MINISZTERELNÖKI KABINETIRODÁT VEZETŐ MINISZTER

Közli: Magyar Közlöny

A Miniszterelnöki Kabinetirodát vezető miniszter

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) 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. § 2024. október 18-án 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.

1. melléklet a …/2023. (…..) 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 biztonság-felügyeleti 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,

1.1.1.2.3. 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 üzembehelyezésére 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. pontok 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,

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,

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,

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 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 a 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 teljeskörű 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 pontok 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 …/2023. (…..) 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 jellemzőket. 2.18.4. Kiválaszthatja az újonnan létrehozott vagy módosított objektumokhoz rendelt biztonsági jellemzőket. 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 hozzáférés-szabályozással 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 jellemzők 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 jellemzőket.	-	-	-

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 – Hálózati 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 az elektronikus információs 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 rendszerelemek hatékony elszámolását beleértve. 6.36.2. Meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelemek leltárát.	X	X	X
38.	6.37. Rendszerelem leltár – Frissítések a telepítés és eltávolítás során	6.37. A szervezet az elektronikus információs 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 az elektronikus információs 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 az elektronikus információs 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 az elektronikus információs 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 az elektronikus információs rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani, olyan ellenőrzött konfigurációból és sértetlenségvédett információkból, amelyek az elem ismert működési állapotát reprezentálják.	-	-	X
47.	7.46. Az elektronikus információs rendszer helyreállítása és újraindítása – Rendszerelem védelem	7.46. A szervezet védi azokat az elektronikus információs 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 biztonságosüzemmódra	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 elektronikus információs 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 helyt 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 helyt 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 helyt 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 elektronikus információs 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 alkalmazza 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 helyt 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 helyt 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 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 helyt 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 architektúrális 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. A 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 elteltidőt. 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. Előrelátható 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. Előrelátható 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 …/2023. (…..) 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 szofverek (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