes díjon nyújtott kezességvállalásából származó támogatás tekintetében csekély összegű támogatás jogcímen biztosított készfizető kezesség biztosítására. Ez esetben a megítélt támogatás összegébe az (1) bekezdés d) pontja szerinti, a 29. alcímben meghatározott válságtámogatásnak minősülő kamattámogatás, kezelési költségtámogatás, kezességi díjtámogatás és valamint az AVHGA csekély összegű támogatás jogcímen vállalt kedvezményes kezességvállalásából adódó támogatástartalom együttes összege számít bele.

(5) Az Agrár Széchenyi Kártya Konstrukciók keretében a vállalkozásoknak járó kamattámogatás, kezességi díjtámogatás, kezelési költségtámogatás esetén a Magyar Államkincstár írásban tájékoztatja a kedvezményezettet arról, hogy támogatásban részesült.

(6) Az Agrár Széchenyi Kártya Konstrukciók az (1) bekezdés d) pontja szerinti, a 29. alcímben meghatározott válságtámogatásnak minősülő kamattámogatás, kezelési költségtámogatás biztosítása esetén lehetőség van az AVHGA által a válságközlemény 2.2. szakasza szerint vállalt készfizető kezesség biztosítására is, amely készfizető kezességvállalásnak és a hozzá kapcsolódó kezességi díjtámogatásnak nincs a válságközlemény 2.1. szakasza szerinti támogatási keretet terhelő támogatástartalma.

12. § (1) Az 1. mellékletben foglalt táblázat 4. sora szerint az MFB Magyar Fejlesztési Bank Zártkörűen Működő Részvénytársaság (a továbbiakban: MFB Zrt.) hitelprogramjainak kamattámogatása a támogatott ügylet jellegétől függően az 5. alcímben meghatározott regionális beruházási támogatásnak, a 6. alcímben meghatározott kis- és középvállalkozásnak nyújtott beruházási támogatásnak, a 22. alcímben meghatározott csekély összegű támogatásnak, a 23. alcímben meghatározott mezőgazdasági csekély összegű támogatásnak, a 25. alcímben meghatározott elsődleges mezőgazdasági termeléshez kapcsolódó, mezőgazdasági üzemekben végrehajtott, tárgyi eszközökre vagy immateriális javakra irányuló beruházásokhoz nyújtott támogatásnak, a 26. alcímben meghatározott mezőgazdasági termékek feldolgozásával és a mezőgazdasági termékek forgalmazásával kapcsolatos beruházásokhoz nyújtott támogatásnak vagy a 29. alcímben meghatározott válságtámogatásnak minősül.

(2) A támogatás összegébe a hitelkeret támogatott futamidejének időszakára jutó kamattámogatás, valamint az MFB Krízis Hitel és az MFB Gazdaság Újjáépítési Hitel Program 2.0. esetében ezen felül a kezességi díjtámogatás támogatástartalmának összege számít bele.

(3) Az állami támogatásról szóló igazolást az Atr. 4. §-ában foglaltakkal összhangban a kedvezményezett (adós) részére közvetlen finanszírozás esetén az MFB Zrt. adja ki. Refinanszírozás esetén az MFB Zrt. által előkészített igazolást a közreműködő pénzügyi vállalkozás vagy hitelintézet dokumentált módon átadja a kedvezményezett (adós) részére. A tájékoztatás csekély összegű támogatás esetén kifejezetten utal a csekély összegű támogatásokról szóló (EU) 2023/2831 bizottsági rendeletre, valamint az 1408/2013/EU bizottsági rendeletekre hivatkozva annak pontos címére és az Európai Unió Hivatalos lapjában való kihirdetésre.

5. A regionális beruházási támogatás

13. § (1) A regionális beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) igénybevételének feltétele, hogy a tervezett beruházás olyan induló beruházásnak minősüljön, amelyet az Atr. 25. § (1) bekezdése szerinti területeken kis- és középvállalkozás vagy nagyvállalkozás valósít meg.

(2) Nagyvállalkozás esetén a termelési folyamat alapvető megváltozását eredményező beruházás esetén a támogatás akkor vehető igénybe, ha az elszámolható költségek összege meghaladja az alapvetően megváltoztatandó eredeti termelési folyamathoz kapcsolódó eszközökre a kérelem benyújtásának adóévét megelőző három adóévben elszámolt terv szerinti értékcsökkenés összegét.

(3) Meglévő létesítmény termékkínálatának a létesítményben addig nem gyártott termékkel történő bővítését eredményező induló beruházás esetén az elszámolható költségeknek legalább 200%-kal meg kell haladniuk az eredeti tevékenység keretében használt és az új tevékenység keretében is használni tervezett tárgyi eszközöknek és immateriális javaknak a beruházás megkezdése előtti adóévben nyilvántartott könyv szerinti értékét.

14. § (1) A támogatás akkor vehető igénybe, ha a támogatott vállalkozás kötelezettséget vállal arra, hogy a beruházással létrehozott tevékenységet az üzembe helyezés időpontjától számított legalább öt évig, kis- és középvállalkozás esetén legalább három évig fenntartja.

(2) A beszerzett eszköznek újnak kell lennie, kivéve a felvásárlás esetét, vagy ha a beruházó kis- és középvállalkozásnak minősül.

(3) Az (1) bekezdés szerinti követelmény nem akadályozza a gyors technológiai változások miatt a fenntartási időszak alatt korszerűtlenné vált vagy meghibásodott tárgyi eszköz cseréjét, ha a fenntartási időszak alatt a gazdasági tevékenység fenntartása az érintett régióban biztosított. A korszerűtlenné vált vagy meghibásodott és támogatásban már részesült tárgyi eszköz cseréjére a fenntartási időszakban a beruházó állami támogatásban nem részesülhet. Az új eszköznek a lecserélt tárgyi eszközzel azonos funkcióval és azonos vagy nagyobb kapacitással kell rendelkeznie, továbbá a gyártási időpontja nem lehet korábbi, mint a lecserélt tárgyi eszközé.

(4) A támogatás akkor vehető igénybe, ha a beruházó az elszámolható költségek legalább 25%-át saját forrásból biztosítja, továbbá a teljes beruházás megvalósításához szükséges költségek forrását a támogató számára bemutatja.

(5) A kedvezményezett – a támogatási kérelem benyújtásával egyidejűleg – a támogatás visszafizetésének terhe mellett nyilatkozik arról, hogy a támogatási kérelem benyújtását megelőző két évben nem valósított meg áttelepítést abba a létesítménybe, amelyben a támogatási kérelem tárgyát képező induló beruházást meg kívánja valósítani, és kötelezettséget vállal arra, hogy a támogatási kérelem tárgyát képező induló beruházás befejezését követő legalább két évig nem kerül sor a létesítmény áttelepítésére abba a létesítménybe, amelyben a támogatási kérelem tárgyát képező induló beruházást meg kívánja valósítani.

15. § Nem nyújtható támogatás

a) az acélipari tevékenységhez,

b) a lignitipari tevékenységhez,

c) a szénipari tevékenységhez,

d) az ellenszolgáltatásért végzett légi, tengeri, közúti, vasúti és belvízi úton történő személy- vagy áruszállítási szolgáltatás nyújtásához vagy a kapcsolódó infrastruktúrához,

e) az energiatermelési, energiatárolási, energiaátviteli, energiaelosztási tevékenységhez és energetikai célú infrastruktúra létrehozását szolgáló beruházáshoz,

f) a szélessávú ágazatban végzett tevékenységhez.

16. § (1) A támogatási intenzitás legmagasabb mértéke az egyes területeken az Atr. 25. § (1) bekezdésében meghatározott mérték, figyelemmel a (2)–(5) bekezdésben foglaltakra.

(2) A támogatási intenzitás – a nagyberuházások kivételével – kisvállalkozás esetén 20 százalékponttal, középvállalkozás esetén 10 százalékponttal növelhető, ha a beruházó a kérelem benyújtásakor, valamint a döntés meghozatalakor is megfelel az adott vállalkozási méret feltételeinek.

(3) A támogatási intenzitás legmagasabb mértéke nagyberuházás esetén az Atr. 25. § (3) bekezdésében meghatározott mérték.

(4) Nagyberuházás esetén az odaítélhető összes állami támogatás összegéből le kell vonni a beruházás megkezdését megelőző háromszor háromszázhatvanöt napos időszakban a kedvezményezett által vagy a kedvezményezettől független harmadik félnek nem minősülő beruházó által azonos vármegyében megkezdett olyan beruházáshoz vagy beruházásokhoz odaítélt állami támogatás jelenértéken meghatározott összegét, amely azonos vagy hasonló tevékenységhez kapcsolódik.

(5) Ha az összeszámítási szabály figyelembevétele nélkül az adott beruházáshoz nyújtható állami támogatás jelenértéken kisebb, mint a (4) bekezdés szerint meghatározott támogatási összeg, akkor ez a kisebb összeg az odaítélhető állami támogatás felső korlátja. Ellenkező esetben állami támogatás a (4) bekezdésben meghatározott összegig nyújtható.

17. § (1) A támogatás keretében elszámolható

a) a beruházás érdekében felmerült tárgyi eszközök és immateriális javak költsége,

b) a beruházás által létrehozott munkahelyek két évre számított becsült bérköltsége vagy

c) az a) és b) pontban szereplő költségtípusok kombinációja, ha az így kapott összeg nem haladja meg az a) és b) pont szerinti összeg közül a magasabbat.

(2) Az elszámolható költség az (1) bekezdés a) pontja szerinti esetben a következők szerint határozható meg:

a) a tárgyi eszköznek az Sztv. 47., 48. és 51. §-a szerinti költsége,

b) immateriális javak esetén a vagyoni értékű jogok és a szellemi termékek (a továbbiakban együtt: támogatható immateriális javak) Sztv. 47., 48. és 51. §-a szerinti költsége,

c) létesítmény felvásárlása esetén a tárgyi eszközök és a támogatható immateriális javak vételára,

d) az ingatlan, gép, berendezés bérleti díjának a fenntartási időszak végéig elszámolt összege.

(3) A (2) bekezdés c) pontja szerinti esetben, ha a tárgyi eszköz és az immateriális javak beszerzéséhez a vásárlást megelőzően már nyújtottak támogatást, ezen tárgyi eszköz és immateriális javak költségét le kell vonni a létesítmény felvásárlásához kapcsolódó elszámolható költségekből. Ha egy kisvállalkozást az eredeti tulajdonos családtagjai vagy korábbi munkavállalók vesznek át, a tárgyi eszköznek és az immateriális javaknak a vevőtől független harmadik féltől való megvásárlására vonatkozó feltételnek nem kell teljesülnie.

(4) A tárgyi eszköz bérléséhez kapcsolódó költség elszámolható, ha

a) a földterületre vagy épületre vonatkozó bérleti jogviszony nagyvállalkozás esetén a beruházás üzembe helyezését követő legalább öt évig, kis- és középvállalkozás esetén a beruházás üzembe helyezését követő legalább három évig fennáll, illetve

b) a pénzügyi lízing formájában beszerzett üzemre, gépre, berendezésre vonatkozó szerződés tartalmazza az eszköznek a bérleti időtartam lejáratakor történő megvásárlására vonatkozó kötelezettséget.

(5) Tárgyi eszköz esetén az elszámolható költséget a szokásos piaci áron kell figyelembe venni, ha az a beruházó és a beruházótól nem független harmadik vállalkozás között a szokásos piaci áránál magasabb áron kötött szerződés alapján merült fel.

(6) Az immateriális javak költsége elszámolható, ha
a) azokat kizárólag a támogatásban részesült létesítményben használják fel,
b) az az Sztv. előírásai szerinti terv szerinti értékcsökkenési leírás alá esik,
c) azokat szokásos piaci feltételek mellett, a vevőtől független harmadik féltől vásárolják meg,
d) azok kis- és középvállalkozás esetén legalább három évig a beruházó eszközei között szerepelnek, és ahhoz a projekthez kapcsolódnak, amelyhez a támogatást nyújtották,
e) azok nagyvállalkozás esetén legalább öt évig a beruházó eszközei között szerepelnek, és ahhoz a projekthez kapcsolódnak, amelyhez a támogatást nyújtották,
f) azok költsége nagyvállalkozás esetén az elszámolható költségek legfeljebb 50%-át teszik ki.

(7) Nem minősül elszámolható költségnek
a) a szinten tartást szolgáló tárgyi eszköz és immateriális javak költsége,
b) a kérelem benyújtásának napja előtt felmerült költség, ráfordítás.

(8) Az (1) bekezdés b) pontja szerinti esetben a beruházás üzembe helyezését követő háromszor háromszázhatvanöt napon belül újonnan létrehozott munkahelyeken foglalkoztatott munkavállalók – Sztv. 79. §-a szerint elszámolható – személyi jellegű ráfordításának – ide nem értve az egyéb személyi jellegű kifizetéseket – 24 havi összege számolható el a munkakör betöltésének napjától számítva.

(9) Az (1) bekezdés b) pontja szerinti elszámolható költség esetén akkor nyújtható támogatás, ha
a) a beruházás a kedvezményezettnél foglalkoztatottak számának nettó növekedését eredményezi a beruházás megkezdését megelőző 12 hónap átlagához képest, azt követően, hogy a megszüntetett munkahelyek száma levonásra került a b) pont szerinti időszak alatt létrehozott munkahelyek számából,
b) a munkahelyeket a beruházás befejezésétől számított három éven belül betöltik,
c) kis- és középvállalkozás esetén a beruházó a beruházás megkezdésekor már létező, továbbá a beruházással létrejött új munkahelyeket a munkahely első betöltésétől számított legalább három évig az érintett területen fenntartja,
d) nagyvállalkozás esetén a beruházó a beruházás megkezdésekor már létező, továbbá a beruházással létrejött új munkahelyeket a munkahely első betöltésétől számított legalább öt évig az érintett területen fenntartja.

6. A kis- és középvállalkozásnak nyújtott beruházási támogatás

18. § (1) A kis- és középvállalkozásnak nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) kis- és középvállalkozás induló beruházásához nyújtható.

(2) A támogatási intenzitás nem haladhatja meg kisvállalkozás esetén az elszámolható költségek 20%-át, középvállalkozás esetén az elszámolható költségek 10%-át.

(3) A támogatás keretében
a) a beruházás érdekében felmerült tárgyi eszközök és immateriális javak, beleértve a beruházáshoz és annak üzembe helyezéséhez közvetlenül kapcsolódó egyszeri, nem amortizálható költségeket is,
b) a közvetlenül a beruházási projekt által létrehozott munkahelyek két évre számított, becsült bérköltsége,
c) – ha a kapott összeg nem haladja meg az a) és b) pont szerinti összeg közül a magasabbat, akkor – az a) és b) pontban szereplő költségtípusok kombinációja
számolható el.

(4) A támogatás a 17. § (2)–(5) bekezdése, (6) bekezdés a)–d) pontja, (7)–(8) bekezdése, valamint (9) bekezdés a)–c) pontja szerinti feltételekkel nyújtható.

(5) A (3) bekezdés b) pontja szerinti elszámolható költség esetén akkor nyújtható támogatás, ha a kis- és középvállalkozás a beruházás megkezdésekor már létező, továbbá a beruházással létrejött új munkahelyeket a munkahely első betöltésétől számított legalább három évig fenntartja.

7. A kis- és középvállalkozás vásáron való részvételéhez nyújtott támogatás

19. § (1) A kis- és középvállalkozás vásáron való részvételéhez nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) esetén a támogatási intenzitás nem haladhatja meg az elszámolható költségek 50%-át.

(2) A támogatás keretében a vállalkozásnak valamely kiállításon vagy vásáron való részvételekor felmerülő, a kiállítóhelyiség bérletével, felállításával és működtetésével kapcsolatos költség számolható el.

8. A kis- és középvállalkozás részére tanácsadáshoz nyújtott támogatás

20. § (1) A kis- és középvállalkozás részére tanácsadáshoz nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) esetén a támogatási intenzitás nem haladhatja meg az elszámolható költségek 50%-át.

(2) A támogatás keretében a külső szakértő által nyújtott tanácsadási szolgáltatás költsége számolható el, azzal, hogy az érintett szolgáltatás nem lehet folyamatos vagy időszakosan visszatérő tevékenység és nem kapcsolódhat a vállalkozás szokásos működési költségeihez, különösen folyamatos adótanácsadáshoz, rendszeres jogi szolgáltatáshoz vagy hirdetéshez.

9. Az induló vállalkozásnak nyújtott támogatás

21. § (1) Az induló vállalkozásnak nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) támogatási program keretében azon tőzsdén nem jegyzett kisvállalkozás (ezen alcím alkalmazásában a továbbiakban: kedvezményezett) részére nyújtható, amely

a) legfeljebb öt éve került bejegyzésre,

b) még nem osztott fel nyereséget,

c) nem egy másik vállalkozás tevékenységét vette át, kivéve ha az átvett tevékenység árbevétele a kedvezményezett árbevételének kevesebb mint 10%-át tette ki az átvételt megelőző pénzügyi évben,

d) nem felvásárlás útján jött létre, kivéve, ha a felvásárolt vállalkozás árbevétele a kedvezményezett által a felvásárlást megelőző pénzügyi évben elért árbevételnek kevesebb mint 10%-át teszi ki, és

e) nem összefonódás útján jött létre, kivéve, ha

ea) az összefonódás útján létrejövő vállalkozás árbevétele kevesebb mint 10%-kal magasabb, mint az összefonódó vállalkozások által az összefonódást megelőző pénzügyi évben elért összesített árbevétel, vagy

eb) az összefonódásban részt vevő legrégebbi vállalkozás bejegyzésétől számított öt év még nem telt el.

(2) Azon kedvezményezett esetében, amelyet nem kell bejegyezni, az (1) bekezdés a) pontja és e) pont eb) alpontja szerinti ötéves támogathatósági időszak kezdete az az időpont, amikor a vállalkozás megkezdi gazdasági tevékenységét, vagy amikor gazdasági tevékenysége alapján adóztathatóvá válik, attól függően, hogy melyik a korábbi időpont.

(3) Ezen alcím keretében támogatás pénzügyi közvetítőn keresztül nem nyújtható.

22. § (1) Ha a támogatás formája nem piaci kamatozású, legfeljebb 10 éves futamidőre nyújtott hitel, annak névértéke nem haladhatja meg

a) az 1,1 millió eurót,

b) az Atr. 25. § (1) bekezdése szerinti területen letelepedett vállalkozás esetén a 2,2 millió eurót.

(2) Az 5 és 10 év közötti futamidővel rendelkező hitel nyújtása esetén a névérték legmagasabb összege az (1) bekezdésben meghatározott összeg, valamint a 10 év és a hitel tényleges futamideje hányadosának szorzataként határozható meg. Az 5 évnél rövidebb futamidejű hitel nyújtása esetén a legmagasabb összeg megegyezik az 5 éves futamidejű hitelre vonatkozó legmagasabb összeggel.

23. § (1) Ha a támogatás formája nem piaci díj ellenében, legfeljebb 10 éves futamidőre nyújtott kezességvállalás, a kezességvállalással biztosított hitel névértéke nem haladhatja meg

a) az 1,65 millió eurót,

b) az Atr. 25. § (1) bekezdése szerinti területen letelepedett vállalkozás esetén a 3,3 millió eurót.

(2) Az 5 és 10 év közötti futamidővel rendelkező kezességvállalás nyújtása esetén a kezességvállalással biztosított legmagasabb hitelösszeg az (1) bekezdésben meghatározott összeg, valamint a 10 év és a kezességvállalás tényleges futamideje hányadosának szorzataként határozható meg. Az 5 évnél rövidebb futamidejű kezességvállalás nyújtása esetén a legmagasabb összeg megegyezik az 5 éves futamidejű kezességvállalásra vonatkozó legmagasabb összeggel.

(3) A kezességvállalás nem haladhatja meg az alapul szolgáló hitel összegének 80%-át.

24. § Ha a támogatás formája vissza nem térítendő támogatás – ideértve a sajáttőke-befektetést és a kvázi sajáttőke-befektetést is –, adókedvezmény, adómentesség, kamatlábcsökkentés vagy kezességvállalási díjcsökkentés, annak bruttó támogatási egyenértéke nem haladhatja meg

a) a 0,5 millió eurót,
b) az Atr. 25. § (1) bekezdése szerinti területen letelepedett vállalkozás esetén az 1 millió eurót.

25. § (1) A kedvezményezett támogatásban részesülhet a 22–24. §-ban meghatározott támogatási eszközök kombinációja révén is, ha az egyik támogatási eszközzel nyújtott támogatásnak az adott eszközre vonatkozóan megengedett legmagasabb támogatási összege alapján kiszámított hányadát figyelembe veszik a kombinált eszköz részét képező másik eszközre vonatkozóan megengedett legmagasabb támogatási összeg maradványhányadának meghatározásakor.
(2) Innovatív kisvállalkozás esetén a 22–24. §-ban meghatározott legmagasabb összegek megkétszerezhetőek.

10. Kutatás-fejlesztési projekthez nyújtott támogatás

26. § (1) A kutatás-fejlesztési projekthez nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) a (2) bekezdés szerinti kategóriába tartozó kutatás-fejlesztési projekthez nyújtható.
(2) A kutatás-fejlesztési projekt kategóriái:
a) alapkutatás,
b) ipari kutatás,
c) kísérleti fejlesztés,
d) megvalósíthatósági tanulmány.
(3) Ha egy projekt több tevékenységet foglal magában, az egyes tevékenységeket be kell sorolni a (2) bekezdés szerinti kutatás-fejlesztési kategóriák közé.

27. § (1) Az elszámolható költségeket a kutatás-fejlesztési projekt valamely meghatározott kategóriájához kell rendelni.
(2) A 26. § (2) bekezdés a)–c) pontja esetén a támogatás keretében elszámolható
a) a kutatók, technikusok és egyéb kisegítő személyzet személyi jellegű ráfordítása a projektben való foglalkoztatásuk mértékéig,
b) az eszközök, berendezések költsége a projekt céljaira való használatuk mértékéig és idejére, azzal, hogy ahol ezeket az eszközöket és felszereléseket nem a teljes élettartamuk alatt használják a projekthez, csak az általános számviteli elvek alapján elfogadott, a projekt idejére számított amortizációs költségek számolhatóak el,
c) az épületek és a földterület költsége a projekt céljaira való használatuk mértékéig és idejére, azzal, hogy az épületek esetén csak az általános számviteli elvek alapján elfogadott, a projekt idejére számított amortizációs költségek, földterület esetén a kereskedelmi, illetve a ténylegesen felmerülő beruházási költségek számolhatóak el,
d) a szerződéses kutatás, a külső forrásokból szokásos piaci feltételek mellett megvásárolt vagy licencia tárgyát képező műszaki ismeretek és szabadalmak költsége, valamint a tanácsadás és hasonló szolgáltatások költsége, ha azokat kizárólag a projekthez veszik igénybe,
e) a további általános és egyéb működési költség, beleértve az anyagok, a fogyóeszközök és hasonló termékek költségeit, amelyek közvetlenül a projekt folyamán merülnek fel.
(3) A 26. § (2) bekezdés d) pontja esetén a támogatás keretében a megvalósíthatósági tanulmány költsége számolható el.

28. § (1) A támogatási intenzitás nem haladhatja meg
a) alapkutatás esetén az elszámolható költségek 100%-át,
b) ipari kutatás esetén az elszámolható költségek 50%-át,
c) kísérleti fejlesztés esetén az elszámolható költségek 25%-át,
d) megvalósíthatósági tanulmány esetén az elszámolható költségek 50%-át.
(2) A támogatási intenzitást külön kell megállapítani az egyes kedvezményezettekre, ideértve az (5) bekezdés a) pont ab) alpontja és b) pont bb) alpontja szerinti együttműködési projektben részt vevőket is.
(3) Ipari kutatás, kísérleti fejlesztés és megvalósíthatósági tanulmány esetén az (1) bekezdés szerinti támogatási intenzitás középvállalkozás esetén 10 százalékponttal, kisvállalkozás esetén 20 százalékponttal növelhető.
(4) Ipari kutatás és kísérleti fejlesztés esetén az (1) bekezdés szerinti támogatási intenzitás a (3) bekezdésben foglalt mértéken felül legfeljebb az elszámolható költségek 80%-áig növelhető nagyvállalkozás esetén is oly módon, hogy az (5) bekezdés a) és b) pontja együttesen nem alkalmazható.

(5) Ipari kutatás és kísérleti fejlesztés esetén a támogatási intenzitás

a) 15 százalékponttal növelhető, ha

aa) a projekt az Atr. 25. § (1) bekezdése szerinti területen valósul meg,

ab) a projekt hatékony együttműködést foglal magában, és legalább egy kis- és középvállalkozás bevonásával vagy legalább két tagállamban vagy egy tagállamban és egy, az EGT megállapodás szerinti szerződő fél között zajlik, és egyik vállalkozás sem viseli az elszámolható költségek több mint 70%-át, vagy a projekt legalább egy olyan kutatási és tudásközvetítő szervezet bevonásával zajlik, amely egymagában vagy más hasonló szervezetekkel közösen az elszámolható költségek legalább 10%-át viseli, és jogosult közzétenni saját kutatási eredményeit,

ac) a projekt eredményeit széles körben terjesztik konferenciák, publikációk, nyílt hozzáférésű adattárak, ingyenes vagy nyílt forráskódú szoftverek útján, vagy

ad) a kedvezményezett vállalja, hogy a projekt szellemitulajdon-jogok által védett kutatási eredményeire vonatkozó hasznosítási engedélyeket késedelem nélkül bocsát rendelkezésre piaci áron, megkülönböztetés mentes és nem kizárólagos módon az EGT-n belül érdekelt felek használatára,

b) 25 százalékponttal növelhető, ha

ba) olyan nyílt felhívás alapján került kiválasztásra a projekt, melynek célja, hogy az legalább három tagállam vagy az EGT-megállapodásban szerződő fél közösen tervezett projektjének részét képezze,

bb) a projekt legalább két – nagyvállalkozás esetén három – tagállamban vagy az EGT-megállapodásban szerződő fél területén működő vállalkozások hatékony együttműködését foglalja magában, és

bc) az a) pont ac) vagy ad) alpontja szerinti feltétel teljesül, azzal, hogy az ac) alpont esetén az eredmények széles körű terjesztésének legalább három tagállamban vagy az EGT-megállapodásban szerződő fél területén kell megvalósulnia.

11. Kutatási infrastruktúrához nyújtott beruházási támogatás

29. § (1) A kutatási infrastruktúrához nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) gazdasági tevékenység folytatására használt kutatási infrastruktúra építéséhez és korszerűsítéséhez nyújtható.

(2) A támogatás keretében az immateriális javak és a tárgyi eszköz költsége számolható el.

(3) A támogatási intenzitás nem haladhatja meg az elszámolható költségek 50%-át, amely 60%-ig növelhető, ha a kutatási infrastruktúrát legalább két tagállam finanszírozza, vagy azt uniós szinten minősítik és választják ki.

(4) A kutatási infrastruktúra üzemeltetéséért vagy használatáért a szokásos piaci árat kell fizetni.

(5) A kutatási infrastruktúrának több felhasználó számára hozzáférhetőnek kell lennie, és a hozzáférést átlátható és megkülönböztetésmentes módon kell biztosítani. A kutatási infrastruktúra beruházási költségeit legalább 10%-ban finanszírozó vállalkozás kedvezőbb feltételekkel járó kedvezményes hozzáférési lehetőséget kaphat. A túlkompenzáció elkerülése érdekében a hozzáférési lehetőségnek arányban kell állnia a beruházási költséghez való hozzájárulás mértékével, és a hozzáférés feltételeit közzé kell tenni.

(6) Ha a kutatási infrastruktúra gazdasági és nem gazdasági tevékenységre vonatkozóan egyaránt részesül közfinanszírozásban, az egyes tevékenységekhez kapcsolódó finanszírozást, költségeket és az azokból származó bevételeket külön kell elszámolni, következetesen alkalmazott és objektíven indokolható számviteli elvek alapján.

(7) Ebben az esetben a (3) bekezdés szerinti maximális támogatási intenzitás túllépésének elkerülése érdekében ellenőrzési és visszakövetelési mechanizmust kell alkalmazni arra az esetre vonatkozóan, ha a gazdasági tevékenység részaránya nagyobb, mint az a támogatás odaítélésekor megállapításra került.

12. A kis- és középvállalkozásnak nyújtott innovációs támogatás

30. § (1) A kis- és középvállalkozásnak nyújtott innovációs támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) keretében elszámolható

a) a szabadalmak és egyéb immateriális javak megszerzésének, érvényesítésének és védelmének költsége,

b) olyan, kutatási és tudásközvetítő szervezettől vagy nagyvállalkozástól kirendelt, magasan képzett munkaerő költsége, aki kutatás-fejlesztési és innovációs tevékenységen, a kedvezményezettnél újonnan létrehozott, nem helyettesítő munkakörben dolgozik,

c) innovációs tanácsadás és innovációs támogató szolgáltatás költsége, beleértve a kutató- tudásközvetítő szervezet, kutatási infrastruktúra, tesztelési és kísérleti infrastruktúra vagy innovációs klaszter által nyújtott ezen szolgáltatásokat is.

(2) A támogatási intenzitás nem haladhatja meg az elszámolható költségek 50%-át.

(3) Az (1) bekezdés c) pontja szerinti esetben a támogatási intenzitás az elszámolható költségek 100%-áig növelhető, ha az innovációs tanácsadáshoz és innovációs támogató szolgáltatáshoz nyújtott támogatás összege nem haladja meg három év alatt a 220 000 eurónak megfelelő forintösszeget.

13. Az eljárási innováció és szervezési innováció támogatása

31. § (1) Az eljárási innováció és szervezési innováció támogatása (ezen alcím alkalmazásában a továbbiakban: támogatás) keretében elszámolható

a) a személyi jellegű ráfordítás,

b) a tárgyi eszköz, immateriális javak, berendezés, épület és földterület költsége, a projektben való használatuk mértékéig és idejére,

c) a szerződéses kutatás, a külső forrásból szokásos piaci feltételek mellett megvásárolt vagy licencia tárgyát képező ismeret és szabadalom költsége,

d) a további általános és egyéb működési költség, ideértve az anyagok, a fogyóeszközök és hasonló termékek költségeit, amelyek közvetlenül a projekt eredményeként merülnek fel.

(2) A támogatási intenzitás nagyvállalkozás esetén nem haladhatja meg az elszámolható költségek 15%-át, kis- és középvállalkozás esetén az elszámolható költségek 50%-át.

(3) Nagyvállalkozásnak akkor nyújtható támogatás, ha az a támogatott tevékenység során hatékony együttműködést folytat kis- és középvállalkozással, és ha az együttműködő kis- és középvállalkozás viseli az összes elszámolható költség legalább 30%-át.

14. A képzési támogatás

32. § (1) A képzési támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) esetén a támogatási intenzitás nem haladhatja meg az elszámolható költségek 50%-át.

(2) A támogatási intenzitás

a) megváltozott munkaképességű munkavállaló vagy hátrányos helyzetű munkavállaló részére nyújtott képzés esetén 10 százalékponttal,

b) középvállalkozásnak nyújtott támogatás esetén 10 százalékponttal,

c) kisvállalkozásnak nyújtott támogatás esetén 20 százalékponttal

növelhető.

(3) A támogatási intenzitás legfeljebb az elszámolható költségek 70%-áig növelhető.

(4) A támogatás keretében elszámolható

a) az oktatók személyi jellegű ráfordítása, azokra az órákra vonatkozóan, amikor az oktatók részt vesznek a képzésen,

b) az oktatóknak és a képzés résztvevőinek közvetlenül a képzési projekthez kapcsolódó működési költségei, különösen a közvetlenül a projekthez kapcsolódó útiköltség és szállásköltség, anyagok és fogyóeszközök költsége, valamint az eszközök és berendezések értékcsökkenése kizárólag a képzési projekt céljaira való használatuk mértékéig,

c) a képzési projekthez kapcsolódó tanácsadás költsége és

d) a képzésben részt vevők személyi jellegű ráfordításai és az általános közvetett költségek, mint például adminisztrációs költségek, bérleti díj, rezsiköltségek, azokra az órákra vonatkozóan, amikor a képzésben részt vevők részt vesznek a képzésen.

(5) Nem nyújtható támogatás a kötelező nemzeti képzési előírásoknak való megfeleléshez, valamint támogatott beruházás esetén a beruházás alapvető működtetéséhez szükséges képzéshez.

15. Az épületek energiahatékonyságának kivételével az energiahatékonysági intézkedéshez nyújtott beruházási támogatás

33. § (1) Az épületek energiahatékonyságának kivételével energiahatékonysági intézkedéshez nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) energiamegtakarítást eredményező beruházáshoz nyújtható.

(2) Nem nyújtható támogatás

a) a fosszilis tüzelőanyaggal – ideértve a földgázt is – működő energiatermelő berendezések telepítésére,

b) kapcsolt energiatermelésre, távfűtésre és távhűtésre, valamint

c) a már elfogadott és hatályos uniós szabványnak való megfelelés érdekében megvalósított beruházáshoz.

(3) A már elfogadott, de még nem hatályos uniós szabványoknak való megfelelés érdekében végrehajtott beruházás támogatható, feltéve, hogy a beruházást a szabvány hatálybalépése előtt legalább 18 hónappal végrehajtották.

(4) A támogatás keretében a magasabb energiatakarékossági szint eléréséhez közvetlenül kapcsolódó beruházási többletköltségek számolhatók el. Az elszámolható költségek meghatározásához a beruházási költségeket össze kell vetni egy olyan alternatív forgatókönyv költségeivel, amely támogatás nélkül valósulna meg. Ha ennek eredményeként a támogatás hiányában

a) olyan, kevésbé energiahatékony beruházás valósulna meg, amely az adott ágazat vagy az érintett tevékenység esetében megfelel a szokásos kereskedelmi gyakorlatnak, az elszámolható költségek a támogatott beruházás költségeinek és a kevésbé energiahatékony beruházás költségeinek a különbözete,

b) ugyanazon beruházás későbbi időpontban valósulna meg, az elszámolható költségek a támogatásban részesülő beruházás költségeinek és a későbbi beruházás nettó jelenértéken számított költségeinek különbözete arra az időpontra diszkontálva, amikor a támogatott beruházás megvalósul,

c) a meglévő berendezések és felszerelések további üzemben tartása valósulna meg, az elszámolható költségek a támogatásban részesülő beruházás költségeinek és a meglévő létesítmények és berendezések karbantartására, javítására és korszerűsítésére irányuló beruházások nettó jelenértékének különbözete arra az időpontra diszkontálva, amikor a támogatott beruházás megvalósul,

d) kevésbé energiahatékony eszközök lízingelésére kerülne sor, az elszámolható költségek a támogatásban részesülő és a kevésbé környezetbarát eszközök lízingelésének nettó jelenértékének különbözete.

(5) A (4) bekezdés szerinti esetekben azon alternatív forgatókönyvnek, amely a támogatás hiányában valósulna meg,

a) a támogatott beruházással hasonló termelési kapacitással és élettartammal kell rendelkeznie, és eleget kell tennie az érvényben lévő uniós szabványoknak, és

b) hitelesnek kell lennie a piaci körülmények, az uniós kibocsátás kereskedelmi rendszer által létrehozott ösztönzők és a jogszabályi követelmények tekintetében.

(6) A (4) bekezdés d) pontja szerinti esetben a lízing költségei nem foglalják magukban a felszerelés vagy berendezés üzemeltetésével kapcsolatos költségeket – különösen az üzemanyagköltségeket, biztosítás, karbantartás, egyéb fogyóeszközök költségeit –, függetlenül attól, hogy azok részét képezik-e a lízingszerződésnek.

(7) A (4)–(6) bekezdéstől eltérően a teljes beruházási költség elszámolható, amennyiben a támogatott beruházás egy egyértelműen beazonosítható, kizárólag az energiahatékonyság növelésére irányul, és nincs olyan kevésbé energiahatékony beruházás, amely támogatás hiányában megvalósulna.

(8) A (4) bekezdéstől eltérően az elszámolható költségek alternatív forgatókönyv és a 2. § 121. pontja szerinti versenyeztetéses ajánlattételi eljárás nélkül is meghatározhatóak, amely esetben a magasabb szintű energiahatékonysági eléréséhez közvetlenül kapcsolódó beruházási költségek számolhatók el.

(9) A (4)–(8) bekezdés esetén nem számolhatók el a magasabb szintű energiahatékonyság eléréséhez közvetlenül nem kapcsolódó költségek.

34. § (1) A támogatási intenzitás nem haladhatja meg az elszámolható költségek 30%-át.

(2) Az (1) bekezdés szerinti támogatási intenzitás

a) középvállalkozás esetén 10 százalékponttal, kisvállalkozás esetén 20 százalékponttal és

b) az Atr. 25. § (1) bekezdése szerinti területen megvalósuló beruházás esetén 15 százalékponttal

növelhető.

(3) A támogatás az elszámolható költségek 100%-áig nyújtható, ha a támogatást olyan, a 2. § 121. pontja szerinti versenyeztetéses ajánlattételi eljárásban ítélik oda, amely esetén

a) az eljárást objektív, világos, átlátható és megkülönböztetésmentes, a tényleges verseny lehetővé tétele érdekében előzetesen meghatározott és az ajánlatok benyújtásának határideje előtt legalább 6 héttel közzétett kritériumok alapján dolgozzák ki,

b) a támogatási program végrehajtása során valamennyi ajánlattevő támogatásban részesül, és ezért újabb ajánlattételi eljárás kiírására kerül sor, az eredeti ajánlattételi eljárást a tényleges verseny helyreállítása céljából, az újabb ajánlattételi eljárásban igazítják ki, többek között a költségvetés vagy a mennyiség csökkentésével,

c) tilos bármely ajánlattételi eljárás eredményének utólagos kiigazítása, így különösen az ajánlatok eredményével kapcsolatos utólagos tárgyalás, és

d) az ajánlatok rangsorolásához – és végső soron a támogatásnak a versenyeztetéses ajánlattételi eljárás keretében történő elosztásához – használt összes kiválasztási kritérium legalább 70%-át a projektnek a támogatási intézkedés környezetvédelmi célkitűzéseihez való hozzájárulása – így különösen a megtakarított energia vagy a megnövelt energiahatékonyság egy egysége után igényelt támogatás – alapján határozzák meg.

(4) A 33. § (8) bekezdése szerinti esetben az (1) és (2) bekezdésben meghatározott támogatási intenzitások és bónuszok 50%-kal csökkennek.

16. Épület-energiahatékonysági intézkedéshez nyújtott beruházási támogatás

35. § (1) Az épület-energiahatékonysági intézkedéshez nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) épületek energia-hatékonyságát növelő beruházáshoz, felújításhoz nyújtható, ideértve az épületen belül található fűtő- vagy hűtőberendezések energiahatékonyságának javítását is.

(2) Az (1) bekezdés szerinti beruházáshoz kapcsolódóan támogatás nyújtható

a) a megújuló energiaforrásból villamos energiát, fűtő- vagy hűtőenergiát előállító integrált helyszíni berendezések, különösen napelemek és hőszivattyúk telepítésére,

b) a helyszíni megújulóenergia-létesítmények által termelt energia tárolására szolgáló berendezésekre, amennyiben a tárolást szolgáló berendezés energiájának évi legalább 75%-át a közvetlenül összekapcsolt megújulóenergia-termelő létesítményből nyeri,

c) az energiahatékony távfűtési és távhűtési rendszerhez való csatlakozáshoz, valamint az ehhez kapcsolódó berendezésekhez,

d) az épületet használók számára elektromos töltő- és kapcsolódó infrastruktúra – ideértve a kábelcsatornák – kiépítéséhez és telepítéséhez, abban az esetben is, amennyiben a parkoló az épületen kívül helyezkedik el, de ahhoz fizikailag csatlakozik,

e) az épület digitalizációját, különösen az épület okosfunkció-fogadási alkalmasságának növelését szolgáló berendezések – beleértve adathálózatok esetén az épületen belüli passzív hálózatot és strukturált kábelezést –, továbbá az épülethez tartozó ingatlanon található szélessávú infrastruktúra kiegészítő részeinek telepítéséhez,

f) zöldtetőkbe, valamint az esővíz megtartására és felhasználására szolgáló berendezésekbe történő beruházásokhoz.

(3) Nem nyújtható támogatás

a) a fosszilis tüzelőanyaggal – ideértve a földgázt is – működő energiatermelő berendezések telepítésére,

b) kapcsolt energiatermelésre, távfűtésre és távhűtésre, valamint

c) a már elfogadott és hatályos uniós szabványnak való megfelelés érdekében megvalósított beruházáshoz.

(4) A már elfogadott, de még nem hatályos uniós szabványoknak való megfelelés érdekében végrehajtott beruházás akkor támogatható, amennyiben

a) a vonatkozó uniós szabványok nem energiahatékonysági minimumkövetelmények, a beruházást az uniós szabvány hatálybalépése előtt legalább 18 hónappal végrehajtották,

b) a vonatkozó uniós szabványok energiahatékonysági minimumkövetelmények, a támogatás odaítélésének még azelőtt meg kell történnie, hogy a szabványok kötelezővé válnának az érintett vállalkozásra nézve, azzal, hogy ebben az esetben a kedvezményezett pontos felújítási tervet és ütemtervet nyújt be, melyek igazolják, hogy a támogatott felújítás elegendő legalább ahhoz, hogy biztosítsa az épület energiahatékonysági minimumkövetelményeknek való megfelelését.

(5) A támogatás nyújtásának feltétele, hogy az épület primer energiában mért energiahatékonyságának
a) meglévő épületek felújítása esetén legalább 20%-os javulását eredményezi a beruházást megelőző állapothoz képest,
b) az épületek energiahatékonyságáról szóló, 2010. május 19-i 2010/31/EU európai parlamenti és tanácsi irányelv (a továbbiakban: 2010/31/EU európai parlamenti és tanácsi irányelv) 2. cikk (9) bekezdésében meghatározott egyetlen épületelem-típus telepítését vagy cseréjét érintő felújítás esetén legalább 10%-os javulását eredményezi a beruházást megelőző állapothoz képest,
c) új épületek esetén legalább 10%-os javulását eredményezi a közel nulla energiaigényű épületekre vonatkozóan a 2010/31/EU európai parlamenti és tanácsi irányelvben foglalt küszöbértékhez képest.

(6) Az (5) bekezdés alkalmazásában a kezdeti primerenergia-igényt és annak becsült javulását a 2010/31/EU európai parlamenti és tanácsi irányelv 2. cikk 12. pontjában meghatározott energiahatékonysági tanúsítványra való hivatkozással kell megállapítani.

(7) Az (5) bekezdés b) pontja alapján nyújtott támogatások összege nem haladhatja meg az Atr. 2. § 23. pontja szerinti támogatási program energiahatékonysági intézkedésekre vonatkozó költségvetésének 30%-át.

36. § (1) A támogatás keretében a teljes beruházási költség számolható el, azzal, hogy az épületben megvalósuló magasabb energiahatékonysági szint eléréséhez közvetlenül nem kapcsolódó költségek nem számolhatók el.

(2) A 35. § (2) bekezdése szerinti esetben az ott meghatározott létesítmények és berendezések teljes beruházási költsége számolható el, azzal, hogy a magasabb energiahatékonysági szint vagy környezeti teljesítményszint eléréséhez közvetlenül nem kapcsolódó költségek nem számolhatók el.

37. § (1) A támogatási intenzitás nem haladhatja meg
a) a b) és c) pont kivételével az elszámolható költségek 30%-át,
b) a 35. § (5) bekezdés b) pontja szerinti esetben az elszámolható költségek 25%-át,
c) amennyiben az uniós szabványoknak minősülő energiahatékonysági minimumszabványoknak való megfelelés érdekében végzett beruházásokhoz nyújtott támogatást kevesebb mint 18 hónappal az uniós szabványok hatálybalépése előtt nyújtják
ca) a 35. § (5) bekezdés b) pontja szerinti esetben az elszámolható költségek 15%-át,
cb) a ca) alpontba nem tartozó minden más esetben az elszámolható költségek 20%-át.

(2) Az (1) bekezdés szerinti támogatási intenzitás
a) a 34. § (2) bekezdése szerint és
b) a 35. § (5) bekezdés a) pontja szerinti esetben, ha a támogatás az épület primer energiában mért energiahatékonyságának legalább 40%-os javulását eredményezi, a beruházás előtti helyzethez képest 15 százalékponttal
növelhető.

(3) A (2) bekezdés b) pontja nem alkalmazható abban az esetben, ha a beruházás a megvalósításától számított 18 hónapon belül nem javítja az épület energiahatékonyságát az uniós szabványnak minősülő energiahatékonysági minimumkövetelmények által előírt szint fölé.

17. A megújuló energia-, nagy hatásfokú kapcsolt energia- és megújuló hidrogén termeléshez nyújtott beruházási támogatás

38. § (1) A megújuló energia-, nagy hatásfokú kapcsolt energia- és megújuló hidrogén termeléshez nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) kizárólag új vagy felújított berendezéshez nyújtható.

(2) Nem nyújtható támogatás megújuló hidrogénből előállított villamosenergia-termelésre irányuló beruházáshoz.

(3) A villamosenergia-tárolási projektekhez – ideértve a hőtárolást is – nyújtott beruházási támogatás abban az esetben nyújtható, amennyiben
a) a beruházás megújulóenergia-termelésre és -tárolásra vagy
b) meglévő megújulóenergia-termelő létesítmény esetén kizárólag tárolásra
irányul, és a tárolást szolgáló berendezés energiájának évi legalább 75%-át a közvetlenül összekapcsolt megújulóenergia-termelő létesítményből nyeri.

(4) A bioüzemanyagok, folyékony bio-energiahordozók, biogáz – ideértve a biometánt is – és biomassza előállításához és tárolásához nyújtott beruházási támogatás abban az esetben nyújtható, amennyiben

a) a támogatott üzemanyagok megfelelnek az (EU) 2018/2001 irányelvben és annak végrehajtási vagy felhatalmazáson alapuló jogi aktusaiban foglalt, a fenntarthatóságra és az üvegházhatásúgáz-kibocsátás megtakarítására vonatkozó kritériumoknak, valamint az (EU) 2018/2001 irányelv IX. mellékletében felsorolt alapanyagból készültek, és

b) a tárolást szolgáló berendezés tüzelőanyag-tartalmának évi legalább 75%-át a közvetlenül összekapcsolt, bioüzemanyagot, folyékony bio-energiahordozót, biogázt – ideértve a biometánt – és biomasszából előállított üzemanyagot termelő létesítményből szerzi be.

(5) A (3) bekezdés a) pontja és a (4) bekezdés esetén a termelés, az előállítás és a tárolás a 7. § (5) bekezdés 11. pontja szerinti értékhatár tekintetében egyetlen beruházási projektnek minősül.

(6) A hidrogén előállítására irányuló beruházási támogatás kizárólag megújuló hidrogént előállító létesítményekhez nyújtható, ideértve a megújuló hidrogén átvitelére és elosztására szolgáló infrastruktúrát, valamint a megújuló hidrogént tároló létesítményeket is.

(7) A (6) bekezdés esetén, amennyiben a támogatott projekt elektrolizátorból, egy vagy több megújulóenergia-termelő egységből áll, és egy hálózati csatlakozási ponttal rendelkezik, az elektrolizátor kapacitása nem haladhatja meg a megújulóenergia-termelő egységek együttes kapacitását.

(8) A nagy hatásfokú kapcsolt energiatermelő egységekre irányuló beruházási támogatás abban az esetben nyújtható, amennyiben a 2012/27/EU irányelv, illetve a részben vagy egészben helyébe lépő későbbi jogszabályok rendelkezései szerinti hő- és villamosenergia külön-külön történő termeléséhez képest összességében primerenergia-megtakarítást eredményeznek.

(9) A (8) bekezdés szerinti beruházási támogatás nem nyújtható fosszilis tüzelőanyaggal működő kapcsolt energiatermelő létesítményhez, kivéve az olyan földgázzal működő kapcsolt energiatermelő létesítményt, amely esetében az (EU) 2021/2139 felhatalmazáson alapuló bizottsági rendelet 1. melléklet 4.30. szakaszával összhangban, a 2030-ra és 2050-re vonatkozó éghajlati céloknak való megfelelés biztosított.

(10) Megújuló energiaforrásokon alapuló, nagy hatásfokú kapcsolt energiatermeléshez közvetlenül kapcsolódó villamosenergia- és hőtárolási projektekhez nyújtott beruházási támogatás a (3) bekezdésben foglalt feltételek teljesülése esetén nyújtható.

39. § (1) A támogatás keretében a teljes beruházási költség számolható el, és támogatás nem függhet a termelés eredményétől.

(2) A támogatási intenzitás nem haladhatja meg az elszámolható költségek

a) 45%-át a megújulóenergia-termelésre – ideértve az (EU) 2018/2001 irányelv VII. mellékletének megfelelő hőszivattyúkat –, a megújuló hidrogén és megújuló energiaforrásokon alapuló nagy hatásfokú kapcsolt energiatermelésre irányuló beruházások esetében,

b) 30%-át minden egyéb esetben.

(3) A támogatási intenzitás középvállalkozás esetén 10 százalékponttal, kisvállalkozás esetén 20 százalékponttal növelhető.

(4) A támogatás az elszámolható költségek 100%-áig nyújtható, ha a támogatást olyan, a 2. § 121. pontja szerinti versenyeztetéses ajánlattételi eljárásban ítélik oda, amely esetén

a) az eljárást objektív, világos, átlátható és megkülönböztetésmentes, a tényleges verseny lehetővé tétele érdekében előzetesen meghatározott és az ajánlatok benyújtásának határideje előtt legalább 6 héttel közzétett kritériumok alapján dolgozzák ki,

b) a támogatási program végrehajtása során valamennyi ajánlattevő támogatásban részesül, és újabb ajánlattételi eljárás kiírására kerül sor, az eredeti ajánlattételi eljárást a tényleges verseny helyreállítása céljából az újabb ajánlattételi eljárásban igazítják ki, többek között a költségvetés vagy a mennyiség csökkentésével,

c) tilos bármely ajánlattételi eljárás eredményének utólagos kiigazítása, így különösen az ajánlatok eredményével kapcsolatos utólagos tárgyalás, és

d) az ajánlatok rangsorolásához – és végső soron a támogatásnak a versenyeztetéses ajánlattételi eljárás keretében történő elosztásához – használt összes kiválasztási kritérium legalább 70%-át a megújuló energiaforrásból vagy nagy hatásfokú kapcsolt energiatermeléssel előállított energiakapacitás egy egysége után igényelt támogatás alapján határozzák meg.

18. Az energetikai célú infrastruktúrához nyújtott beruházási támogatás

40. § (1) Az energetikai célú infrastruktúrához nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) energetikai célú infrastruktúra létrehozásához, korszerűsítéséhez és bővítéséhez nyújtható.

(2) Nem nyújtható támogatás

a) a belső energiapiacra vonatkozó jogszabályok szerint harmadik felek hozzáférésére vagy díjakra vonatkozó szabályozás alól részben vagy egészében mentesülő energetikai infrastruktúrához,

b) villamosenergiatároló- és gáztározó-projektekhez kapcsolódó beruházáshoz.

(3) A gázinfrastruktúrára irányuló támogatás abban az esetben nyújtható, amennyiben a támogatás következtében

a) az infrastruktúra kizárólag hidrogén vagy megújuló gázok használatára alkalmas,

b) az infrastruktúra kizárólag hidrogén és megújuló gázok használatára alkalmas, vagy

c) az infrastruktúrát 50%-ot meghaladó mértékben hidrogén és megújuló gázok szállítására használják.

41. § (1) A támogatás keretében a teljes beruházási költség számolható el.

(2) A támogatási intenzitás nem haladhatja meg a 2. § 32. pontja szerinti finanszírozási hiány 100%-át, azzal, hogy a támogatásnak a támogatott projekt megvalósításához minimálisan szükséges összegre kell korlátozódnia.

(3) A (2) bekezdéstől eltérően, amennyiben a támogatás összege versenyeztetéses ajánlattételi eljárás útján kerül meghatározásra, a 2. § 32. pontja szerinti finanszírozási hiány kiszámítása során a nettó többletköltség részletes értékelése nem szükséges.

19. A kultúrát és a kulturális örökség megőrzését előmozdító támogatás

42. § (1) A kultúrát és a kulturális örökség megőrzését előmozdító támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás)

a) beruházási támogatásként, ideértve az infrastruktúra építését, bővítését vagy korszerűsítését,

b) működési támogatásként,

c) zenei és irodalmi alkotások kiadásához nyújtott támogatásként

nyújtható.

(2) A támogatás – a nyomtatott vagy elektronikus formában közzétett sajtótermék és magazin kivételével – a következőkhöz nyújtható:

a) múzeum, levéltár, könyvtár, művészeti és kulturális központ vagy kulturális tér, színház, filmszínház, operaház, koncertterem, egyéb élő előadásokat bemutató szervezet, filmművészeti örökséggel foglalkozó intézmény és egyéb hasonló művészeti és kulturális infrastruktúra, szervezet és intézmény,

b) tárgyi kulturális örökség, régészeti lelőhely, emlékmű, történelmi emlékhely és épület, a kulturális örökséghez kapcsolódó természeti örökség, kulturális vagy természeti örökséggé nyilvánított örökség,

c) a szellemi kulturális örökség valamennyi formája, különösen a népi hagyományok, kézművesség,

d) művészeti vagy kulturális esemény, előadás, fesztivál, kiállítás és hasonló kulturális tevékenység,

e) kulturális és művészeti oktatási tevékenység, a kulturális kifejezésmódok sokfélesége védelmének és támogatásának jelentőségét tudatosító, oktatási és társadalmi célú figyelemfelhívó programok, ideértve az új technológiák alkalmazását is ezen célokra,

f) zenei és irodalmi alkotások írása, szerkesztése, gyártása, terjesztése, digitalizálása, kiadása és fordítása.

43. § (1) Beruházási támogatás keretében a tárgyi eszközök és az immateriális javak következő költségei számolhatók el:

a) az infrastruktúra építésének, korszerűsítésének, bővítésének, megvásárlásának, megőrzésének és fejlesztésének költsége, ha az infrastruktúra időbeli vagy térbeli kapacitását évente legalább 80%-ban kulturális célra használják,

b) a kulturális örökség megszerzésének költsége, ideértve a kulturális örökség bérletének, birtokátruházásának és a kulturális örökség áthelyezésének költségeit is,

c) a tárgyi és szellemi kulturális örökség védelmének, megőrzésének, újjáépítésének és helyreállításának költsége, különösen a megfelelő körülmények között történő tárolás költsége, a speciális eszközök, anyagok használatából fakadó többletköltség, valamint a dokumentációs, kutatási, digitalizálási és publikációs költség,

d) a közönség kulturális örökséghez való hozzáférésének javítását szolgáló intézkedések költsége, különösen a digitalizálással és más új technológiákkal, a speciális szükségletű személyek hozzáférési lehetőségeinek

javításával kapcsolatos, valamint a prezentációk, programok és látogatók tekintetében a kulturális sokszínűség elősegítésével kapcsolatos költség,

e) a kulturális projektek és tevékenységek, együttműködési és csereprogramok, valamint ösztöndíjak költsége, ideértve a kiválasztási eljárás, a marketing és a projekt eredményeként közvetlenül felmerülő költségeket is.

(2) Beruházási támogatás esetén a támogatás összege nem haladhatja meg az elszámolható költség és a beruházás megvalósításából származó működési eredmény különbségét, azzal, hogy az infrastruktúra üzemeltetője – a támogatást nyújtó döntésétől függően – jogosult észszerű nyereséget szerezni.

(3) A működési eredmény mértékét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell levonni az elszámolható költségekből.

44. § (1) Működési támogatás keretében elszámolható

a) a kulturális intézmény vagy örökségi helyszín állandó vagy időszakos tevékenységéhez – különösen kiállításokhoz, előadásokhoz, rendezvényekhez és hasonló kulturális tevékenységekhez – kapcsolódó, a szokásos üzletmenetben felmerülő költség,

b) a kulturális és művészeti oktatási tevékenység költsége és a kulturális kifejezésmódok sokfélesége védelmének és előmozdításának fontosságát tudatosító oktatási és társadalmi célú figyelemfelhívó programok népszerűsítésének költsége – ideértve az új technológiák ezen célokra történő alkalmazásának költségét is –,

c) a közönség kulturális intézményhez vagy örökségi helyszínhez és tevékenységhez való hozzáférésének javítását szolgáló költség – ideértve a digitalizálással, egyéb új technológiákkal és a fogyatékkal élő személyek hozzáférési lehetőségeinek javításával kapcsolatos költséget is –,

d) közvetlenül a kulturális projekthez vagy tevékenységhez kapcsolódó működési költség, különösen

da) az ingatlanok és kulturális helyszínek bérletének, lízingjének költsége,

db) a kulturális projektekhez vagy tevékenységekhez közvetlenül kapcsolódó utazási, anyag- és felszerelési költség,

dc) a kiállítások és díszletek építészeti elemeinek költsége,

dd) az eszközökhöz, szoftverekhez és felszerelésekhez igénybe vett hitel vagy lízing költsége,

de) az eszközök, szoftverek, felszerelések amortizációja és a finanszírozási költség, ha e költségeket nem fedezte beruházási támogatás,

df) szerzői jogi védelem alatt álló alkotásokhoz és egyéb kapcsolódó szellemi tulajdonjogi védelem alatt álló tartalmakhoz való hozzáférésre vonatkozó jogokkal kapcsolatos költség,

dg) a marketing költsége,

dh) a projekt vagy tevékenység eredményeként közvetlenül felmerült költség,

e) a kulturális intézmény, örökségi helyszín vagy projekt személyi jellegű ráfordítása,

f) a külső tanácsadással és külső szolgáltatók által biztosított támogató szolgáltatásokkal kapcsolatos, közvetlenül a projekt eredményeként felmerülő költség.

(2) Működési támogatás esetén a támogatás összege nem haladhatja meg a támogatással érintett időszakban keletkező működési veszteséget, ideértve az észszerű nyereséget is.

(3) A működésből származó veszteség és az észszerű nyereség összegét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell meghatározni.

45. § A 2,2 millió eurónak megfelelő forintösszeget meg nem haladó beruházási vagy működési támogatás esetén a támogatás összege a 43. § (2) és (3) bekezdésében, valamint a 44. § (2) és (3) bekezdésében meghatározott módszerek alkalmazásától eltérően is meghatározható, azzal, hogy a támogatási intenzitás nem haladhatja meg az elszámolható költségek 80%-át.

46. § (1) A 42. § (2) bekezdés f) pontja szerinti támogatás esetén
a) a támogatási intenzitás nem haladhatja meg az elszámolható költségek 70%-át, vagy
b) a támogatás összege nem haladhatja meg az elszámolható költségek és a projektből származó bevételek jelenértékének különbségét, azzal, hogy a bevételeket az elszámolható költségekből előzetesen vagy visszakövetelési mechanizmus alkalmazásával kell levonni.

(2) A 42. § (2) bekezdés f) pontja szerinti támogatás keretében a zenei és irodalmi kiadói költségek számolhatók el, különösen
a) a szerző díjazása, ideértve a szerzői joggal kapcsolatos költséget is,
b) a fordító díjazása,
c) a szerkesztő díjazása,
d) az egyéb szerkesztési költség, ideértve a korrektúrázás, javítás, lektorálás költségét is,
e) az elrendezés és nyomdai előkészítés költsége és
f) a nyomtatás vagy elektronikus közzététel költsége.

20. A sportlétesítményhez és multifunkcionális szabadidős létesítményhez nyújtott támogatás

47. § (1) A sportlétesítményhez és multifunkcionális szabadidős létesítményhez nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás)
a) beruházási támogatásként sportlétesítmény és multifunkcionális szabadidős létesítmény építéséhez, bővítéséhez vagy korszerűsítéséhez,
b) működési támogatásként sportlétesítmény működéséhez
nyújtható.

(2) A multifunkcionális szabadidős létesítmény többfunkciós, a sportfunkció mellett egyéb, különösen kulturális és szabadidős szolgáltatásokat nyújtó szabadidős létesítmény, a szabadidőparkok és a szállodai létesítmények kivételével.

(3) A támogatott sportlétesítmény és multifunkcionális szabadidős létesítmény építésével, bővítésével, korszerűsítésével, működtetésével, üzemeltetésével történő megbízás odaítélése során átlátható és megkülönböztetésmentes módon, a vonatkozó közbeszerzési jogszabályok betartásával kell eljárni.

(4) A támogatott sportlétesítményhez és multifunkcionális szabadidős létesítményhez a felhasználók számára átlátható és megkülönböztetésmentes módon kell hozzáférést biztosítani. A beruházási költséget legalább 30%-ban finanszírozó vállalkozás a támogatott létesítményt kedvezőbb feltételek mellett használhatja, ha e feltételeket nyilvánossá teszik.

(5) A támogatott sportlétesítmény nem állhat egyetlen hivatásos sportoló vagy hivatásos csapat kizárólagos használatában. A sportlétesítményt az éves időbeli kapacitás legalább 20%-ában más hivatásos vagy amatőr sportolónak vagy csapatnak kell használnia. Amennyiben a sportlétesítményt egyidejűleg több használó veszi igénybe, az időbelikapacitás-kihasználás megfelelő hányadát kell figyelembe venni.

(6) Ha a támogatott sportlétesítményt hivatásos csapatok használják, az esetükben alkalmazott díjszámítási feltételeket nyilvánossá kell tenni.

48. § (1) A beruházási támogatás keretében a tárgyi eszközök és az immateriális javak beruházási költsége számolható el.

(2) Beruházási támogatás esetén a támogatás összege nem haladhatja meg az elszámolható költségek és a működési eredmény közötti különbséget.

(3) A működési eredmény mértékét
a) előzetesen, megalapozott előrejelzések alapján vagy
b) visszafizetési mechanizmus alkalmazásával utólag
kell levonni az elszámolható költségekből.

49. § (1) A működési támogatás keretében a sportlétesítmény által nyújtott szolgáltatásokkal kapcsolatban felmerülő működési költség – ideértve az igénybe vett szolgáltatások és a karbantartás költségét, a bérleti díjat, a személyi, az anyag-, a kommunikációs, az energia- és az adminisztrációs költségeket is – számolható el.

(2) Működési támogatás esetén az értékcsökkenés és a finanszírozási költségek olyan mértékben nem számolhatóak el, amilyen mértékben az értékcsökkenéssel vagy finanszírozással érintett tárgyi eszközök, immateriális javak tekintetében a kedvezményezett beruházási támogatásban részesült.

(3) Működési támogatás esetén a támogatás nem haladhatja meg a támogatással érintett időszakban keletkező működési veszteséget.

(4) A működésből származó veszteség összegét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell meghatározni.

50. § A 2,2 millió eurónak megfelelő forintösszeget meg nem haladó támogatás esetén a támogatás összege a 48. § (2) és (3) bekezdésében és a 49. § (3) és (4) bekezdésében meghatározott módszerek alkalmazásától eltérően is meghatározható, azzal, hogy a támogatási intenzitás nem haladja meg az elszámolható költségek 80%-át.

21. Helyi infrastruktúrára irányuló támogatás

51. § (1) Helyi infrastruktúrára irányuló támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) helyi infrastruktúra építéséhez, bővítéséhez vagy korszerűsítéséhez nyújtható, ha ezen infrastruktúra helyi szinten hozzájárul az üzleti és a fogyasztói környezet korszerűsítéséhez és ipari bázisok fejlesztéséhez.

(2) A támogatás olyan infrastruktúra-fejlesztésre nyújtható, amelyre – a regionális beruházási támogatás kivételével – nem nyújtható támogatás a 651/2014/EU bizottsági rendelet egyéb cikke alapján. Nem nyújtható támogatás dedikált infrastruktúra fejlesztéséhez.

(3) A támogatás nyújtásának feltétele, hogy a megvalósuló infrastruktúrát nyílt, átlátható és megkülönböztetésmentes alapon kell a felhasználók rendelkezésére bocsátani. Az infrastruktúra használata vagy eladása során a szokásos piaci árat kell fizetni.

(4) Az infrastruktúra működtetését koncesszióba adni, vagy azzal harmadik felet megbízni csak nyílt, átlátható és megkülönböztetésmentes módon, a vonatkozó közbeszerzési jogszabályok betartásával lehet.

52. § (1) A támogatás keretében a beruházáshoz kapcsolódó tárgyi eszközök és immateriális javak beruházási költsége számolható el.

(2) A támogatás összege nem haladhatja meg az elszámolható költségek és a működési eredmény közötti különbséget.

(3) A működési eredmény mértékét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell levonni az elszámolható költségekből.

22. A csekély összegű támogatás

53. § (1) A kedvezményezett és a vele egy és ugyanazon vállalkozásnak minősülő vállalkozások részére az (EU) 2023/2831 bizottsági rendelet hatálya alá tartozó, bármely három év során Magyarországon odaítélt csekély összegű támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) bruttó támogatástartalma nem haladhatja meg a 300 000 eurónak megfelelő forintösszeget, figyelembe véve az (EU) 2023/2831 bizottsági rendelet 3. cikk (8) és (9) bekezdését.

(2) A kedvezményezettnek az (EU) 2023/2831 bizottsági rendelet 7. cikk (4) bekezdése figyelembevételével – az ott meghatározott feltételek teljesítésének megállapítására alkalmas módon – nyilatkoznia kell a részére a támogatás odaítélését megelőző három év (háromszor háromszázhatvanöt nap) során nyújtott csekély összegű támogatások támogatástartalmáról.

(3) A támogatást nyújtó a kedvezményezett részére az (EU) 2023/2831 bizottsági rendelet 7. cikk (4) bekezdésével összhangban igazolást állít ki a támogatás összegéről, bruttó támogatási egyenértékben kifejezve, és annak csekély összegű jellegéről, közvetlenül utalva az (EU) 2023/2831 bizottsági rendeletre.

(4) Hitel vagy kezességvállalás formájában nyújtott támogatás esetén – az (EU) 2023/2831 bizottsági rendelet 4. cikk (6) bekezdés a) pontja szerinti esetben – nem lehet kedvezményezett az a vállalkozás, amelyet kollektív fizetésképtelenségi eljárás alá vontak, vagy hitelezői kérelemre kollektív fizetésképtelenségi eljárás alá lenne vonható, valamint az a nagyvállalkozás, amely B hitelminősítésnek megfelelő helyzetnél rosszabb helyzetben van.

(5) A támogatás más csekély összegű támogatásokról szóló rendeleteknek megfelelően nyújtott csekély összegű támogatással a vonatkozó bizottsági rendeletekben foglalt felső támogatási határok közül a legmagasabb felső határig halmozható.

(6) A támogatás halmozható azonos elszámolható költségek vagy azonos kockázatfinanszírozási célú intézkedés vonatkozásában nyújtott állami támogatással, ha a halmozás következtében az odaítélt támogatások nem lépik túl a csoportmentességi rendeletekben vagy az Európai Bizottság jóváhagyó határozatában meghatározott legmagasabb támogatási intenzitást vagy összeget.

23. A mezőgazdasági csekély összegű támogatás

54. § (1) A kedvezményezett és a vele egy és ugyanazon vállalkozásnak minősülő vállalkozások részére az 1408/2013/EU bizottsági rendelet hatálya alá tartozó, Magyarországon odaítélt csekély összegű támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) bruttó támogatástartalma nem haladhatja meg a 25 000 eurónak megfelelő forintösszeget, figyelembe véve az 1408/2013/EU bizottsági rendelet 3. cikk (3a) bekezdés a) és b) pontját, (8) és (9) bekezdését, valamint 5. cikkét.

(2) A támogatás odaítélése során az adott pénzügyi évben, valamint az előző két pénzügyi év alatt odaítélt csekély összegű támogatások bruttó támogatástartalmának összegét kell figyelembe venni.

(3) Az 1408/2013/EU bizottsági rendelet 1. cikk (2) és (3) bekezdésében foglaltak kivételével nem lehet kedvezményezett az a vállalkozás, amely az igényelt támogatást az 1408/2013/EU bizottsági rendelet 1. cikk (1) bekezdésében meghatározott kivételek szerint használná fel.

(4) Hitel vagy kezességvállalás formájában nyújtott támogatás esetén – az 1408/2013/EU bizottsági rendelet 4. cikk (3) bekezdés a) pontja szerinti esetben – nem lehet kedvezményezett az a vállalkozás, amelyet kollektív fizetésképtelenségi eljárás alá vontak, vagy hitelezői kérelemre kollektív fizetésképtelenségi eljárás alá lenne vonható, valamint az a nagyvállalkozás, amely B hitelminősítésnek megfelelő helyzetnél rosszabb helyzetben van.

(5) A támogatás más csekély összegű támogatásról szóló rendeletnek megfelelően nyújtott csekély összegű támogatással az adott csekély összegű támogatásról szóló rendeletben meghatározott felső határig halmozható.

(6) A támogatás halmozható azonos elszámolható költségek vagy azonos kockázatfinanszírozási célú intézkedés vonatkozásában nyújtott állami támogatással, ha a halmozás következtében az odaítélt támogatások nem lépik túl a csoportmentességi rendeletekben vagy az Európai Bizottság jóváhagyó határozatában meghatározott legmagasabb támogatási intenzitást vagy összeget.

(7) A kedvezményezettnek az 1408/2013/EU bizottsági rendelet 5. cikk (1) és (2) bekezdése figyelembevételével – az ott meghatározott feltételek teljesítésének megállapítására alkalmas módon – nyilatkoznia kell a részére a támogatás odaítélésének évében és az azt megelőző két pénzügyi évben nyújtott csekély összegű támogatások támogatástartalmáról, kivéve az Agrár Széchenyi Kártya Konstrukció kedvezményezettjei esetében.

(8) A támogatást nyújtó az 1408/2013/EU bizottsági rendelet 5. cikk (1) bekezdésében meghatározott feltételek teljesülését a Magyar Államkincstár által, a mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 26. § (1) bekezdés f) pontja alapján vezetett támogatások nyilvántartása alapján ellenőrzi az Atr.-ben szabályozottaknak megfelelően.

24. A halászati és akvakultúra ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról

55. § (1) A kedvezményezett és a vele egy és ugyanazon halászati és akvakultúra-ágazati vállalkozásnak minősülő vállalkozások részére a 717/2014/EU bizottsági rendelet hatálya alá tartozó, Magyarországon odaítélt csekély összegű támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) bruttó támogatástartalma nem haladhatja meg a 30 000 eurónak megfelelő forintösszeget, figyelembe véve a 717/2014/EU bizottsági rendelet 3. cikk (8) és (9) bekezdésében foglaltakat.

(2) A támogatás odaítélése során az adott pénzügyi évben, valamint az előző két pénzügyi év alatt odaítélt csekély összegű támogatások bruttó támogatástartalmának összegét kell figyelembe venni.

(3) A halászati és akvakultúra termékek elsődleges előállításával foglalkozó vállalkozásoknak bármely, három pénzügyi évet felölelő időszakban nyújtott csekély összegű támogatások halmozott összege Magyarországon nem haladhatja meg a 846 353 eurónak megfelelő forintösszeget.

(4) Nem lehet kedvezményezett az a vállalkozás, amely az igényelt támogatást a 717/2014/EU bizottsági rendelet 1. cikk (1) bekezdésében meghatározott kivételek szerint használná fel.

(5) A támogatás más csekély összegű támogatásokról szóló rendeleteknek megfelelően nyújtott csekély összegű támogatással a vonatkozó bizottsági rendeletekben foglalt felső támogatási határok közül a legmagasabb felső határig halmozható.

(6) A halászati csekély összegű támogatás halmozható azonos elszámolható költségek vonatkozásában vagy azonos kockázatfinanszírozási célú intézkedés vonatkozásában nyújtott állami támogatással, ha a halmozás következtében az odaítélt támogatások nem lépik túl bármely csoportmentességi rendeletben vagy az Európai Bizottság által elfogadott határozatban meghatározott maximális intenzitást vagy összeget.

(7) A támogatást nyújtó az 1408/2013/EU bizottsági rendelet 5. cikk (1) bekezdésében meghatározott feltételek teljesülését a Magyar Államkincstár által, a mezőgazdasági, agrár-vidékfejlesztési, valamint halászati támogatásokhoz és egyéb intézkedésekhez kapcsolódó eljárás egyes kérdéseiről szóló 2007. évi XVII. törvény 26. § (1) bekezdés f) pontja alapján vezetett támogatások nyilvántartása alapján ellenőrzi az Atr.-ben szabályozottaknak megfelelően.

25. A mezőgazdasági üzemekben végrehajtott, elsődleges mezőgazdasági termelésre irányuló beruházásokhoz nyújtott támogatás

56. § (1) A mezőgazdasági üzemekben végrehajtott, elsődleges mezőgazdasági termeléshez nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) esetén a beruházásnak az alábbi célkitűzések egyikéhez kell kapcsolódnia:

a) a mezőgazdasági üzem összteljesítményének és fenntarthatóságának javítása, különösen a termelési költségek csökkentése, illetve a termelés javítása és átcsoportosítása révén,

b) a természeti környezet minőségének, a higiéniai körülményeknek vagy az állatjólét színvonalának javítása,

c) a mezőgazdaság fejlesztéséhez, átalakításához és korszerűsítéséhez kapcsolódó infrastruktúra kiépítése és fejlesztése, ideértve a mezőgazdasági földterületekhez való hozzáférést, a birtokrendezést és a termőföld minőségének javítását, az energiahatékonyságot, a fenntartható energiaellátást, valamint a víz- és energiatakarékosságot is,

d) a természeti katasztrófák, természeti katasztrófához hasonlítható kedvezőtlen éghajlati jelenségek, állatbetegségek és növénykárosítók, védett állatok által károsított termelési potenciál helyreállítása és ezen események és tényezők általi károkozás megelőzése,

e) az éghajlatváltozás mérsékléséhez és az éghajlatváltozáshoz való alkalmazkodás, különösen az üvegházhatásúgáz-kibocsátás csökkentése és a szénmegkötés fokozása, valamint a fenntartható energia használatának és az energiahatékonyságnak az előmozdítása,

f) a fenntartható körforgásos biogazdasághoz való hozzájárulás, valamint a fenntartható fejlődés és az olyan természeti erőforrásokkal – különösen a vízzel, termőfölddel és levegővel – való hatékony gazdálkodás támogatása, ideértve a vegyi anyagoktól való függés csökkentését is,

g) hozzájárulás a biológiai sokféleség csökkenésének megállításához és visszafordításához, az ökoszisztéma-szolgáltatások gyarapításához, valamint az élőhelyek és a tájak megőrzéséhez.

(2) Az (1) bekezdés d) pontja szerinti esetben, amennyiben a kár összefüggésbe hozható az éghajlatváltozással, a beruházás magában foglalhatja az éghajlatváltozáshoz való alkalmazkodást célzó helyreállítási intézkedéseket is.

(3) A támogatás feltétele, hogy

a) a beruházást elsődleges mezőgazdasági termeléssel foglalkozó egy vagy több kis- és középvállalkozás valósítsa meg, vagy

b) a beruházás olyan tárgyi eszközt, illetve olyan immateriális javat érint, amelyet elsődleges mezőgazdasági termeléssel foglalkozó kis- és középvállalkozás használ.

(4) Amennyiben környezeti hatásvizsgálati és az egységes környezethasználati engedélyezési eljárásról szóló 314/2005. (XII. 25.) Korm. rendelet [a továbbiakban: 314/2005. (XII. 25.) Korm. rendelet] értelmében környezeti hatásvizsgálat szükséges, az arra irányuló eljárást a támogatás odaítéléséről szóló döntés időpontját megelőzően szükséges lefolytatni.

(5) A visszanyert víz alternatív vízellátásként történő felhasználására irányuló beruházásokhoz kizárólag akkor nyújtható támogatás, ha az ilyen víz rendelkezésre bocsátása és felhasználása megfelel az (EU) 2020/741 európai parlamenti és tanácsi rendeletnek.

(6) Amennyiben a támogatás öntözésre irányul, támogatás akkor nyújtható, ha a beruházás helye szerinti vízgyűjtő kerület tekintetében biztosított, hogy a mezőgazdasági ágazat általi különböző vízhasználatok a 2000/60/EK irányelv 9. cikke (1) bekezdése második albekezdésének első franciabekezdésével összhangban hozzájáruljanak a vízszolgáltatások költségeinek megtérüléséhez, szükség esetén figyelembe véve a költségek megtérítésének szociális, környezeti és gazdasági hatásait, továbbá az érintett régió vagy régiók földrajzi és éghajlati jellemzőit is.

(7) Nem nyújtható támogatás
a) támogatási jogosultság vásárlásához,
b) egynyári növény vásárlásához és telepítéséhez, ide nem értve az 58. § (1) bekezdés h) pontja szerinti elszámolható költségeket,
c) vízelvezetési munkálatokhoz,
d) adathálózatok ingatlanon kívüli vezetékezéséhez vagy kábelezéséhez,
e) állatok vásárlásához, ide nem értve az őrkutyavásárlást és az 58. § (1) bekezdés h) pontja szerinti elszámolható költségeket,
f) az 1308/2013/EU európai parlamenti és tanácsi rendeletben megállapított valamely tiltás vagy korlátozás megszegésével, ideértve azokat a tiltásokat és korlátozásokat, amelyek kizárólag az 1308/2013/EU európai parlamenti és tanácsi rendelet szerinti támogatásokra vonatkoznak.

57. § (1) Amennyiben a támogatás a bioüzemanyag vagy a megújuló energiaforrásból származó energia mezőgazdasági üzemen belül történő előállításához kapcsolódó beruházásra irányul, az előállított üzemanyag- vagy energiamennyiség nem lépheti túl a mezőgazdasági üzem átlagos éves üzemanyag- vagy energiafogyasztását.
(2) Amennyiben a támogatás a bioüzemanyag előállításához kapcsolódó beruházásra irányul,
a) az üzemanyag-termelő létesítmény termelési kapacitása nem haladja meg a mezőgazdasági üzem átlagos éves üzemanyag-fogyasztását, és
b) az előállított bioüzemanyag nem értékesíthető a piacon.
(3) Amennyiben a támogatás megújuló energiaforrásból származó hőenergia és villamos energia mezőgazdasági üzemen belül történő előállításához kapcsolódó beruházásra irányul,
a) az energiatermelő létesítmény csak a kedvezményezett saját energiaszükségletének fedezésére szolgálhat, és termelési kapacitása nem haladja meg a mezőgazdasági üzem és az ahhoz kapcsolódó mezőgazdasági háztartás átlagos éves kombinált hőenergia- és villamosenergia-fogyasztását,
b) az előállított villamos energia hálózatba történő eladása az a) pontban meghatározott termelési korlát betartásával történhet.
(4) Az (1)–(3) bekezdésben foglalt esetekben, amennyiben a beruházást saját bioüzemanyag- és energiaszükségletük fedezése céljából több kedvezményezett valósítja meg, az átlagos éves fogyasztást valamennyi kedvezményezett átlagos éves fogyasztásának összegeként kell meghatározni.
(5) Amennyiben a beruházás energiát fogyasztó vagy termelő, valamely megújuló energiához kapcsolódó infrastruktúrára irányul, meg kell felelnie az irányadó hazai energiahatékonysági szabványoknak.
(6) Amennyiben a támogatás elsődlegesen biomasszaalapú villamosenergia-termeléshez kapcsolódó beruházásra irányul, az csak akkor nyújtható, ha a támogatott létesítmény az irányadó hazai előírás szerinti arányban hőenergiát is hasznosít.
(7) Az (1), (2) és (6) bekezdés szerinti esetekben támogatás akkor nyújtható, ha a bioenergiát előállító létesítmény megfelel az (EU) 2018/2001 irányelv 26. cikke szerinti követelményeknek a bioenergia-termeléshez – beleértve a bioüzemanyagok előállítását is – a felhasznált gabonafélék és más, keményítőben gazdag termények, valamint cukor- és olajnövények maximális arányára vonatkozóan.

58. § (1) A támogatás keretében elszámolható
a) az ingatlanszerzés költsége, ideértve a lízinget is,
b) az ingatlan építésével és korszerűsítésével kapcsolatos költségek, ideértve az adathálózatok passzív, ingatlanon belüli vezetékezése vagy strukturált kábelezése, és adott esetben a passzív hálózatnak az ingatlanon belül elhelyezkedő, épületen kívüli kiegészítő részére fordított beruházások kapcsán felmerülő költségeket is,
c) a gépek és berendezések vásárlásának és lízingelésének költsége az eszköz piaci értékéig,
d) az a)–c) pont szerinti költségekhez kapcsolódó általános költségek, különösen építészek, mérnökök díjai, tanácsadási díjak, a környezeti és a gazdasági fenntarthatóságra, a fenntartható energiára, energiahatékonyságra, a megújuló energia előállítására és használatára vonatkozó tanácsadással kapcsolatos díjak, ideértve a megvalósíthatósági tanulmányok költségeit akkor is, ha a tanulmányok eredményei alapján nem merülnek fel az a)–c) pont szerinti költségek,
e) a számítógépes szoftver, felhőalapú és hasonló megoldások vásárlásának, fejlesztésének és használatának díja, valamint szabadalom, licencia, szerzői jog és védjegy megszerzésének költsége,
f) az 56. § (1) bekezdés e)–g) pontja szerinti célkitűzésekhez kapcsolódó nem termelő beruházások költsége,

g) az öntözéshez kapcsolódó beruházás költsége, amennyiben az (5) bekezdésben meghatározott feltételek teljesülnek,

h) az 56. § (1) bekezdés d) pontjához kapcsolódó beruházás esetén az a költség, amely a mezőgazdasági termelésipotenciál-károsító események bekövetkezése előtti szintre történő helyreállítása kapcsán merül fel, illetve az okozott károk megelőzésére irányuló intézkedések költségei.

(2) A támogatás keretében a működőtőke költsége nem számolható el.

(3) Az (1) bekezdés a) és b) pontja esetén a telekvásárlás költsége csak az adott művelethez kapcsolódó teljes elszámolható költségek 10%-áig számolható el.

(4) A lízingszerződésekkel kapcsolatos, az (1) bekezdés a)–c) pontjában meghatározott költségeken túl egyéb költségek – ideértve a lízingbe adó árrését, a kamatok refinanszírozási költségeit, a közvetett költségeket és a biztosítási díjakat – nem számolhatók el.

(5) Az (1) bekezdés g) pontjában meghatározott költség akkor számolható el, ha

a) a 2000/60/EK európai parlamenti és tanácsi irányelvnek megfelelő vízgyűjtő-gazdálkodási terv került benyújtásra a Bizottságnak a beruházás helyszínéül szolgáló teljes területre, valamint minden más olyan területre vonatkozóan, ahol a beruházás hatással lehet a környezetre és a 2000/60/EK európai parlamenti és tanácsi irányelv 11. cikke szerinti intézkedési program részletesen ismerteti a vízgyűjtő-gazdálkodási tervben szereplő, a mezőgazdasági ágazat szempontjából releváns intézkedéseket,

b) rendelkezésre áll egy olyan vízfogyasztásmérő, amely a támogatott beruházás vonatkozásában lehetővé teszi a vízfogyasztás mérését, vagy a vízfogyasztásmérő a beruházás részeként kerül kiépítésre,

c) meglévő öntözőberendezések vagy az öntözési infrastruktúra elemeinek fejlesztésére irányuló beruházás esetében előzetes értékelés elvégzésére kerül sor annak biztosítására, hogy a vízmegtakarítás tükrözze a meglévő létesítmény vagy infrastruktúra műszaki paramétereit,

d) a beruházás olyan, talajvízből vagy felszíni vizekből álló víztesteket érint, amelyek a vonatkozó vízgyűjtő-gazdálkodási tervben vízmennyiséggel kapcsolatos okok miatt jónál rosszabb minősítést kaptak, vagy ha az éghajlatváltozással szembeni sérülékenységgel kapcsolatos legújabb értékelésekben és kockázatértékelésekben megállapítást nyert, hogy a jó minősítést kapott érintett víztestek elveszíthetik minősítésüket az éghajlatváltozás hatásaira visszavezethető, vízmennyiséggel kapcsolatos okok miatt, akkor a vízfogyasztás tényleges csökkentését kell elérni, amely hozzájárul az említett víztestek jó állapotának eléréséhez a 2000/60/EK irányelv 4. cikk (1) bekezdése szerint,

e) a támogatást nyújtó támogathatósági feltételként százalékos arányokat határoz meg a potenciális vízmegtakarításra és a tényleges vízhasználat-csökkentésre vonatkozóan annak biztosítása érdekében, hogy a berendezéseken keresztül áramló víz mennyisége ténylegesen csökkenjen a 2014–2020-as szintekhez képest, és ezáltal elkerülhető legyen a környezetvédelmi törekvések szintjének mérséklődése.

(6) Az (5) bekezdés d) pontjában meghatározott feltételek nem alkalmazandók

a) meglévő öntözőberendezések esetén a kizárólag az energiahatékonyságot célzó beruházásokra,

b) a tározók létrehozására vagy az újrahasznosított víz használatára irányuló olyan beruházásokra, amelyek nem érintenek felszín alatti vagy felszíni víztestet.

(7) Az (5) bekezdés e) pontja alkalmazásában a vízmegtakarításnak tükröznie kell a 2000/60/EK irányelvből eredő vízgyűjtő-gazdálkodási tervekben meghatározott igényeket, és

a) a potenciális vízmegtakarításnak

aa) legalább 5%-nak kell lennie, ha a meglévő létesítmény vagy infrastruktúra műszaki paraméterei már a beruházás előtt magas fokú hatékonyságot biztosítanak,

ab) legalább 25%-nak kell lennie, ha a hatékonyság jelenlegi foka alacsony, vagy olyan beruházás esetében, amely olyan területen valósul meg, ahol a legnagyobb szükség van a vízmegtakarításra a jó vízállapot eléréséhez,

b) a vízfogyasztás tényleges csökkenésének a beruházás egészének szintjén a meglévő öntözőberendezések vagy a meglévő öntözőinfrastruktúra elemeinek fejlesztésére irányuló beruházás által lehetővé tett potenciális vízmegtakarítás legalább 50%-ának kell lennie.

59. § (1) A támogatási intenzitás nem haladhatja meg az elszámolható költségek 65%-át.

(2) A támogatási intenzitás legfeljebb 80%-ra növelhető, ha

a) a kedvezményezett fiatal mezőgazdasági termelőnek minősül,

b) a beruházás az 56. § (1) bekezdés e)–g) pontja szerinti célkitűzések legalább egyikéhez vagy az állatjóléthez kapcsolódik.

(3) A támogatási intenzitás legfeljebb 100%-ra növelhető, ha a beruházás
   a) az 56. § (1) bekezdés e)–g) pontja szerinti célokhoz kapcsolódó, nem termelő beruházás,
   b) az 56. § (1) bekezdés d) pontja szerinti termelési potenciál helyreállítására irányuló beruházás, valamint a természeti katasztrófák, rendkívüli események, természeti katasztrófához hasonlítható kedvezőtlen éghajlati jelenségek vagy védett állatok által okozott károk megelőzésével és kockázatának csökkentésével kapcsolatos beruházás.

(4) Az 58. § (1) bekezdés g) pontja szerinti öntözési támogatási intenzitása haladhatja meg
   a) az 58. § (5) bekezdés d) pontja szerint végrehajtott, mezőgazdasági üzemen belüli öntözéssel kapcsolatos beruházások esetében az elszámolható költségek 80%-át,
   b) a mezőgazdasági üzemen kívüli, öntözésre szánt mezőgazdasági infrastruktúrába történő beruházások esetében az elszámolható költségek 100%-át,
   c) a mezőgazdasági üzemekben végrehajtott egyéb öntözési beruházások esetében az elszámolható költségek 65%-át.

26. A mezőgazdasági termékek feldolgozásával vagy forgalmazásával kapcsolatos beruházásokhoz nyújtott támogatás

60. § (1) A mezőgazdasági termékek feldolgozásával vagy forgalmazásával kapcsolatos beruházáshoz nyújtott támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) mezőgazdasági termékek feldolgozásával vagy forgalmazásával kapcsolatos tárgyi eszközök és immateriális javak támogatására irányul.

(2) Amennyiben a 314/2005. (XII. 25.) Korm. rendelet értelmében környezeti hatásvizsgálat szükséges, az arra irányuló eljárást a támogatás odaítéléséről szóló döntés időpontját megelőzően szükséges lefolytatni.

(3) Nem nyújtható támogatás
   a) élelmiszeralapú bioüzemanyagok előállításához,
   b) hatályos uniós szabványoknak való megfelelést szolgáló beruházásokhoz,
   c) adathálózatok ingatlanon kívüli vezetékezéséhez vagy kábelezéséhez,
   d) az 1308/2013/EU európai parlamenti és tanácsi rendeletben megállapított valamely tiltás vagy korlátozás megszegésével, ideértve azokat a tiltásokat és korlátozásokat, amelyek kizárólag az 1308/2013/EU európai parlamenti és tanácsi rendelet szerinti támogatásokra vonatkoznak.

61. § (1) A támogatás keretében elszámolható
   a) az ingatlanszerzés költsége, ideértve a lízinget is,
   b) az ingatlan építésével és korszerűsítésével kapcsolatos költségek, ideértve az adathálózatok passzív, ingatlanon belüli vezetékezése vagy strukturált kábelezése, és adott esetben a passzív hálózatnak az ingatlanon belül elhelyezkedő, épületen kívüli kiegészítő részére fordított beruházások kapcsán felmerülő költségeket is,
   c) a gépek és berendezések vásárlásának és lízingelésének költsége az eszköz piaci értékéig,
   d) az a)–c) pont szerinti költségekhez kapcsolódó általános költségek, különösen építészek, mérnökök díjai, tanácsadási díjak, a környezeti és a gazdasági fenntarthatóságra vonatkozó tanácsadással kapcsolatos díjak, ideértve a megvalósíthatósági tanulmányok költségeit akkor is, ha a tanulmányok eredményei alapján nem merülnek fel az a)–c) pont szerinti költségek,
   e) a számítógépes szoftver, felhőalapú és hasonló megoldások vásárlásának, fejlesztésének, és használatának díja, valamint szabadalom, licencia, szerzői jog és védjegy megszerzésének költsége.

(2) A támogatás keretében a működőtőke költsége nem számolható el.

(3) Az (1) bekezdés a) és b) pontja esetén a telekvásárlás költsége csak az adott művelethez kapcsolódó teljes elszámolható költségek 10%-áig számolható el.

(4) A lízingszerződésekkel kapcsolatos, az (1) bekezdés a)–c) pontjában meghatározott költségeken túl egyéb költségek – ideértve a lízingbe adó árrését, a kamatok refinanszírozási költségeit, a közvetett költségeket és a biztosítási díjakat – nem számolhatók el.

62. § (1) A támogatási intenzitás nem haladhatja meg az elszámolható költségek 65%-át.

(2) A támogatási intenzitás legfeljebb 80%-ra növelhető, ha
   a) a kedvezményezett fiatal mezőgazdasági termelőnek minősül,

b) a beruházás az 56. § (1) bekezdés e)–g) pontja szerinti célkitűzések közül egyhez vagy többhöz vagy az állatjóléthez kapcsolódik.

27. A regionális repülőterekre irányuló támogatás

63. § (1) A regionális repülőterekre irányuló támogatás beruházási és működési támogatásként nyújtható.

(2) A repülőtérnek valamennyi légitársaság számára hozzáférhetőnek kell lennie. A kapacitás fizikai korlátozottsága esetén a hozzáférést releváns, nyílt, átlátható és megkülönböztetésmentes módon kell biztosítani.

(3) Nem nyújtható támogatás

a) meglévő repülőtér áttelepítéséhez vagy új személyforgalmi repülőterek létesítéséhez, ideértve a meglévő repülőterek személyforgalmi repülőtérré történő átalakítását is,

b) azoknak a repülőtereknek, amelyeknek az átlagos éves teherforgalma a támogatás odaítélését megelőző két pénzügyi évben meghaladta a 200 000 tonnát, és a támogatás az odaítélését követő két pénzügyi évben előzetesen, megalapozott előrejelzések alapján nem vezethet a repülőtér átlagos éves teherforgalmának 200 000 tonna fölé emelkedéséhez.

(4) Beruházási támogatás a (3) bekezdésben foglaltakon túl nem nyújtható

a) olyan repülőtérnek, amelynek az átlagos éves utasforgalma a támogatás odaítélését megelőző két pénzügyi évben meghaladta a hárommillió főt, és a támogatás az odaítélését követő két pénzügyi évben előzetesen, megalapozott előrejelzések alapján nem vezethet a repülőtér átlagos éves utasforgalmának hárommillió fő fölé emelkedéséhez,

b) meglévő, a Közösségben a légi járatok működtetésére vonatkozó közös szabályokról szóló, 2008. szeptember 24-i 1008/2008/EK európai parlamenti és tanácsi rendelet 2. cikk 16. pontjában meghatározott menetrend szerinti légi járatokat üzemeltető repülőtértől 100 kilométeren belül elhelyezkedő és onnan gépjárművön, buszon, vonaton vagy nagysebességű vonaton 60 percen belül megközelíthető repülőtérnek.

(5) A beruházás nem haladhatja meg – az észszerű forgalmi előrejelzések alapján – a középtávon várt forgalom fogadásához szükséges mértéket.

(6) Beruházási támogatás esetén repülőtéri infrastruktúrához kapcsolódó tárgyi eszközök és immateriális javak számolhatók el, ideértve a tervezési költségeket is.

(7) A beruházási támogatás összege nem haladhatja meg az elszámolható költségeknek és a beruházás működési eredményének a különbségét.

(8) A (7) bekezdés szerinti működési eredmény mértékét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell levonni az elszámolható költségekből.

(9) A beruházási támogatás összege a (8) bekezdés szerinti felső korláton túl nem haladhatja meg

a) az elszámolható költségek 50%-át azon repülőterek esetében, amelyeknek átlagos éves utasforgalma a támogatás odaítélését megelőző két pénzügyi évben egymillió és hárommillió fő között alakult;

b) az elszámolható költségek 75%-át azon repülőterek esetében, amelyeknek az átlagos éves utasforgalma a támogatás odaítélését megelőző két pénzügyi évben nem haladta meg az egymillió főt.

(10) A (4) bekezdés b) pontja és az (5) bekezdés nem alkalmazandó azokra a repülőterekre, amelyeknek az átlagos éves utasforgalma a támogatás tényleges odaítélését megelőző két pénzügyi évben nem haladta meg a 200 000 főt, amennyiben a beruházási támogatás következtében a repülőtér átlagos éves utasforgalma valószínűsíthetően nem emelkedik 200 000 fő fölé a támogatás odaítélését követő két pénzügyi évben.

(11) A (10) bekezdés szerinti kisforgalmú repülőtereknek nyújtott beruházási támogatás a támogatást nyújtó választása szerint a (7) bekezdés szerinti maximális támogatási összegig vagy az elszámolható költségek 75%-áig nyújtható.

(12) Működési támogatás a (3) bekezdésben foglaltakon túl nem nyújtható

a) olyan repülőtérnek, amelynek átlagos éves utasforgalma a támogatás odaítélését megelőző két pénzügyi évben meghaladta a 200 000 főt,

b) olyan naptári évre vonatkozóan, amely során a repülőtér átlagos éves utasforgalma meghaladja a 200 000 főt,

c) olyan feltétellel, hogy a kedvezményezettnek megállapodást kell kötnie bizonyos légitársaságokkal a repülőtéri díjakról, a marketingjellegű kifizetésekről vagy a légitársaságok adott repülőtéren végzett tevékenységének egyéb pénzügyi vonatkozásairól.

(13) A működési támogatás összege nem haladhatja meg a támogatással érintett időszakban keletkezett működési veszteséget és észszerű nyereséget fedező összeget.

(14) A működési támogatás kifizetése történhet előzetesen meghatározott részletekben, amely esetében a részletek összege a támogatásnyújtás időtartama alatt nem növelhető, vagy a tényleges működési veszteség alapján utólagosan megállapított összegek folyósítása útján.

28. A belvízi kikötő fejlesztéséhez nyújtott beruházási támogatás

64. § (1) A belvízi kikötő fejlesztéséhez nyújtott beruházási támogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) belvízi kikötő

a) kikötői infrastruktúrájának és hozzáférési infrastruktúrájának – ideértve a töltő infrastruktúrát is – létrehozására, cseréjére vagy korszerűsítésére irányuló beruházáshoz, valamint

b) kotrásához

nyújtható.

(2) Nem nyújtható támogatás

a) a hajókat fosszilis tüzelőanyagokkal – így különösen dízellel, gáz halmazállapotú földgázzal (sűrített földgáz, CNG), cseppfolyósított földgázzal (LNG) és cseppfolyós propán-bután gázzal (LPG) – ellátó töltő infrastruktúra építéséhez, telepítéséhez vagy korszerűsítéséhez,

b) a szállítással össze nem függő tevékenységekhez, különösen a kikötő területén működő ipari gyártólétesítményekhez, irodahelyiségekhez és üzletekhez, valamint a kikötői felépítményekhez.

(3) A kikötői infrastruktúra működtetésével, építésével vagy fejlesztésével harmadik felet megbízni, a kikötői infrastruktúrát bérbe adni vagy a kikötői infrastruktúra működtetését, építését vagy fejlesztését koncesszióba adni csak átlátható és megkülönböztetésmentes módon, versenyeztetés útján és a vonatkozó közbeszerzési jogszabályok betartásával lehet.

(4) A kikötői infrastruktúrához való hozzáférést az érdekelt felhasználók számára egyenlő és piaci feltételek mellett, megkülönböztetésmentes módon kell biztosítani.

65. § (1) A támogatás keretében a 64. § (1) bekezdése szerinti tevékenységekhez kapcsolódó költségek számolhatók el, ideértve a tervezés költségeit is.

(2) A villamos energiát, hidrogént, ammóniát és metanolt biztosító elektromos és hidrogéntöltő infrastruktúrákhoz nyújtott támogatás esetén a töltő infrastruktúra megépítésének, telepítésének, korszerűsítésének és bővítésének költségei számolhatók el.

(3) A (2) bekezdés szerinti tevékenységek esetén az elszámolható költségek többek között

a) a töltő infrastruktúrának és a kapcsolódó műszaki berendezéseknek a költségei, ideértve a rögzített, mobil vagy úszó létesítményeket,

b) a töltő infrastruktúrának a hálózathoz, illetve a helyi villamosenergia- vagy hidrogéntermelő vagy -tároló egységhez való csatlakoztatásához szükséges bármilyen elektromos vagy egyéb komponensek – többek között az elektromos kábelek és transzformátorok – telepítésének vagy korszerűsítésének költségei,

c) az építési munkálatok, a földterület- vagy útátalakítás költségei, a telepítési és a vonatkozó engedélyek beszerzési költségei,

d) a megújuló villamos energia vagy a megújuló hidrogén helyszíni előállításának beruházási költségei,

e) a megújuló villamos energia vagy a hidrogén tárolóegységeinek beruházási költségei.

(4) A (3) bekezdés d) pontja esetén a termelőlétesítmény névleges termelési kapacitása nem haladhatja meg a csatlakoztatott töltő infrastruktúra maximális névleges teljesítményét vagy töltési kapacitását.

(5) Amennyiben a támogatás hidrogént biztosító töltőinfrastruktúra megépítésére, telepítésére vagy korszerűsítésére irányul, a kedvezményezett kötelezettséget vállal arra, hogy a támogatott töltőinfrastruktúra legkésőbb 2036. január 1-jétől kizárólag megújuló hidrogént fog szolgáltatni.

(6) Amennyiben a támogatás ammóniát vagy metanolt biztosító töltő infrastruktúra megépítésére, telepítésére vagy korszerűsítésére irányul, a kedvezményezett kötelezettséget vállal arra, hogy a támogatott töltő infrastruktúra legkésőbb 2036. január 1-jétől kizárólag olyan ammóniát vagy metanolt fog szolgáltatni, amelynek energiatartalma a biomasszától eltérő megújuló forrásokból származik, és amelyet az (EU) 2018/2001 irányelvben és annak végrehajtási vagy felhatalmazáson alapuló jogi aktusaiban a nem biológiai eredetű megújuló folyékony és gáznemű közlekedési üzemanyagokra vonatkozóan meghatározott módszerekkel összhangban állítottak elő.

66. § (1) A támogatás összege nem haladhatja meg az elszámolható költségeknek és a beruházás, illetve a kotrás működési eredményének a különbségét.

(2) A működési eredmény mértékét

a) előzetesen, megalapozott előrejelzések alapján vagy

b) visszafizetési mechanizmus alkalmazásával utólag

kell levonni az elszámolható költségekből.

(3) A 2,2 millió eurónak megfelelő forintösszeget meg nem haladó támogatás esetén a támogatás összege az (1) és (2) bekezdésben meghatározott módszertől eltérően is meghatározható, azzal, hogy a támogatási intenzitás nem haladhatja meg az elszámolható költségek 80%-át.

29. Válságtámogatás

67. § (1) A válságtámogatás (ezen alcím alkalmazásában a továbbiakban: támogatás) az EUMSz 107. cikk (1) bekezdése szerinti állami támogatásnak minősül, és az „Az állami támogatásokra vonatkozó, az Ukrajna elleni orosz agresszióval összefüggésben a gazdaság támogatását célzó ideiglenes válság- és átállási keret” című, 2023. március 17-i, 2023/C 101/03. számú európai bizottsági közlemény (ezen alcím alkalmazásában a továbbiakban: közlemény) 2.1. szakaszának szabályaival és ezen alcím szerinti támogatási programot jóváhagyó SA.106542 (2023/N) számú, valamint az azt módosító európai bizottsági határozatokban foglaltakkal összhangban nyújtható olyan vállalkozásoknak, amelyek működését a háború gazdasági hatásai hátrányosan érintik. Az érintettségről a vállalkozás a támogatás odaítélését megelőzően nyilatkozik.

(2) A támogatás vissza nem térítendő támogatás, hitel és tőke formájában nyújtható, azzal, hogy hitel és tőke formájában nyújtott támogatás esetén a hitel teljes névértékét vagy a tőke teljes összegét kell figyelembe venni a 69. § (1)–(3) bekezdése szerinti értékhatároknak való megfelelés ellenőrzésekor.

(3) A támogatás 2024. június 30-ig ítélhető oda.

(4) A hitel formájában nyújtott támogatás tőke formájában nyújtott támogatássá alakítható 2024. június 30-ig, úgy, hogy az átalakított támogatás összegét az átalakításkor nem kell újból figyelembe venni a 69. § (1)–(3) bekezdése szerinti értékhatárok vizsgálatakor, de a kedvezményezettnek ezen alcím egyéb feltételeinek az átalakításkor is meg kell felelnie.

68. § (1) Nem részesülhet támogatásban a közlemény 1.1. szakaszában felsorolt jogi aktusokban meghatározott szankciók, valamint a közlemény elfogadását követően az Európai Unió szervei által Oroszország Ukrajna elleni agressziójára tekintettel bevezetett egyéb szankciók hatálya alá tartozó vállalkozás, így különösen nem részesülhet támogatásban a szankciókat bevezető jogi aktusokban kifejezetten megnevezett jogalany, valamint az ilyen jogalany meghatározó befolyása alatt lévő vállalkozás.

(2) Nem nyújtható támogatás az (1) bekezdés szerinti szankciókkal érintett ágazatokban folytatott tevékenységhez, ha a támogatás veszélyeztetné a szankciók célkitűzéseit.

(3) A támogatás nyújtásának nem lehet feltétele az, hogy a kedvezményezett a gazdasági tevékenységét áthelyezze az EGT-n belül egy másik országból Magyarország területére.

(4) A mezőgazdasági termékek elsődleges termelésével foglalkozó vállalkozásoknak nyújtott támogatás nem határozható meg a piacon forgalmazott termékek ára vagy mennyisége alapján.

(5) A halászati és akvakultúra-ágazatban működő vállalkozásoknak nyújtott támogatás nem tartozhat a 717/2014/EU bizottsági rendelet 1. cikk (1) bekezdés a)–k) pontja szerinti támogatási kategóriák közé.

69. § (1) A támogatás támogatástartalma a közlemény 2.1. szakasza alapján nyújtott egyéb támogatásokkal együtt vállalkozásonként – a vállalkozás kapcsolt vállalkozásait is figyelembe véve, a (2) és (3) bekezdésben meghatározott kivétellel – nem haladhatja meg a 2,25 millió eurónak megfelelő forintösszeget.

(2) A mezőgazdasági termékek elsődleges termelésével foglalkozó vállalkozások esetén az e tevékenységekhez összesen nyújtott támogatás támogatástartalma a közlemény 2.1. szakasza alapján nyújtott egyéb támogatásokkal együtt vállalkozásonként – a vállalkozás kapcsolt vállalkozásait is figyelembe véve – nem haladhatja meg a 280 000 eurónak megfelelő forintösszeget.

(3) A halászati és akvakultúra-ágazatban működő vállalkozások esetén az e tevékenységekhez összesen nyújtott támogatás támogatástartalma a közlemény 2.1. szakasza alapján nyújtott egyéb támogatásokkal együtt vállalkozásonként – a vállalkozás kapcsolt vállalkozásait is figyelembe véve – nem haladhatja meg a 335 000 eurónak megfelelő forintösszeget.

(4) Ha egy vállalkozás több ágazatban is tevékenységet folytat, és ezekre az (1)–(3) bekezdés szerint eltérő felső határok vonatkoznak, a vállalkozás a támogatásokról olyan elkülönített nyilvántartást vezet, amely biztosítja az érintett tevékenységekre vonatkozó, (1)–(3) bekezdés szerinti felső határok betartását, és azt, hogy a teljes maximális összeg vállalkozásonként – a vállalkozás kapcsolt vállalkozásait is figyelembe véve – ne haladja meg a 2,25 millió eurónak megfelelő forintösszeget.

(5) Ha egy vállalkozás a (2) és (3) bekezdés szerinti ágazatokban tevékenykedik, a teljes maximális támogatási összeg vállalkozásonként – a vállalkozás kapcsolt vállalkozásait is figyelembe véve – nem haladhatja meg a 335 000 eurónak megfelelő forintösszeget.

70. § (1) A mezőgazdasági termékek feldolgozásával vagy forgalmazásával foglalkozó vállalkozások számára a 69. § (1) bekezdése szerinti maximális támogatástartalommal nyújtható támogatás, ha a támogatás mértéke nem függ a mezőgazdasági termék elsődleges termelője részére történő teljes vagy részleges átadásától, és a támogatás mértékét nem az elsődleges termelőktől beszerzett vagy az érintett vállalkozások által forgalomba hozott termékek ára vagy mennyisége alapján határozzák meg.

(2) A mezőgazdasági termékek feldolgozásával vagy forgalmazásával foglalkozó vállalkozások számára nyújtott támogatás mértéke az (1) bekezdéstől eltérően meghatározható az elsődleges termelőktől beszerzett vagy az elsődleges termelők által forgalomba hozott termékek ára vagy mennyisége alapján, ha a kérdéses termékeket az elsődleges termelő nem élelmiszeripari célokra vagy egyáltalán nem hozta volna forgalomba.

71. § (1) Azonos vagy részben azonos elszámolható költségek esetén a támogatás abban az esetben halmozható más állami támogatással, ha az nem vezet az Atr. 2. § 2a. pontja szerinti csoportmentességi rendeletekben vagy az Európai Bizottság jóváhagyó határozatában meghatározott legmagasabb támogatási intenzitás vagy összeg túllépéséhez.

(2) Ha a támogatás mellett a kedvezményezett az Atr. 2. § 1. pontja szerinti rendeletekben meghatározott csekély összegű támogatásban is részesül, az igénybe veendő vagy igénybe vett csekély összegű támogatás nem csökkenti a támogatás 69. § (1)–(3) bekezdése szerinti legmagasabb mértékét. Ha a támogatás mellett a kedvezményezett azonos vagy részben azonos elszámolható költségek vonatkozásában csekély összegű támogatást is igénybe vesz, a támogatáshalmozás nem vezethet a támogatás 69. § (1)–(3) bekezdése szerinti legmagasabb mértékének túllépéséhez.

(3) A támogatás akkor halmozható az EUMSz 107. cikk (2) bekezdés b) pontja szerinti támogatással, ha az nem vezet a kedvezményezett által elszenvedett kár túlkompenzációjához.

(4) Azonos vagy részben azonos elszámolható költségek esetén a támogatás nem halmozható az „A gazdaságnak a jelenlegi Covid19-járvánnyal összefüggésben való támogatását célzó, állami támogatási intézkedésekre vonatkozó ideiglenes keret módosítása” című, 2022. november 7-i, 2022/C 423/04. számú európai bizottsági közleménnyel módosított, az „A gazdaságnak a jelenlegi Covid19-járvánnyal összefüggésben való támogatását célzó, állami támogatási intézkedésekre vonatkozó ideiglenes keret hatodik módosítása, és az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a rövid lejáratú exporthitel-biztosításokra történő alkalmazásáról szóló, a tagállamokhoz címzett bizottsági közlemény mellékletének módosítása” című, 2021. november 24-i, 2021/C 473/01. számú európai bizottsági közlemény 3.13. szakasza szerinti támogatással.

72. § (1) A támogatást nyújtó az Atr. 18/C. § (1) bekezdésében meghatározott határidők szerint továbbítja az állami támogatások európai uniós versenyszempontú vizsgálatáért felelős szervezet részére a támogatásoknak az Atr. 6. melléklete szerinti adatait az Atr. 18/D. § (1) bekezdés e) pontja szerinti közzététel céljából.

(2) A támogatást nyújtó az Atr. 18/A. § (7) bekezdés a) pontjára figyelemmel minden év április 30-áig beszámolót készít a megelőző évben nyújtott támogatásokról az állami támogatások európai uniós versenyszempontú vizsgálatáért felelős szervezet részére.

(3) A támogatást nyújtó és a kedvezményezett a támogatással kapcsolatos iratokat a támogatás odaítélésétől számított tíz évig megőrzi.

(4) A közlemény 92. pontjára figyelemmel a támogatást nyújtó átadja az állami támogatások európai uniós versenyszempontú vizsgálatáért felelős szervezet részére az Európai Bizottság megkeresésének megválaszolásához szükséges összesített adatokat.

IV. FEJEZET
ZÁRÓ RENDELKEZÉSEK

73. § Ez a rendelet a kihirdetését követő napon lép hatályba.

74. § (1) E rendelet rendelkezéseit a rendelet hatálybalépésekor folyamatban lévő ügyekben is alkalmazni kell, különösen az e rendelet hatálybalépését megelőzően benyújtott igénylések alapján létrejövő hitel-, kezességvállalási és lízingügyletek e rendelet hatálybalépését megelőzően megkötött, valamint hatályba lépett hitel-, kezességvállalási és lízingszerződések kapcsán kiállításra kerülő támogatói okiratok, valamint e rendelet hatálybalépésekor fennálló valamennyi fennálló hitel-, kezességvállalási és lízingügylet kapcsán a kifizetésre kerülő támogatások vonatkozásában.

(2) Ha a miniszter vagy az e rendelet alapján kijelölt kezelő szerv az e rendelet hatálya alá tartozó fejezeti kezelésű előirányzatok vonatkozásában e rendelet hatálybalépését megelőzően – a jogelőd miniszter által irányított szerv fejezetére vonatkozó, a fejezeti és az egyes központi kezelésű előirányzatok kezeléséről és felhasználásáról szóló miniszteri rendeletben foglalt szabályok alapján jogszerűen – tett kötelezettségvállalást és teljesített kifizetést, azt a miniszter, valamint az arra jogosult kezelő szerv által jogszerűen tett kötelezettségvállalásnak és kifizetésnek kell tekinteni.

75. § Ez a rendelet

a) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a csekély összegű támogatásokra való alkalmazásáról szóló, 2023. december 13-i (EU) 2023/2831 bizottsági rendelet,

b) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a mezőgazdasági ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról szóló, 2013. december 18-i 1408/2013/EU bizottsági rendelet,

c) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének a halászati és akvakultúra ágazatban nyújtott csekély összegű támogatásokra való alkalmazásáról szóló, 2014. június 27-i 717/2014/EU bizottsági rendelet,

d) a Szerződés 107. és 108. cikke alkalmazásában bizonyos támogatási kategóriáknak a belső piaccal összeegyeztethetővé nyilvánításáról szóló, 2014. június 17-i 651/2014/EU bizottsági rendelet I. és II. fejezete, valamint 13–14. cikke, 17. cikke, 18. cikke, 19. cikke, 22. cikke, 25. cikke, 26. cikke, 28. cikke, 29. cikke, 31. cikke, 38. cikke, 38a. cikke, 41. cikke, 48. cikke, 53. cikke, 55. cikke, 56. cikke, 56a. cikke, 56c. cikke,

e) az Európai Unió működéséről szóló szerződés 107. és 108. cikkének alkalmazásában a mezőgazdasági és az erdőalapú ágazatban, valamint a vidéki térségekben nyújtott támogatások bizonyos kategóriáinak a belső piaccal összeegyeztethetőnek nyilvánításáról szóló, 2022. december 14-i (EU) 2022/2472 bizottsági rendelet 14. cikke és 17. cikke,

f) az „Az állami támogatásokra vonatkozó, az Ukrajna elleni orosz agresszióval összefüggésben a gazdaság támogatását célzó ideiglenes válság- és átállási keret" című, 2023. március 17-i, 2023/C 101/03. számú európai bizottsági közlemény 2.1. szakasza,

g) az „Állami támogatási intézkedésekre vonatkozó ideiglenes keret a gazdaságnak a jelenlegi COVID-19-járvánnyal összefüggésben való támogatása céljából" című, 2020. március 19-i, 2020/C 91 I/01 számú európai bizottsági közlemény,

h) az Európai Bizottságnak a repülőtereknek és a légitársaságoknak nyújtott állami támogatásról szóló közleménye (2014/C99/03)

hatálya alá tartozó támogatást tartalmaz.

Nagy Márton István s. k.,
nemzetgazdasági miniszter

1. melléklet a 20/2024. (VI. 24.) NGM rendelethez

XXIII. Nemzetgazdasági Minisztérium fejezet 2024. évi fejezeti kezelésű kiadási előirányzatainak feladatterve

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1.	**Áht-azonosító**	**Címnév**	**Alcímnév**	**Jogcímcsop. név**	**Jogcímnév**	**Előirányzat célja**	**Kifizetésben részesülők köre**	**Támogatás biztosításának módja**	**Támogatási előleg**	**Rendelkezésre bocsátás módja**	**Visszafizetés határideje**	**Biztosíték**	**Kezelő szerv**	**Lebonyolító szerv**	**Európai uniós forrásból finanszírozott költségvetési támogatás közreműködő szervezete**
2.	**401428**	**10 Fejezeti kezelésű előirányzatok**													
3.	**401439**		**1 Gazdaságfejlesztési feladatok**												
4.	**386595**			**1 Gazdaságfejlesztési programok**		Az előirányzat fedezetet nyújt kormányzati gazdaságfejlesztési célú feladatok és támogatási programok keretében hitelszerződésekhez biztosított kamattámogatás, kezességi díjtámogatás, kezelési költségtámogatás, egyéb költségtámogatás és azok járulékos költségei finanszírozására, így különösen: 1) Széchenyi Kártya Program, 2) Agrár Széchenyi Kártya Konstrukció, 3) Intézményi Kezességi Díjtámogatások, 4) az MFB Zrt. hitelprogramjainak kamattámogatása, 5) az előirányzat felhasználásához kapcsolódó kincstári díj és lebonyolító szerv igénybevétele.	1) Pénzügyi intézmények és pénzügyi vállalkozások (ideértve a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény alapján működő megyei és fővárosi vállalkozásfejlesztési alapítványokat is). 2) A végső Kedvezményezettek részére biztosított támogatásokat megelőlegező pénzügyi intézmények, továbbá az Európai Unió működéséről szóló szerződés 107. és 108. cikkének alkalmazásában a mezőgazdasági és az erdészeti ágazatban, valamint a vidéki térségekben nyújtott támogatások bizonyos kategóriáinak a belső piaccal összeegyeztethetőnek nyilvánításáról szóló, 2014. június 25-i 702/2014/EU bizottsági rendelet I. mellékletében meghatározott kis- és középvállalkozás kritériumoknak megfelelő vállalkozások, valamint természetes személyek. 3) Pénzügyi intézmények és pénzügyi vállalkozások (ideértve a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény alapján működő megyei és fővárosi vállalkozásfejlesztési alapítványokat is). 4) MFB Zrt. 5) Központi költségvetési szerv, gazdasági társaság.	Egyedi döntés és kérelem alapján, támogatói okiratban, csoportos támogatói okiratban, támogatási szerződésben vagy a Támogató, a támogatásokat megelőlegező pénzügyi intézmények és az 1. pont esetén a KAVOSZ Zrt., a 3. pont esetén a Garantiqa Zrt. közötti háromoldalú keretszerződésekben, a 4. pont esetén a Támogató és az MFB Zrt. közötti keretszerződésben foglaltak szerint.	-	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
5.	**401984**			**2 Gazdasági ellenálló-képesség fejlesztése és ipari alkalmazott technológiák bevezetése**		Az előirányzat fedezetet nyújt a kormányzati technológiai és digitális fejlesztési célú, valamint célzott vállalkozásfejlesztési programokhoz, feladatokhoz és azok járulékos költségeihez, különösen: 1) Digitális Export Stratégia, 2) Mesterséges Intelligencia Stratégia, 3) Nemzeti Technológiai Platform, illetve az ehhez kapcsolódó ágazati és szakmai koordinációs feladatok, 4) Digitális Agrárstratégia, 5) a World Robot Olympiad támogatásával kapcsolatos feladatok, 6) Élelmiszeripari Beszállító-fejlesztési Program, 7) az előirányzat felhasználásához kapcsolódó kincstári díj és lebonyolító szerv igénybevétele.	1)-6) Költségvetési szerv, gazdasági társaság, civil szervezet, helyi önkormányzat, köztestület, közfeladatot ellátó közérdekű vagyonkezelő alapítvány, alapítvány, felsőoktatási intézmény. 7) Központi költségvetési szerv, gazdasági társaság.	Egyedi döntéssel, kérelem vagy pályázat alapján, támogatói okiratban vagy támogatási szerződésben foglaltak szerint, a közfeladatot ellátó közérdekű alapítványokról szóló 2021. évi IX. törvény (a továbbiakban: KEKVA tv.) szerinti megállapodásban foglaltaknak megfelelően.	Előleg biztosítható.	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
6.	**401440**			**3 Járműipari innovációs és fejlesztési feladatok**		Az előirányzat fedezetet nyújt a nemzetgazdasági miniszter feladat- és hatáskörébe tartozó járműipari innovációs és közlekedésfejlesztési feladatok finanszírozására, valamint a kapcsolódó kincstári díj megfizetésére.	Gazdasági társaság, közfeladatot ellátó közérdekű vagyonkezelő alapítvány, közfeladatot ellátó közérdekű vagyonkezelő alapítvány által fenntartott felsőoktatási intézmény, központi költségvetési szerv.	Egyedi döntés és kérelem alapján, támogatói okiratban, támogatási szerződésben, vagy a KEKVA tv. szerinti megállapodásban foglaltaknak megfelelően.	Előleg biztosítható.	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	-	-

7.	**401962**			**4 Iparfejlesztési programok**		Az előirányzat fedezetet nyújt a nemzetgazdasági miniszter iparügyekért való felelősségi körébe tartozó programok, feladatok és azok járulékos költségei finanszírozásához, különösen: 1) nemzetközi szabványosítással kapcsolatos feladatok, 2) az ágazat védelmi és biztonsági felkészítésének állami feladatai a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény alapján, 3) Bay Zoltán Nonprofit Kft. támogatása, 4) az előirányzat felhasználásához kapcsolódó kincstári díj és lebonyolító szerv igénybevétele.	1) Magyar Szabványügyi Testület. 2)–3) Gazdasági társaság, felsőoktatási intézmény, államilag elismert szakképző iskolának minősülő köznevelési intézmény, a tudományos kutatásról, fejlesztésről és innovációról szóló 2014. évi LXXVI. törvény szerinti kutatóhely. 4) Központi költségvetési szerv, gazdasági társaság.	Egyedi döntés és kérelem alapján, támogatói okiratban vagy támogatási szerződésben foglaltak szerint.	Előleg biztosítható.	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
8.	**401973**			**5 Vállalkozásfejlesztési programok**		Az előirányzat fedezetet nyújt kormányzati vállalkozásfejlesztési célú programok, feladatok és azok járulékos költségei – különösen az előirányzat felhasználásához kapcsolódó kincstári díj és lebonyolító szerv igénybevétele – finanszírozására.	Gazdasági társaság, egyéni cég, egyéni vállalkozó, szövetkezet, európai részvénytársaság, európai szövetkezet, civil szervezet, természetes személy, köztestület, központi költségvetési szerv.	Egyedi döntéssel, kérelem vagy pályázat alapján, támogatói okirat vagy támogatási szerződés szerint, egyéb szerződések, dokumentumok alapján.	Előleg biztosítható.	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint. Egyéb szerződések, dokumentumok alapján.	Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
9.	**400628**			**6 Energiaintenzív vállalatok támogatása**		Az előirányzat forrást biztosít az energiaintenzív mikro-, kis- és középvállalkozások működési (energia) költségeinek finanszírozására, az e vállalkozások energiahatékonyság-növelését célzó beruházásaihoz igényelt hitelek önerő-kiegészítő támogatására, valamint az előirányzat felhasználásához kapcsolódó kincstári díj és lebonyolító szerv igénybevétele költségeinek megfizetésére.	Gazdasági társaság, egyéni cég, egyéni vállalkozó, egyéb önálló vállalkozó, központi költségvetési szerv.	Egyedi döntés és kérelem alapján, támogatói okiratban vagy támogatási szerződésben foglaltak szerint.	Előleg biztosítható.	Egy összegben vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
10.	**256101**		**2 Hozzájárulás a Művészetek Palotájának működtetéséhez**			Az előirányzat célja a Művészetek Palotája épülete kapcsán a rendelkezésre állási díj, az épület üzemeltetésével kapcsolatos közüzemi díjak (víz, csatorna, fűtés, villamos energia), az egyéb kapcsolódó üzemeltetési, fenntartási és pénzügyi szolgáltatási díjak, valamint az előirányzat felhasználásához kapcsolódó kincstári díj finanszírozása.	Nemzeti Filharmónia Ingatlanfejlesztési Korlátolt Felelősségű Társaság, központi költségvetési szerv.	Rendelkezésre Állási Szerződés szerint.	-	Rendelkezésre Állási Szerződés szerint.	Rendelkezésre Állási Szerződés szerint.	Rendelkezésre Állási Szerződés szerint.	-	-	-
11.	**270701**		**3 Hozzájárulás a sportlétesítmények PPP bérleti díjához**			Az előirányzat forrást biztosít: 1) a Sport XXI. Létesítményfejlesztési Program keretében megvalósult tornatermek, tanuszodák és sportcsarnokok szolgáltatási díjának és a szolgáltatási szerződésekből eredő egyéb kötelezettségek – ideértve a késedelmi kamatokat –, 2) a PPP megállapodások kapcsán az állam érdekeinek védelmében igénybe vett pénzügyi, műszaki és jogi tanácsadói díjak és perviteli költségek, 3) az előirányzat felhasználásához kapcsolódó kincstári díj finanszírozására.	Szolgáltatási szerződésekben meghatározott kedvezményezettek, egyéb szerződéses partnerek, központi költségvetési szerv	Visszterhes polgári jogi szerződés szerint.	-	Visszterhes polgári jogi szerződés szerint.	Visszterhes polgári jogi szerződés szerint.	Visszterhes polgári jogi szerződés szerint.	-	-	-
12.	**401451**		**4 Egyéb ágazati feladatok**			Az előirányzat célja a nemzetgazdasági miniszter feladat- és hatáskörébe tartozó, az e fejezetbe sorolt más költségvetési kiadási előirányzatok terhére nem finanszírozható feladatok és azok járulékos költségei költségvetési fedezetének biztosítása, különösen: 1) szakértői, tanácsadási, valamint médiafigyelési és -elemzési szolgáltatások, 2) az OFA Országos Foglalkoztatási Közhasznú Nonprofit Kft. működése és feladatellátása, 3) az Ágazati Párbeszéd Bizottságok belföldi szakmai munkája, 4) a Magyar Turisztikai Ügynökség Zrt. működtetése és szakmai feladatainak ellátása, így különösen a turisztikai térségek fejlesztésének állami feladatairól szóló törvény végrehajtásáról szóló 235/2019. (X. 15.) Korm. rendelet szerinti turisztikai tárhelyszolgáltatói és vagyonkezelői feladatok, 5) az előirányzat felhasználásával kapcsolatos kincstári díj és lebonyolító szerv igénybevétele.	1)-4) gazdasági társaság, civil szervezet, szakszervezet, szakszervezeti szövetség, munkáltatói érdekképviselet, központi költségvetési szerv, alapítvány, közfeladatot ellátó közérdekű vagyonkezelő alapítvány, 5) központi költségvetési szerv, gazdasági társaság	Egyedi döntés alapján, támogatói okiratban vagy támogatási szerződésben foglaltak szerint, a KEKVA tv. szerinti megállapodásban foglaltaknak megfelelően.	Előleg biztosítható.	Egy összegben, vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	Igénybe vehető.	-
13.	**401851**		**5 Nemzetközi tagdíjak**			Az előirányzat célja a nemzetgazdasági miniszter feladat- és hatáskörébe tartozó nemzetközi szervezetek felé tagdíjfizetési, hozzájárulási kötelezettségek teljesítése, valamint a kapcsolódó kincstári díj fedezetének biztosítása.	nemzetközi szervezetek, központi költségvetési szerv	Csatlakozási vagy finanszírozási megállapodásokban foglaltak szerint.	-	Csatlakozási vagy finanszírozási megállapodásokban foglaltak szerint.	-	-	-	-	-

14.	**402906**		**6 Budai Egészség-központ Zrt. beruházása**			Az előirányzat fedezetet nyújt a Budai Egészségközpont Zrt. egészségügyi ellátással összefüggő kapacitásbővítő beruházása támogatásának, valamint az előirányzat felhasználásához kapcsolódó kincstári díjnak a finanszírozására.	Budai Egészségközpont Zrt., központi költségvetési szerv	Egyedi döntés alapján, támogatói okiratban vagy támogatási szerződésben foglaltak szerint.	Előleg biztosítható.	Egy összegben, vagy részletekben, idő- vagy teljesítés-arányosan.	A támogatási jogviszony szerinti dokumentumban meghatározottak szerint.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	-	-	-
15.	**360239**		**Turisztikai fejlesztési feladatok**			Az előirányzat fedezetet nyújt: 1) a Magyar Turisztikai Ügynökség Zrt. turizmussal és vendéglátással kapcsolatos egyes feladatainak ellátásához, így a turisztikai térségek fejlesztésének állami feladatairól szóló 2016. évi CLVI. törvényben, annak felhatalmazása alapján kiadott Korm. rendeletekben, különösen a Magyar Turisztikai Ügynökség Zártkörűen Működő Részvénytársaság turizmussal és vendéglátással kapcsolatos egyes feladatainak meghatározásáról szóló 61/2017. (III. 20.) Korm. rendeletben foglaltakra; 2) a Kisfaludy fejlesztési program lebonyolítására, a Nemzeti Turisztikai Adatszolgáltató Központ informatikai rendszerével összefüggő költségek finanszírozására, kivéve az informatikai alapinfrastruktúra működtetésének kiadásait; 3) a nemzeti rendezvényekhez kapcsolódó közszolgáltatási célú rendezvények megszervezésére; 4) a hazai és nemzetközi rendezvények kommunikációs és promóciós kiadásaira, valamint a rendezvények közvetítésével kapcsolatos kiadásokra; 5) térségi turisztikai fejlesztési projektek lebonyolítására, célzott támogatására; 6) egyéb turisztikai fejlesztési projektek lebonyolítására, célzott támogatására; 7) turisztikai jelentőséggel bíró fesztiválok, rendezvények, valamint a kis- és középvállalkozások ezeken való részvételének támogatására; 8) ágazati jelentőségű informatikai rendszerek fejlesztésére és működtetésére; 9) gasztronómiai projektek lebonyolítására, célzott támogatására; 10) célzott támogatások nyújtására szakágazatokkal összefüggő események, projektek szervezéséhez; 11) turizmus-diplomáciai feladatokkal összefüggő, nem a fejezetnél keletkező közvetlen kiadások finanszírozására; 12) az idegenvezetők tevékenységének támogatására; 13) a beutazó egészségturizmusban érintettek tevékenységének támogatására; 14) a minőségi vendéglátóipari beszállítói tevékenység fenntartásának, gasztronómiai jelentőségű mezőgazdasági, halászati és akvakultúra-termékek előállításának, feldolgozásának, értékesítésének és forgalmazásának támogatását célzó programok megvalósítására; 15) turizmus és vendéglátás területét érintő beruházások, infrastrukturális fejlesztések, szolgáltatások támogatására és a meglévő kapacitások bővítésére; 16) cigányzenészek, népzenészek számára támogatási program megvalósítására; 17) a beutaztató, utazásszervezéssel foglalkozó vállalkozások támogatási programjainak megvalósítására; 18) az előirányzat céljaihoz kapcsolódóan határon túlra nyújtott támogatáshoz, összhangban a határon túli költségvetési támogatások sajátos szabályairól szóló 98/2012. (V. 15.) Korm. rendeletben [a továbbiakban: 98/2012. (V. 15.) Korm. rendelet] foglaltakkal; 19) jogszabályban vagy kormányhatározatban a turizmusért és a vendéglátásért való kormányzati felelősségi körben meghatározott egyéb, a turisztikai és a vendéglátási szakágazattal kapcsolatos célok végrehajtására; 20) a Magyar Turisztikai Ügynökség Zrt.-vel kötött partnerségi megállapodás keretében együttműködő szervezetek turisztikai feladataihoz közvetlenül kapcsolódó, a megállapodásban meghatározott tevékenységek végrehajtásához szükséges kiadásokra; 21) a 29. alcím szerint nyújtott válságtámogatás finanszírozására; 22) az előirányzat felhasználásával kapcsolatos kincstári díjakra.	Természetes személy, adószámos magánszemély, őstermelő, egyéni vállalkozó, gazdasági társaság, civil szervezet, egyéni cég, szövetkezet, helyi önkormányzat és az általa fenntartott költségvetési szerv, köztestület, központi költségvetési szerv és az általa fenntartott költségvetési intézmény, szakmai érdekképviselet, egyházi jogi személy, befektetési alapok és az azok nevében eljáró alapkezelők, 98/2012. (V. 15.) Korm. rendelet 2. § (1) bekezdésében meghatározott személyek és szervezetek.	Egyedi döntéssel, kérelem vagy pályázat alapján, támogatói okirat vagy támogatási szerződés szerint.	Előleg folyósítható.	Egy összegben, vagy részletekben, idő- vagy teljesítés-arányosan.	Kezelői megállapodás, a támogatási jogviszony szerinti dokumentumban meghatározottak.	Az Ávr. 84. § (2) bekezdése szerinti lehetséges biztosítékok.	Magyar Turisztikai Ügynökség Zrt.	-	-

2. melléklet a 20/2024. (VI. 24.) NGM rendelethez

XXIII. Nemzetgazdasági Minisztérium fejezet központi kezelésű kiadási előirányzatainak feladatterve

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1.	**Áht-azonosító**	**Címnév**	**Alcímnév**	**Jogcím-csop. név**	**Jogcímnév**	**Előirányzat célja**	**Kifizetésben részesülők köre**	**Támogatás biztosításának módja**	**Támogatási előleg**	**Rendelkezésre bocsátás módja**	**Visszafizetés határideje**	**Biztosíték**	**Kezelő szerv**	**Lebonyolító szerv**	**Európai uniós forrásból finanszírozott költségvetési támogatás közreműködő szervezete**
2.	**399062**	**11 Központi kezelésű előirány-zatok**													
3.	**368206**		**01 Egyetemes postai szolgáltató méltánytalan többletter-hének megtérítése**			Az előirányzat fedezetet biztosít az egyetemes postai szolgáltató méltánytalan többletterhének megtérítésére, amelynek részletes szabályait az állam és a Magyar Posta Zrt. között megkötött Egyetemes Postai Közszolgáltatási Szerződés (a továbbiakban: EPKSZ) tartalmazza.	A postai szolgáltatásokról szóló 2012. évi CLIX. törvény 18. § (1) bekezdése alapján kijelölt egyetemes postai szolgáltató	Az EPKSZ alapján kötött külön megállapodásban foglaltak szerint.	-	Az EPKSZ alapján kötött külön megállapodás-ban foglalt feltételek teljesülését követő 15 napon belül.	-	-	-	-	
4.	**019051**		**02 Eximbank Zrt. kamat-kiegyenlítése**			Az előirányzat célja az Eximbank Zrt. hitelnyújtásait és követelésvásárlásait támogató, a Magyar Export-Import Bank Részvénytársaság kamatkiegyenlítési rendszeréről szóló 85/1998. (V. 6.) Korm. rendelet szerinti kamatkiegyenlítési rendszerből eredő kifizetések teljesítése.	Eximbank Zrt.	-	-	A Magyar Államkincstár utalványa alapján a Nemzeti Adó- és Vámhivatal folyósítja.	-	-	Magyar Államkincstár	-	
5.	**295980**		**03 Peres ügyek**			Az előirányzat célja: 1) a jogerős bírósági ítéleten, végzésen, illetve a bíróság jogerős végzésével jóváhagyott egyezségen alapuló, az államot terhelő kifizetések, 2) a stabil vérkészítménytől HCV vírussal megfertőződött veleszületett vérzékenységben szenvedő állampolgárok egységes állami kártalanításáról szóló 1093/2000. (XI. 24.) Korm. határozatból eredő kötelezettségek, valamint az ezekhez kapcsolódó szakértői tevékenység költségeinek, 3) polgári jogviszonyokban a nemzetgazdasági miniszter által képviselt magyar állam jogi képviseletét ellátó ügyvédek megbízási díjának, költségeinek, 4) az állammal szemben kezdeményezett valamennyi választottbírósági kötelező erejű határozatból eredő kifizetési kötelezettségek finanszírozása.	Jogerős döntésben foglaltak szerint megjelöltek, stabil vérkészítménytől HCV-vírussal megfertőződött veleszületett vérzékenységben szenvedő állampolgárok, ügyvédek, ügyvédi irodák, szakértők, választottbíróságok, bíróságok.	-	-	Jogerős és végrehajtható, vagy előzetesen végrehajtható bírósági határozat, eljárási díj- és költségfizetési kötelezettséget megállapító határozat, kártalanításról szóló megállapodás, egyéb szerződések alapján.	-	-	Magyar Államkincstár, a kötelezettség-vállalás, a teljesítésigazolás, az érvényesítés, illetve az ezekkel kapcsolatos adatszolgáltatás kivételével	-	
6.	**399073**		**04 Gazdaság-fejlesztési célú nemzetközi pénzügyi kapcsola-tokból eredő kiadások**			Az előirányzat célja a nemzetgazdasági miniszter feladat- és hatáskörébe tartozó nemzetközi pénzügyi intézményekben és alapokban viselt tagságból eredő kiadások fedezetének biztosítása, így különösen: 1) Magyarországnak az Európa Tanács Fejlesztési Bankban lévő tagsága fenntartását szolgáló kifizetések, 2) a Multilaterális Fejlesztésfinanszírozási Együttműködési Központhoz való magyar csatlakozás kapcsán vállalt hozzájárulás, 3) az Európai Újjáépítési és Fejlesztési Bank képviseletét segítő horvát és szlovák tanácsadók költségeiből hazánkat érintő hányad, 4) letétőrzési díjak, utalási költségek megfizetése.	Nemzetközi pénzügyi intézmények, valamint az ezekkel kötött finanszírozási megállapodások szerinti szakértők.	Finanszírozási megállapodásokban foglaltak szerint.	-	Finanszírozási megállapodá-sokban foglaltak szerint.	-	-	-	-	-

VIII. A Kúria határozatai

A Kúria 7/2024. JEH határozata (Jpe.IV.60.056/2023/11. szám) a mintaperben hozott – felülvizsgálattal nem támadott – határozattól való eltérésről

A Kúria Jogegységi Panasz Tanácsa a Kúria K.V. tanácsának előzetes döntéshozatali indítványa alapján lefolytatott jogegységi eljárásban meghozta a következő

jogegységi határozatot:

1. A mintaperben, alsóbb bírósági szinten hozott ítélet a Kúriát nem köti, vagyis a felülvizsgálattal nem támadott mintaperben hozott ítélettől a Kúria eltérhet az annak alapján hozott ítéletek jogszerűségének vizsgálatára irányuló felülvizsgálati eljárásban.
2. A Kúria K.V. ítélkező tanácsa a Bírósági Határozatok Gyűjteményében közzétett Kfv.37.471/2019/11. számú ítélet indokolásának [48] bekezdésében foglalt jogértelmezéstől eltérhet, az és a hasonló jogértelmezést tartalmazó határozatok a továbbiakban kötelező erejűként nem hivatkozhatók.

Indokolás

I.

[1] A Kúria előtt Kfv.37.355/2023. számon folyamatban lévő közigazgatási perben az eljáró tanács (a továbbiakban: Indítványozó tanács) a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény (a továbbiakban: Bszi.) 32. § (1) bekezdés b) pontja alapján előzetes döntéshozatali indítványt terjesztett elő a jogegység érdekében, mert jogkérdésben el kíván térni a Kúria – a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 33. §-ának értelmezésén alapuló – Kfv.37.471/2019/11., Kfv.37.472/2019/8., Kfv.37.473/2019/9. és Kfv.37.481/2019/9. számú, a Bírósági Határozatok Gyűjteményében (a továbbiakban: BHGY) közzétett határozataitól.

[2] Az Indítványozó tanács az előtte folyamatban lévő eljárást a Bszi. 32. § (2) bekezdése szerint felfüggesztette a jogegységi eljárás befejezéséig.

II.

[3] Az Indítványozó tanács előtt folyamatban lévő felülvizsgálati eljárás tényállása szerint a felperes Budapest XXIII. kerületének több önálló helyrajzi számú, külterületi, szántó művelési ágú, nem teljesen összefüggő ingatlanain, összesen 210.119 m^2 területen golfpályát alakított ki. Az alperes – megismételt – földvédelmi eljárásban ingatlanonként hozott összesen 22 db határozatot, amelyekkel elrendelte az engedély nélkül más célra hasznosított termőföldeknek a más célú hasznosítását közvetlenül megelőző, az ingatlan-nyilvántartásban rögzített művelési ágnak és minőségi osztálynak megfelelő állapotába való helyreállítását a termőföld védelméről szóló 2007. évi CXXIX. törvény (a továbbiakban: Tfvt.) 16. § (1), (2), (7) bekezdései és a (11) bekezdés b) pontja alapján.

[4] A felperes egy keresetlevélben indított közigazgatási pert a 22 db határozat jogszerűségének felülvizsgálata iránt. Az elsőfokú bíróság határozatonként elkülönítette a közigazgatási pereket, és a 111.K.702.171/2022. számú perben a Kp. 33. § (1) bekezdése alapján döntött annak mintaperként történő elbírálásáról. Erre tekintettel a többi elkülönített perben az eljárást a mintaper elbírálásáig felfüggesztette. Az elsőfokú bíróság a mintaperben hozott 13. sorszámú ítéletével a támadott közigazgatási határozatot megsemmisítette, és az alperest új eljárás lefolytatására kötelezte. Indokolása szerint az alperesnek az eljárása során a már hatályon kívül helyezett, de az eljárás megindulásakor hatályban volt Tfvt. 16/B. §-át alkalmaznia kellett volna. A mintaperben hozott ítélettel szemben felülvizsgálati kérelmet nem nyújtottak be.

[5] A mintaperben hozott ítéletben foglaltakra figyelemmel az elsőfokú bíróság a többi, felfüggesztett pert folytatta, és a mintaperben hozott ítélet kötőerejére hivatkozva azzal azonos tartalmú ítéleteket hozott.

[6] A mintaperben hozott ítélet alapján meghozott jogerős ítéletek ellen az alperes felülvizsgálati kérelmeket nyújtott be, amelyekben a jogerős ítéletek hatályon kívül helyezését, az elsőfokú bíróság új eljárás lefolytatására és új határozat hozatalára utasítását kérte. Álláspontja szerint a bíróságok jogsértő eljárásai, különösen a kereseti kérelmen való túlterjeszkedés, az elkésett kereseti kérelem befogadása, a jogszabállyal ellentétes döntéshozatalra való kötelezés, a bizonyítási eljárás mellőzésével és felterjesztett közigazgatási iratanyag hiányában hozott döntések megalapozzák a felülvizsgálati eljárást. Az ítéletek az elbíráláskori és a jelenleg hatályos jogszabályokkal ellentétes eljárásrend alkalmazására utasítják.

[7] A Kúria az alperes felülvizsgálati kérelmeit a Kp. 118. § (1) bekezdés a) pont ad) alpontja alapján befogadta, a Kfv.37.355/2023. számon indult pernek a Kp. 33. § (1) bekezdése alapján mintaperként való elbírálásáról határozott, és erre tekintettel a tény- és jogazonos többi pert a mintaper elbírálásáig felfüggesztette.

III.

[8] Az Indítványozó tanács szerint a mintaperként elbírálandó Kfv.37.355/2023. számú perben a felülvizsgálati kérelem érdemi elbírálásának akadálya a Kúria BHGY-ban közzétett Kfv.37.471/2019/11. számú ítéletének [48] bekezdésében, a Kfv.37.472/2019/8. számú ítéletének [43] bekezdésében, a Kfv.37.473/2019/9. számú ítéletének [46] bekezdésében és a Kfv.37.481/2019/9. számú ítéletének [43] bekezdésében tett azon azonos megállapítás, miszerint „amennyiben pedig a jelen ügyben felülvizsgált ítéletet hozó bíróságnak követnie kellett a mintaper eredményét, akkor attól, az ezen ítélet jogszerűségét vizsgáló Kúria sem térhet el még akkor sem, ha a mintaper eredményét felülvizsgálattal a Kúrián nem támadták, és ekként a mintaperben hozott ítélet törvényességéről a Kúria nem foglalhatott állást".

[9] Az Indítványozó tanács álláspontja szerint az ügyazonosság fennáll, mert a közzétett ítéletek alapjául szolgáló esetekben és az előttük folyamatban lévő felülvizsgálati perekben is a Kp. 33. §-a alapján az elsőfokú bíróság előtt mintaper lefolytatására került sor földhasználattal kapcsolatos közigazgatási hatósági ügyben hozott közigazgatási határozat bírósági felülvizsgálata során.

[10] A korlátozott precedensrendszerből következően az Indítványozó tanács kötve van a fentiek szerinti azon állásponthoz, hogy amennyiben a mintaperben hozott ítéletet felülvizsgálati kérelemmel nem támadták meg, a mintapert követően, a mintaper kötőereje alapján meghozott jogerős ítéletek ellen benyújtott felülvizsgálati kérelmek nem bírálhatók el érdemben, mert a mintaperben hozott ítélet kötőereje a Kúriára is kiterjed anélkül, hogy annak jogszerűségét a Kúria felülvizsgálta, felülvizsgálhatta volna.

[11] Az Indítványozó tanácsnak a mintaper természetéből, joghatásaiból, a jogalkotó szándékából, valamint a tisztességes eljáráshoz és a jogorvoslathoz való jogból levont következtetései értelmében nem tartható fenn a közzétett döntésekben kifejtett álláspont.

[12] A Kp. 33. §-hoz fűzött indokolás alapján az Indítványozó tanács hangsúlyozta, hogy elkülönülő, önálló peres eljárásokról van szó. A mintaper eredménye alapján eldöntött többi peres eljárás a mintapertől független, mert a mintaper befejezését követően a felfüggesztett eljárások a mintaper eredménye szerint dönthetők el, de akár további bizonyítási eljárás is lefolytatható.

[13] Hangsúlyozta, hogy a mintaper nem egyenlő a próbaper intézményével, így a mintaperben hozott ítélet joghatása is eltérő attól. A mintaper jogintézményének célja, hogy a tömegével megjelenő, azonos ténybeli és jogi alapon nyugvó eljárások gyorsabbak, olcsóbbak és hatékonyabbak legyenek, miközben biztosítja a joggyakorlat egységesebbé válását is.

[14] Az Alaptörvény XXVIII. cikk (7) bekezdése és az Alkotmánybíróság döntései {14/2018. (IX. 27.) AB határozat [5], [17], 3223/2018. (VII. 2.) AB határozat [66], 36/2013. (XII. 5.) AB határozat, 14/2018. (IX. 27.) AB határozat [18]} alapján hangsúlyozta, hogy amennyiben azért nem lenne lehetőség a mintaperben hozott ítélet alapján hozott döntés kúriai felülvizsgálatára, mert a mintaperben hozott ítéletet rendkívüli perorvoslattal nem támadták, akkor lehetővé válna, hogy egy későbbi ügyben, de a mintaper ítélete alapján hozott döntést sem lehetne a Kúria előtt megmérettetni, kockáztatva ezzel, hogy jogszabályba ütköző vagy valamely alapelv (például a jogorvoslathoz való jog) sérelmét jelentő döntés válik a bírósági joggyakorlat részévé.

[15] Az Indítványozó tanács kiemelte, hogy mintaper nemcsak az azonos felek között folyamatban levő pereket érintően alakítható. Ez esetben a más felek között folyamatban levő perben a mintaperben hozott ítéletre tekintettel meghozott ítélet elleni felülvizsgálati kérelem érdemi elbírálásának kizártsága a fél jogorvoslathoz való jogát csorbítaná, megfosztaná attól, hogy az ügyében a jogegységért felelős Kúria döntését kérhesse.

[16] Utalt arra, hogy a Kúria más döntéseiben, így a Kfv.37.453/2021/16. számú ítélet [51]–[54] és [84] bekezdéseiben, a Kfv.37.382/2022/4. számú ítélet [35] és [51] bekezdéseiben, a Kfv.37.384/202264. számú ítélet [33] és

[48] bekezdéseiben, valamint a Kfv.37.388/2022/4. számú ítélet [18] és [42] bekezdéseiben a mintaperben hozott ítélet kötőerejét csak azon bírósági szintre nézve értelmezte, amely a mintaperben történő elbírálást elrendelte.

IV.

[17] A legfőbb ügyész a Bszi. 37. § (2) bekezdése alapján tett nyilatkozatában a Kp. 33. §-ához fűzött miniszteri indokolás, az Alkotmánybíróságnak a tényleges és hatékony jogorvoslati jog érvényesülésével kapcsolatos egyes döntései alapján, az Alaptörvény 28. cikke szerint irányadó jogértelmezésre figyelemmel leszögezte, hogy a mintaper célja a bíróságok eljárásának időszerűvé tétele és gyorsítása. A Kp. 33. §-ának szabályai a bizonyítékok értékelése és a mintaper jogi érvelése más perben való legitim felhasználhatóságának jogalapját teremti meg, e nélkül a bíróságnak erre perjogi lehetősége nem lenne.

[18] A mintaperbeli másodfokú eljárástól függetlenül biztosított a többi eljárásban a fellebbezés joga, ami azt is magában foglalja, hogy a rendes jogorvoslat során nincs kötve az esetlegesen eljáró másodfokú bíróság a mintaperben hozott ítélethez. A mintaperben hozott ítélet kötőerejéről ezért a felsőbb bíróság irányába nem beszélhetünk. A mintaperben alsóbb bírósági szinten hozott ítélet kötőereje tehát a Kúriára nem terjed ki, a felülvizsgálattal nem támadott mintaperben hozott ítélettől a Kúria eltérhet az annak alapján hozott ítéletek jogszerűségének felülvizsgálatára irányuló eljárásban.

V.

[19] A felperes nyilatkozata szerint nem indokolt az eltérés a Kúria BHGY-ban közzétett határozataitól. Amennyiben ugyanis az Indítványozó tanács általánosságban eltérhetne a mintaperben hozott ítélet alapján hozott további ítéletek kúriai felülvizsgálati eljárása során a mintaperben hozott – kúriai felülvizsgálati kérelem és alkotmányjogi panasz hiányában – anyagi jogerős ítéletben foglaltaktól, akkor egyrészt a mintaper intézménye teljességgel „kiüresedne", másrészt a res judicata elve, valamint a pergazdaságossági- és perkoncentráció elvei is sérülnének.

[20] Hangsúlyozta, hogy a peres felek nem vitatták a mintaper alkalmazásának jogszerűségét, ezzel elfogadták a mintaper sajátosságából fakadó jogkövetkezményeket is. A jogorvoslati jog a peres felek oldalán nem üresedett ki, csupán a mintaper sajátosságaiból fakadóan korlátozódott oly módon, hogy a mintaper vonatkozásában a felülvizsgálati jogorvoslati jognak elenyészése (elmulasztása) kihatott a további, a mintaperben hozott döntés alapján meghozott további perekben született döntésekre is.

[21] Az alperes nyilatkozatában egyetértett az előzetes döntéshozatali indítványban kifejtett álláspontt al, amely szerint a mintaperben hozott ítélet a felülvizsgálati eljárásban eljáró Kúriára nem bír kötőerővel, és nem zárható el a fél a felülvizsgálati kérelme érdemi elbírálásától azon az alapon, hogy a mintaperben hozott ítélet ellen nem nyújtottak be felülvizsgálati kérelmet. Egyetértett azzal a megállapítással is, miszerint nem tehető különbség abban a vonatkozásban, hogy azonos vagy különböző felek között folyó pereket érinti a mintaperré alakítás és a mintaperben való elbírálás.

[22] Az alperes hivatkozott az Alaptörvény XXVIII. cikk (7) bekezdésére, álláspontja szerint a jogorvoslathoz való jog korlátozását jelentené az a jogértelmezés, amely szerint a mintaperrel érintett többi perben érintett peres fél sem terjeszthet elő felülvizsgálati kérelmet, akkor ha a mintaperben meghozott ítélet ellen nem nyújtanak be felülvizsgálati kérelmet. Utalt továbbá arra, hogy a Kp. 33. § (2) bekezdése szerint a mintaper bizonyítási eredményének felhasználása nem akadálya további bizonyítás elrendelésének, amely bizonyítás adott esetben olyan eredményre vezethet, aminek következtében az adott ügyet elbíráló bírói tanácsnak a mintaperben meghozott ítélettől eltérő álláspontra kell helyezkednie. Mindezekre tekintettel az alperes álláspontja szerint indokolt lehet az eltérés az indítványban megjelölt határozatoktól.

VI.

[23] A Jogegységi Panasz Tanács a következőkre alapozta döntését.

[24] Kp. 33. § (1) Ha a bíróság előtt legalább tíz olyan eljárás indul, amelyek jogi és ténybeli alapja azonos, a bíróság dönthet arról, hogy e perek egyikét mintaperben bírálja el, és a többi eljárást az eljárást befejező határozata meghozataláig felfüggeszti.

(2) A bíróság a felfüggesztett eljárásokat a mintaper eredménye szerint, tárgyaláson kívül bírálhatja el, ha azt állapítja meg, hogy azok a mintapertől sem jogi, sem ténybeli szempontból nem különböznek. A mintaper bizonyítási eredményének felhasználása nem akadálya a további bizonyítás elrendelésének.

(3) A bíróság a mintaperben hozott ítélet jogerőre emelkedését követően indult, az (1) bekezdés szerinti jogvitát is e § szabályai szerint bírálhatja el.

[25] A Kp. 33. §-ához fűzött miniszteri indokolás szerint a mintaper új elem a közigazgatási perjogban. A rendelkezés célja az olyan jogviták gyorsabb kezelése, ahol azonos ténybeli alapon, azonos jogi helyzet mellett kell a bíróságnak számos ügyben párhuzamosan döntést hozni, és ennek érdekében tartalmilag szinte azonos eljárási cselekményeket megtenni. Az ilyen eljárások gyorsabb elbírálása érdekében a perrendtartás lehetőséget ad a bírónak arra, hogy egy eljárást annak mintaperré minősítése révén, mintegy előzetesen lefolytasson, s az ott nyert bizonyítékokat és jogértelmezési eredményt a többi eljárásban felhasználva döntsön. A többi per felfüggesztése a mintaper befejezéséig lehetséges, ezt követően a felfüggesztett eljárásokat – ha ismét meggyőződött a tény- és jogbeli azonosságról – tárgyaláson kívül is elbírálhatja. Döntése szerint azonban ekkor is folytathat bizonyítást, a mintaper eredményéhez tehát nincs kötve. A mintaperbeli másodfokú eljárástól függetlenül lesz joga fellebbezést benyújtani a mintaperben hozott ítélet nyomán hozott ítélettel szemben az arra jogosultnak [Indokolás a T/12243. számú törvényjavaslathoz (Kp. Indokolás)].

[26] A mintaper az egyszerre nagyobb számban jelentkező, azonos ténybeli és jogi alapon álló perek koncentrált, gyorsabb, hatékonyabb elintézésére ad lehetőséget, hozzájárul a joggyakorlat egységességéhez és megkönnyíti a bíróságra nehezedő terheket. A mintaper a felek számára is jó megoldás lehet, hiszen az ügy mielőbbi befejezését biztosítja. Előnyös azért is, mert kiszámíthatóvá teszi a döntést, amelyre figyelemmel a felperes olcsóbb megoldásként el is állhat keresetétől. A fél attól sincs elzárva, hogy pernyertessége érdekében újabb bizonyítást indítványozzon.

[27] Az Alaptörvény XXVIII. cikkének (7) bekezdése szerint mindenkinek joga van ahhoz, hogy jogorvoslattal éljen az olyan bírósági, hatósági és más közigazgatási döntés ellen, amely a jogát vagy jogos érdekét sérti.

[28] Az Alkotmánybíróság a 14/2015. (V. 26.) AB határozat [16] bekezdésében kimondta, hogy az Alkotmánybíróság következetes gyakorlata szerint a jogorvoslathoz való jog lényegi tartalma az érdemi határozatok tekintetében a más szervhez, vagy ugyanazon szervezeten belüli magasabb fórumhoz fordulás lehetősége {Lásd: 5/1992. (I. 30.) AB határozat, ABH 1992, 27, 31.; megerősítve: 35/2013. (XI. 22.) AB határozat, Indokolás: [16]}. Az Alaptörvényben biztosított jogorvoslathoz való jog a tényleges és hatékony jogorvoslat lehetőségének a biztosítását követeli meg, így nemcsak abban az esetben állapítható meg az alapjog sérelme, ha a jogorvoslat lehetőségét teljesen kizárták {lásd például: 36/2013. (XII. 5.) AB határozat, Indokolás [61]}, hanem akkor is, ha a jogszabályban egyébként biztosított jogorvoslat más okból nem tud ténylegesen és hatékonyan érvényesülni, így például, ha azt a részletszabályok rendelkezései akadályozzák meg, ezáltal üresítve ki, illetve téve formálissá a jogorvoslathoz való jogot [lásd: 41/1991. (VII. 3.) AB határozat, ABH 1991, 193, 194.; 22/1991. (IV. 26.) AB határozat, ABH 1991, 408, 411.; 21/1997. (III. 26.) AB határozat, ABH 1997, 103, 105–106.].

[29] Az Alkotmánybíróság a 3064/2014. (III. 26.) AB határozat [15] bekezdésében rögzítette, az Alaptörvény megköveteli, hogy a jogorvoslati jog nyújtotta jogvédelem hatékony legyen, vagyis ténylegesen érvényesüljön és képes legyen a döntés által okozott sérelem orvoslására. A jogorvoslat jogának hatékony érvényesülését számos tényező befolyásolhatja, így többek között a felülbírálati lehetőség terjedelme, a jogorvoslat elintézésére meghatározott határidő, vagy a sérelmezett határozat kézbesítésének szabályai és megismerhetőségének lehetősége {22/2013. (VII. 19.) AB határozat, Indokolás [26]}. Minden jogorvoslat lényegi, immanens eleme továbbá a jogorvoslás lehetősége, vagyis a jogorvoslat fogalmilag és szubsztanciálisan tartalmazza a jogsérelem orvosolhatóságát [23/1998. (VI. 9.) AB határozat, ABH 1998, 182, 186.].

[30] A jogviták mintaperben vagy mintaperben hozott ítélet alapján való elbírálása nyilván nem járhat az alkotmányos alapjognak, a jogorvoslathoz való jognak a sérelmével, korlátozásával, elenyészésével.

[31] A Kp. 33. §-a a jogorvoslathoz való jogról nem rendelkezik, a Kp. jogorvoslatokkal kapcsolatos része a mintaperben hozott vagy mintaper alapján hozott ítéletekkel összefüggésben eltérő szabályt, kivételt nem ad. Ahogy azt a Kp. 33. §-ához fűzött indokolás is tartalmazza, a mintaperbeli másodfokú eljárástól függetlenül van joga fellebbezést benyújtani az arra jogosultnak a mintaperben hozott ítélet alapján hozott ítélettel szemben. Bár a Kp. időközbeni módosítása folytán a közigazgatási perekben nincs általános lehetőség az elsőfokú ítéletekkel szembeni fellebbezésre, azonban a Kp. 115. § (2) bekezdése értelmében a fellebbezés szabályait a felülvizsgálatra is alkalmazni kell. A mintaperben hozott ítélet alapján hozott ítéletek tekintetében tehát az általános szabályok szerint helye van felülvizsgálatnak, mégpedig – kizáró törvényi rendelkezés hiányában – akkor is, ha a mintaperben hozott ítélet ellen felülvizsgálati kérelmet nem terjesztettek elő.

[32] A Jogegységi Panasz Tanács megítélése szerint a mintaperben hozott ítéletet követően lefolytatott többi eljárásban a feleket nemcsak az elállás vagy a további bizonyítás joga illeti meg, hanem az is, hogy a saját ügyükben hozott ítélettel szemben az általános szabályok szerint ugyanúgy éljenek jogorvoslattal, ahogy a nem mintaper

alapján hozott ítélettel szemben. Ez a jogorvoslat nem lehet formális, nem lehet korlátozott tartalmú pusztán azért, mert a mintaperben hozott ítélettel szemben nem éltek jogorvoslattal az arra jogosultak. Ugyanígy nem befolyásolja a jogorvoslati jog gyakorlását az, hogy a többi, felfüggesztett perekben hozott ítélettel szemben éltek-e jogorvoslattal, avagy sem. A jogorvoslat lehetősége a Kp. szerint meghatározott körben megilleti a peres eljárás résztvevőit, a mintaperben hozott ítélet elleni felülvizsgálat elmaradása nem hat ki a mintaperben hozott ítélet alapján hozott további döntésekre. Az ítélt dolog *(res judicata)* elve nem érvényesülhet egy másik, akár más személyek között folyamatban lévő ügyben. A mintaperrel elérni kívánt hatékonysági, pergazdaságossági szempontok és a perkoncentráció elve az alkotmányos alapjogot nem írja felül, erre figyelemmel a jogorvoslat nem üresedhet ki.

[33] A mintaperben hozott határozat ennél erősebb joghatásához, ahhoz, hogy annak jogereje kihasson a felfüggesztett eljárásokban hozott későbbi határozatokra, a Kp. szabályainak módosítása lenne szükséges. Ebben az esetben ugyanis a felfüggesztett eljárások felperesei, alperesei és érdekeltjei számára jogorvoslatot kellene biztosítani a mintaperben hozott határozattal szemben annak érdekében, hogy a mintaperben hozott határozat jogereje a saját ügyükben őket megillető jogorvoslati jogot ne vonja el teljesen. Ez a joghatás bírósági értelmezéssel nem biztosítható, ahhoz a jogszabálynak kellene másként rendelkeznie.

[34] A BHGY-ban közzétett, az Indítványozó tanács által megjelölt eseti döntések a fenti következtetésekkel ellentétes megállapítást tartalmaznak, a Kp. 33. §-ából nem vezethető le, hogy a mintaperben hozott ítélet nyomán hozott ítélet jogszerűségét vizsgáló Kúria a felülvizsgálati eljárásban kötve van a mintaperben hozott ítélet eredményéhez, még akkor is, ha a mintaperben hozott ítéletet a Kúrián felülvizsgálattal nem támadták. Az ettől eltérő megállapításon alapuló kúriai gyakorlat nem tartható fenn, ezért a megjelölt határozatokban szereplő jogértelmezéstől az Indítványozó tanács eltérhet.

VII.

[35] Mindezekre figyelemmel a Jogegységi Panasz Tanács a Bszi. 24. § (1) bekezdés c) pontja, a 25. §-a, a 32. § (1) bekezdés b) pontja, a 34. §-a, továbbá a 40. § (1) és (2) bekezdése alapján, a bíróságok jogalkalmazása egységének biztosítása érdekében [Alaptörvény 25. cikk (3) bekezdés] a rendelkező részben foglaltak szerint határozott.

[36] A Jogegységi Panasz Tanács a Bszi. 42. § (1) bekezdése alapján a jogegységi határozatot a Magyar Közlönyben, a BHGY-ban, a bíróságok központi internetes honlapján és a Kúria honlapján közzéteszi. A jogegységi határozat a bíróságokra a Magyar Közlönyben történő közzététel időpontjától kötelező.

[37] A jogegységi határozat a bíróságokra a Magyar Közlönyben történő közzététel időpontjától kötelező. Ettől az időponttól kezdve a Kúria BHGY-ban közzétett Kfv.37.471/2019/11. számú ítélete indokolásának [48] bekezdésében, a Kfv.37.472/2019/8. számú ítélete indokolásának [43] bekezdésében, a Kfv.37.473/2019/9. számú ítélete indokolásának [46] bekezdésében, a Kfv.37.481/2019/9. számú ítélete indokolásának [43] bekezdésében, továbbá a Kfv.37.483/2019/9. számú ítélete indokolásának [40] bekezdésében foglalt és más hasonló jogértelmezés kötelező erejűként nem hivatkozható.

Budapest, 2024. május 6.

Dr. Varga Zs. András s.k. a tanács elnöke, Dr. Vitál-Eigner Beáta s.k. előadó bíró, Böszörményiné dr. Kovács Katalin s.k. bíró, Dr. Farkas Katalin s.k. bíró, Dr. Kalas Tibor s.k. bíró, Dr. Gimesi Ágnes Zsuzsanna s.k. bíró, Dr. Gyarmathy Judit s.k. bíró, Dr. Kövesné dr. Kósa Zsuzsanna s.k. bíró, Dr. Magyarfalvi Katalin s.k. bíró, Dr. Márton Gizella s.k. bíró, Molnár Ferencné dr. s.k. bíró, Dr. Orosz Árpád s.k. bíró, Dr. Varga Zs. András s.k. a tanács elnöke az aláírásban akadályozott Dr. Puskás Péter bíró helyett, Salamonné dr. Piltz Judit s.k. bíró, Dr. Somogyi Gábor s.k. bíró, Dr. Suba Ildikó s.k. bíró, Dr. Szabó Klára s.k. bíró, Dr. Stark Marianna s.k. bíró, Dr. Tóth Kincső s.k. bíró

Dr. Tóth Kincső bíró többségi határozattól eltérő álláspontja

[38] A Bszi. 41/A. § (3) bekezdése alapján és a KÜSZ 32. § (3) bekezdése szerinti határidőben – tisztelettel – az alábbi többségi határozattól eltérő álláspontot terjesztem elő.

[39] Nem értek egyet a többségi határozatban foglaltakkal, különösen két okra figyelemmel:

1.

[40] Álláspontom szerint a Kúria Jogegységi Panasz Tanácsa e döntésével kiüresíti a mintaper intézményét. Elismerem, hogy a szabályozás hiányos és joggal vet fel kételyeket. Ugyanakkor véleményem szerint lett volna lehetőség arra, hogy a Jogegységi Panasz Tanács olyan jogértelmezést fogadjon el, amellyel megfogalmazza a közigazgatási perrendtartás egyik sajátos jogintézményével kapcsolatos kritikáit, egyúttal felhívja a szabályozás hibájára a figyelmet, de jogértelmezésével nem szünteti meg a jogintézmény alkalmazásának minden értelmét. Állítom, hogy a jogorvoslati jog biztosításán nyugvó jogértelmezés bizonyos esetekben nem jogvédelemhez, hanem a jogorvoslati joggal való visszaéléshez vezet. Ezeket az esetek a Jogegységi Panasz Tanács nem tárta fel.

[41] Álláspontom szerint jelentős különbség van az egyes mintaperek között atekintetben, hogy a legalább tíz közigazgatási per ugyanazon felek között, vagy más felek, esetleg egyéb érdekeltek részvételével zajlik, illetve teljesen azonos ténybeli és jogi alapon zajlanak az eljárások vagy esetleg vannak eltérések. Az nem vitatható, hogy a jogorvoslati jog biztosítása minden esetben elengedhetetlen, ha olyan személyek érintettek a mintaperi ítélet nyomán hozott ítéletekben, akik nem voltak a mintaperben az eljárás résztvevői. E körben valóban jogalkotással lehetne a jogintézményt teljes egészében fenntartani.

[42] Ugyanakkor a többségi határozat jogértelmezési elveit nem tartom indokoltnak, mert a jogorvoslati joggal való visszaélésre ad alapot, ha ugyanazon felek között, ugyanazon tények és jogi hivatkozások mentén zajlik a mintaper és az összes, mintaperre felfüggesztett közigazgatási per. Ebben az esetben, ha a mintaperi ítélet ellen egyik peres fél sem kezdeményez felülvizsgálati eljárást, akkor lényegében belenyugszik a mintaítéletben foglaltakba és egyúttal tudomásul veszi (természetesen megfelelő bírói kioktatás mellett), hogy a mintaperre felfüggesztett valamennyi perükben ugyanezt a döntést fogják meghozni, feltéve, hogy újabb jogi hivatkozások vagy újabb tények – akár bizonyítás útján – nem merülnek fel. Nem látom annak valós (akár alapjogi) okát, hogy miért ne lehetne a mintaperi ítélet kötőerejéről beszélni az ugyanazon felek közötti, ténybelileg és jogilag teljesen azonos ügyekben. Itt nem merülhet fel az a kérdés, hogy a mintaperben ne tudták volna a peres felek érveiket előadni, esetleg jogorvoslati jogukkal teljeskörűen élni. Ezekben az ügyekben a később már a pertaktika része lehet a jogorvoslati kérelem előterjesztése, az esetleges – mintaperből már jól ismert – kötelezettségek teljesítésének elodázására törekedhetnek a felek. Ezt az esetkört és a tőle – kisebb vagy nagyobb mértékben – eltérő esetköröket ki kellett volna elemezni az alapjogi védelem szempontjából, ez azonban elmaradt.

2.

[43] Álláspontom szerint e többségi határozatban ki kellett volna arra is térni, hogy miként lehet fenntartani az 1/2021. KJE határozat [33] bekezdés szerinti indokolását.

[44] A Kúria Közigazgatási Kollégiuma 1/2021. KJE határozatának [33] bekezdésében kimondta, hogy „[…] *Tény és jogbeli azonosság esetén ugyanis a mintaper eredménye a további perekben is irányadó, attól eltérni nem lehet. A mintaper kötőereje a bíróság által – kérelemre vagy hivatalból – tett érdemi megállapításokra, jogi következtetésekre korlátozódik.*"

[45] E jogegységi határozatban – 3 évvel ezelőtt – az elsőfokú bírók számára követelményként fogalmazódott meg, hogy – eltérő peres felek, érdekeltek személyétől függetlenül is – követniük kell a mintaperi ítéletet, attól nem térhetnek el, ha a ténybeli és jogi azonosság fennáll (értsd helyesen: ha a mintaperi ítélet meghozatalát követően folytatott, mintaperre figyelemmel felfüggesztett közigazgatási perekben nem folyt le bizonyítás új tényekre, és nem volt újabb vagy más jogi hivatkozás mint a mintaperben.). A Kúria a többségi határozatban lényegében azt mondja ki, hogy ha az elsőfokú bíróság a mintaperi ítélet alapján dönt, kötőerejét értékelve ítélkezik, akkor ítélete a mintaítélet törvénysértő volta miatt minden további nélkül törvénysértő (még akkor is, ha ugyanazon felek között, ugyanazon tények és jogi hivatkozások elbírálására került sor). Ha a Kúria a többségi döntés nyomán az anyagi jogerővel rendelkező mintaítélethez nincs kötve, és arról megállapíthatja (igaz burkoltan), hogy az jogszabálysértő, téves, akkor felmerül a kérdés, mi értelme van a mintaítélet 1/2021. KJE határozattal kimondott kötőerejének.

[46] Véleményem szerint a mintaítélet az 1/2021. KJE határozat [33] bekezdése és a Kp. 33. § (2)–(3) bekezdése alapján többlettartalommal bír egy „átlagos" (értsd úgy, hogy más, de nem mintaperben, ügyazonosság mellett meghozott) jogerős ítéletnél. A többségi határozat a mintaperi ítéletet „átlagos" jogerős ítéletté minősítette.

[47] Itt kell utalni arra, hogy egy első fokon jogerős ítélet is szolgálhat mintául egy hozzá ténybeli és jogi alapon azonosnak minősülő ügyben. Ez az „átlagos" jogerős ítélet észszerűen kötőerővel nem bír, de megkönnyíti az elsőfokú bíróság későbbi döntéshozatalát, segíti az egységes jogértelmezést. Ahogy a mintaperi ítélet is teszi, szolgálja a jogegység kialakítását. Ugyanakkor az „átlagos" jogerős ítélet nem jár azzal a következménnyel, hogy a későbbi, vele ténybelileg és jogilag azonos ügyben más eljárási szabályok érvényesüljenek. A Kp. 33. § (3) bekezdése azonban a mintaperi ítélethez ilyen különös eljárási felhatalmazást társít: *„A bíróság a mintaperben hozott ítélet jogerőre emelkedését követően indult, az (1) bekezdés szerinti jogvitát is e § szabályai szerint bírálhatja el."* Azaz lehetővé teszi a tárgyaláson kívüli elbírálást, sőt az egész eljárás egyszerűsítését, a korábbi bizonyítási eljárás eredményének felhasználását (megjegyzem egy olyan peréét, amelyről a későbbi felperes nem is tudhatott). E szabály és az 1/2021. KJE határozat [33] bekezdésében foglalt kötelezettség számomra azt jelenti, hogy a mintaperi ítélet valami többlettartalommal bír az „átlagos" jogerős ítélethez képest, amit ez a többségi határozat nem keresett meg és nem azonosított.

Budapest, 2024. május 21.

Dr. Tóth Kincső s.k. bíró

IX. Határozatok Tára

A Kormány 1182/2024. (VI. 24.) Korm. határozata az anyatejgyűjtő állomások országos kiterjesztéséről

A Kormány

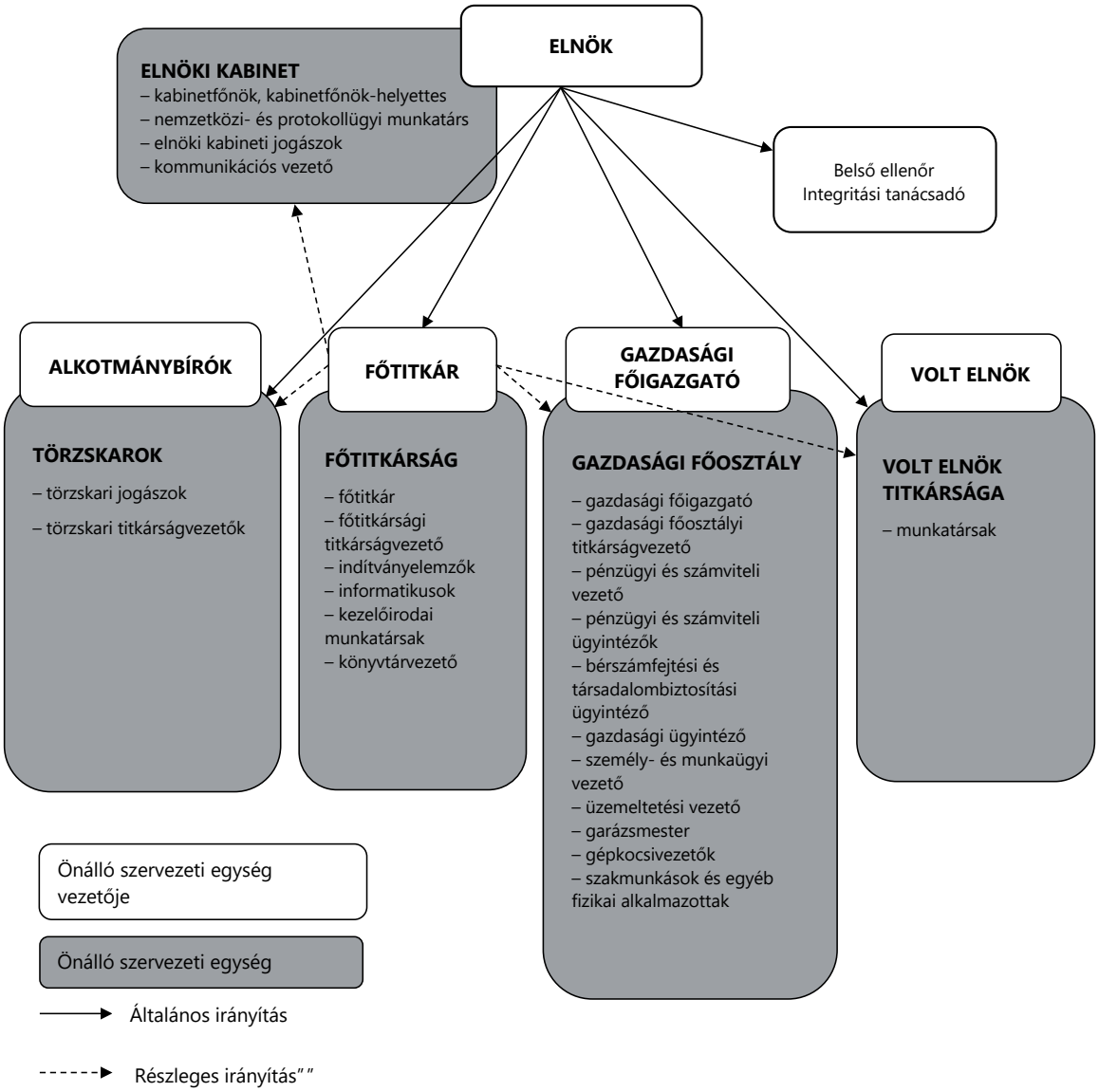
1. elkötelezett a gyermekközpontú és családbarát értékrend mellett, ennek megfelelően támogatja, hogy minden rászoruló kora- és újszülött, valamint csecsemő egyenlő eséllyel hozzáférjen a megfelelő táplálásához szükséges donor anyatejhez;
2. az 1. pontban foglalt célok elérése érdekében
   a) felhívja a belügyminisztert, hogy – a kultúráért és innovációért felelős miniszterrel együttműködve – készítsen részletes szabályozási javaslatot az anyatejgyűjtő állomások tartós működési és jogszabályi feltételeinek felülvizsgálatára, ideértve a finanszírozási szabályok módosítását is,
      Felelős: belügyminiszter
      kultúráért és innovációért felelős miniszter
      Határidő: 2024. október 31.
   b) felhívja a belügyminisztert, hogy – a pénzügyminiszterrel történő előzetes egyeztetés eredménye alapján – a kultúráért és innovációért felelős miniszter bevonásával dolgozza ki minden vármegyére kiterjedően az anyatejgyűjtő állomások országos rendszerének koncepcióját, és vizsgálja felül az infrastruktúra kiépítésének, valamint megújításának lehetőségét,
      Felelős: belügyminiszter
      pénzügyminiszter
      kultúráért és innovációért felelős miniszter
      Határidő: 2025. március 31.
   c) felhívja a belügyminisztert, valamint a kultúráért és innovációért felelős minisztert, hogy intézkedjenek a szoptatás, anyatejes táplálás népszerűsítése és a donor anyatej leadásának ösztönzése érdekében,
      Felelős: belügyminiszter
      kultúráért és innovációért felelős miniszter
      Határidő: 2025. december 31.
   d) felhívja a belügyminisztert, valamint a kultúráért és innovációért felelős minisztert, hogy gondoskodjanak a Nemzeti Anyatejbank keretén belül egy egységes nyilvántartó informatikai rendszer terveinek kialakításáról.
      Felelős: belügyminiszter
      kultúráért és innovációért felelős miniszter
      Határidő: 2026. december 31.

Orbán Viktor s. k.,
miniszterelnök

Helyesbítés

A Magyar Közlöny 2024. június 20-án megjelent 67. számában közzétett, az Alkotmánybíróság Szervezeti és Működési Szabályzatáról szóló 1004/2020. (IV. 30.) AB Tü. határozatának módosításáról szóló 1002/2024. (VI. 20.) AB Tü. határozat 1. melléklete – a jelzett közlönyszám 4068. oldalán – helyesen a következő:

„1. melléklet az 1002/2024. (VI. 20.) AB Tü. határozathoz
„1. melléklet az 1004/2020. (IV. 30.) AB Tü. határozathoz



A Magyar Közlönyt az Igazságügyi Minisztérium szerkeszti.
A szerkesztésért felelős: dr. Bíró Attila.
A szerkesztőség címe: 1051 Budapest, Nádor utca 22.
A Magyar Közlöny hiteles tartalma elektronikus dokumentumként a https://www.magyarkozlony.hu honlapon érhető el.