<Rendszer neve>

rendszerbiztonsági terve

Verzió: <#.#>

Dátum: <dátum>

**A Dokumentum Adatai**

|  |  |
| --- | --- |
| **Cím** | <Rendszer neve> rendszerbiztonsági terve  |
| **Leírás** | A rendszer műszaki felépítésének, paramétereinek, szervezeti és technológiai környezetének bemutatása, biztonsági osztályának meghatározása és a rendszerrel kapcsolatos védelmi intézkedések megvalósításának leírása. |

**Változatok**

|  |  |  |  |
| --- | --- | --- | --- |
| **Kiadás dátuma** | **Szerző** | **Verzió** | **Leírás** |
| 2025.XX.XX |  | 1.0 | Első változat |
|  |  |  |  |

[*Jelen dokumentum egy sablon, amely a rendszerbiztonsági tervhez kapcsolódó alapkövetelményeket határozza meg, annak fejezeteit rögzíti, és rövid tartalommal segíti az egyes fejezetekhez kapcsolódó elvárások körvonalazását. A [ ] zárójelek közötti útmutató részek a sablon kitöltésekor törölhetők.*]

Tartalomjegyzék

[1 Bevezetés 6](#_Toc191366975)

[1.1 A dokumentum célja 6](#_Toc191366976)

[1.2 Fogalmak és rövidítések definíciója 6](#_Toc191366977)

[2 A rendszer átfogó ismertetése 7](#_Toc191366978)

[2.1 Megnevezés 7](#_Toc191366979)

[2.2 A rendszer célja, hatóköre 7](#_Toc191366980)

[2.3 A rendszer alapfeladatait biztosító modulok 7](#_Toc191366981)

[2.4 A rendszer jelenlegi státusza 8](#_Toc191366982)

[2.5 A rendszer típusa 8](#_Toc191366983)

[3 Szervezeti feladatok és felelősségek elhatárolása 8](#_Toc191366984)

[3.1 Engedélyezésért felelős vezető 9](#_Toc191366985)

[3.2 Rendszertulajdonos 9](#_Toc191366986)

[3.3 Adatgazda 10](#_Toc191366987)

[3.4 Informatikai vezető 10](#_Toc191366988)

[3.5 Információbiztonsági felelős 11](#_Toc191366989)

[3.6 Üzemeltetésbiztonsági felelős 11](#_Toc191366990)

[3.7 Rendszer üzemeltetési felelősségek 12](#_Toc191366991)

[3.8 Végfelhasználók és privilegizált felhasználók száma 12](#_Toc191366992)

[4 Biztonsági osztályba sorolás 12](#_Toc191366993)

[4.1 A rendszer által kezelt és tárolt adatok 12](#_Toc191366994)

[4.2 A rendszer biztonsági osztálya 13](#_Toc191366995)

[5 A <Rendszer neve> műszaki megoldásainak bemutatása 13](#_Toc191366996)

[5.1 A <Rendszer neve> főbb elemei és adatkapcsolatai 13](#_Toc191366997)

[5.1.1 A rendszer főbb moduljai, alrendszerei 13](#_Toc191366998)

[5.1.2 Rendszer környezete és határai 13](#_Toc191366999)

[5.2 Rendszer logikai felépítésének bemutatása 14](#_Toc191367000)

[5.2.1 A rendszer topológiája 14](#_Toc191367001)

[5.2.2 A rendszer hardver környezetének összefoglaló bemutatása 14](#_Toc191367002)

[5.2.3 A rendszer szoftver környezetének összefoglaló bemutatása 14](#_Toc191367003)

[5.2.4 A rendszer kapcsolatainak összefoglaló bemutatása 15](#_Toc191367004)

[5.3 Portok, protokollok és szolgáltatások 15](#_Toc191367005)

[5.4 A rendszer fizikai környezete 15](#_Toc191367006)

[6 Alapvető biztonsági események meghatározása 15](#_Toc191367007)

[7 Kapcsolódó dokumentumok 15](#_Toc191367008)

[7.1 Kapcsolódó jogszabályok, megfelelés elvárások 15](#_Toc191367009)

[7.2 Kapcsolódó szabályzatok és dokumentumok 16](#_Toc191367010)

[8 Védelmi intézkedések megvalósítása 16](#_Toc191367011)

[8.1 HOZZÁFÉRÉS-FELÜGYELET 16](#_Toc191367012)

[8.1.1 Szabályzat és eljárásrendek 16](#_Toc191367013)

[8.1.2 Fiókkezelés 17](#_Toc191367014)

[8.1.3 Hozzáférési szabályok érvényesítése 18](#_Toc191367015)

[8.1.4 Sikertelen bejelentkezési kísérletek 18](#_Toc191367016)

[8.1.5 A rendszerhasználat jelzése 18](#_Toc191367017)

[8.1.6 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek 19](#_Toc191367018)

[8.1.7 Távoli hozzáférés 19](#_Toc191367019)

[8.1.8 Vezeték nélküli hozzáférés 20](#_Toc191367020)

[8.1.9 Mobil eszközök hozzáférés-ellenőrzése 20](#_Toc191367021)

[8.1.10 Külső elektronikus információs rendszerek használata 20](#_Toc191367022)

[8.1.11 Nyilvánosan elérhető tartalom 21](#_Toc191367023)

[8.2 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG 21](#_Toc191367024)

[8.2.1 Szabályzat és eljárásrendek 21](#_Toc191367025)

[8.2.2 Naplózható események 22](#_Toc191367026)

[8.2.3 Naplóbejegyzések tartalma 22](#_Toc191367027)

[8.2.4 Naplózás tárkapacitása 23](#_Toc191367028)

[8.2.5 Naplózási hiba kezelése 23](#_Toc191367029)

[8.2.6 Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel 24](#_Toc191367030)

[8.2.7 Időbélyegek 24](#_Toc191367031)

[8.2.8 Naplóinformációk védelme 24](#_Toc191367032)

[8.2.9 A naplóbejegyzések megőrzése 25](#_Toc191367033)

[8.2.10 Naplóbejegyzések létrehozása 25](#_Toc191367034)

[8.3 ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS 25](#_Toc191367035)

[8.3.1 Szabályzat és eljárásrendek 25](#_Toc191367036)

[8.3.2 Biztonsági értékelések 26](#_Toc191367037)

[8.3.3 Biztonsági értékelések – Kiberbiztonsági audit 27](#_Toc191367038)

[8.3.4 Információcsere 27](#_Toc191367039)

[8.3.5 Az intézkedési terv és mérföldkövei 27](#_Toc191367040)

[8.3.6 Engedélyezés 28](#_Toc191367041)

[8.3.7 Folyamatos felügyelet 28](#_Toc191367042)

[8.3.8 Folyamatos felügyelet – Kockázatmonitorozás 29](#_Toc191367043)

[8.3.9 Belső rendszerkapcsolatok 29](#_Toc191367044)

[8.4 KONFIGURÁCIÓKEZELÉS 30](#_Toc191367045)

[8.4.1 Szabályzat és eljárásrendek 30](#_Toc191367046)

[8.4.2 Alapkonfiguráció 30](#_Toc191367047)

[8.4.3 Biztonsági hatásvizsgálatok 31](#_Toc191367048)

[8.4.4 A változtatásokra vonatkozó hozzáférés korlátozások 31](#_Toc191367049)

[8.4.5 Konfigurációs beállítások 31](#_Toc191367050)

[8.4.6 Legszűkebb funkcionalitás 32](#_Toc191367051)

[8.4.7 Rendszerelem leltár 32](#_Toc191367052)

[8.4.8 A szoftverhasználat korlátozásai 33](#_Toc191367053)

[8.4.9 Felhasználó által telepített szoftver 33](#_Toc191367054)

[8.5 KÉSZENLÉTI TERVEZÉS 33](#_Toc191367055)

[8.5.1 Szabályzat és eljárásrendek 33](#_Toc191367056)

[8.5.2 Üzletmenet-folytonossági terv 34](#_Toc191367057)

[8.5.3 A folyamatos működésre felkészítő képzés 35](#_Toc191367058)

[8.5.4 Az elektronikus információs rendszer mentései 35](#_Toc191367059)

[8.5.5 Az elektronikus információs rendszer helyreállítása és újraindítása 36](#_Toc191367060)

[8.6 AZONOSÍTÁS ÉS HITELESÍTÉS 36](#_Toc191367061)

[8.6.1 Szabályzat és eljárásrendek 36](#_Toc191367062)

[8.6.2 Azonosítás és hitelesítés 37](#_Toc191367063)

[8.6.3 Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése 37](#_Toc191367064)

[8.6.4 Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem 37](#_Toc191367065)

[8.6.5 Azonosító kezelés 38](#_Toc191367066)

[8.6.6 A hitelesítésre szolgáló eszközök kezelése 38](#_Toc191367067)

[8.6.7 A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés 39](#_Toc191367068)

[8.6.8 Hitelesítési információk visszajelzésének elrejtése 39](#_Toc191367069)

[8.6.9 Hitelesítés kriptográfiai modul esetén 39](#_Toc191367070)

[8.6.10 Azonosítás és hitelesítés (szervezeten kívüli felhasználók) 40](#_Toc191367071)

[8.6.11 Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata 40](#_Toc191367072)

[8.6.12 Újrahitelesítés 40](#_Toc191367073)

[8.7 KOCKÁZATKEZELÉS 41](#_Toc191367074)

[8.7.1 Sérülékenységek ellenőrzése 41](#_Toc191367075)

[8.7.2 Sérülékenységmenedzsment – Sérülékenységi információk fogadása 41](#_Toc191367076)

[8.7.3 Kockázatokra adott válasz 42](#_Toc191367077)

[8.8 RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS 42](#_Toc191367078)

[8.8.1 Beszerzések 42](#_Toc191367079)

[8.8.2 Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai 42](#_Toc191367080)

[8.8.3 Az elektronikus információs rendszerre vonatkozó dokumentáció 43](#_Toc191367081)

[8.8.4 Támogatással nem rendelkező rendszerelemek 43](#_Toc191367082)

[8.9 RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM 44](#_Toc191367083)

[8.9.1 Szabályzat és eljárásrendek 44](#_Toc191367084)

[8.9.2 Szolgáltatásmegtagadással járó támadások elleni védelem 44](#_Toc191367085)

[8.9.3 A határok védelme 45](#_Toc191367086)

[8.9.4 Kriptográfiai kulcs előállítása és kezelése 45](#_Toc191367087)

[8.9.5 Kriptográfiai védelem 46](#_Toc191367088)

[8.9.6 Együttműködésen alapuló informatikai eszközök 46](#_Toc191367089)

[8.9.7 Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) 46](#_Toc191367090)

[8.9.8 Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás) 47](#_Toc191367091)

[8.9.9 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén 47](#_Toc191367092)

[8.9.10 A folyamatok elkülönítése 47](#_Toc191367093)

[8.10 RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG 48](#_Toc191367094)

[8.10.1 Szabályzat és eljárásrendek 48](#_Toc191367095)

[8.10.2 Hibajavítás 48](#_Toc191367096)

[8.10.3 Kártékony kódok elleni védelem 49](#_Toc191367097)

[8.10.4 Az EIR monitorozása 49](#_Toc191367098)

[8.10.5 Biztonsági riasztások és tájékoztatások 50](#_Toc191367099)

[8.10.6 Információ kezelése és megőrzése 50](#_Toc191367100)

# Bevezetés

## A dokumentum célja

Ez a rendszerbiztonsági terv áttekintést nyújt a <Rendszer neve> biztonsági követelményeiről, és ismerteti a rendszer által továbbítandó, feldolgozandó vagy tárolandó adatoknak megfelelő biztonsági elvárások biztosítása érdekében alkalmazott, vagy tervezett védelmi intézkedéseket és ellenőrzéseket. A rendszerbiztonsági terv meghatározza továbbá a rendszerhez hozzáférő valamennyi személy felelősségét és elvárt viselkedését.

Jelen rendszerbiztonsági terv célja

* megfelelő, költséghatékony biztonsági védelem kialakításának elősegítése a rendszerek fejlesztési szakaszában, illetve a rendszer életciklusának további fázisaiban a biztonsági ellenőrzések értékelésével és a vezetőség által adott felhatalmazás dokumentálásával,
* a biztonsági tevékenységek következetes végrehajtásának és személyi változások esetén történő fenntartásának támogatása,
* a biztonsági követelményeknek való megfelelés támogatása,
* a biztonsági intézkedések minőségbiztosításának támogatása.

## Fogalmak és rövidítések definíciója

A dokumentumban használt rövidítések jelentését az alábbi táblázat tartalmazza.

*[A nem használt fogalmakat kérjük törölje a listából, illetve vegye fel a további magyarázatot igénylő, a dokumentumban használt rövidítéseket és fogalmakat!]*

|  |  |
| --- | --- |
| **Fogalom** | **Meghatározás** |
| **adminisztratív védelem** | a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás |
| **általános védelmi intézkedés** | Egy vagy több szervezeti információs rendszerre alkalmazható védelmi intézkedés, amely a következő tulajdonságokkal rendelkezik: 1. a védelmi intézkedés kialakítás, megvalósítás és értékelés felelőssége nem a rendszertulajdonosé, hanem egy felelős személyhez vagy szervezeti egységhez rendelhető;
2. a védelmi intézkedés értékelésének eredményei felhasználhatók az olyan rendszerek biztonsági tanúsítási és engedélyezési folyamatainak támogatására, ahol a védelmi intézkedést alkalmazták.
 |
| **bizalmasság** | az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról |
| **biztonsági esemény** | nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül |
| **biztonsági esemény kezelése** | az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység |
| **biztonsági osztály** | az elektronikus információs rendszer védelmének elvárt erőssége |
| **biztonsági osztályba sorolás** | a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása |
| **elektronikus információs rendszer** | a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagyc) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok; |
| **elektronikus információs rendszer biztonsága** | az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát; |
| **fizikai védelem**  | a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem |
| **hitelesítés** | Egy felhasználó, folyamat vagy eszköz személyazonosságának ellenőrzése, gyakran az információs rendszer erőforrásaihoz való hozzáférés engedélyezésének előfeltételeként. |
| **információbiztonság** | Az információk és információs rendszerek védelme a jogosulatlan hozzáféréstől, felhasználástól, nyilvánosságra hozataltól, megzavarástól, módosítástól vagy megsemmisítéstől a bizalmasság, sértetlenség és rendelkezésre állás biztosítása érdekében. |
| **kiber-fizikai rendszer** | olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével; |
| **logikai védelem**  | az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem |
| **megfelelő biztonság** | Az információ elvesztéséből, visszaélésszerű használatából, illetéktelen hozzáféréséből vagy módosításából eredő kockázatnak és kár nagyságrendjének megfelelő biztonság. |
| **rendelkezésre állás**  | annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek |
| **rendszer engedélyezése** | A szervezet vezetője által hozott hivatalos vezetői döntés egy információs rendszer üzemeltetésének engedélyezéséről és elfogadott biztonsági védelmi intézkedések végrehajtása alapján a szervezeti működésre, eszközökre vagy egyénekre vonatkozó kockázat elfogadásáról. |
| **sértetlenség** | az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható |

# A rendszer átfogó ismertetése

## Megnevezés

|  |  |
| --- | --- |
| **Rendszer megnevezése** |  |
| Rendszer egyedi azonosítója |  |

## A rendszer célja, hatóköre

*[Adjon rövid (egy-három bekezdéses) leírást a rendszer funkciójáról/céljáról.*

*Ha a rendszer általános támogatási rendszer, sorolja fel az általa támogatott összes alkalmazást. Írja le az egyes alkalmazások funkcióját és a feldolgozott információkat.]*

## A rendszer alapfeladatait biztosító modulok

Az <Rendszer neve> az alábbi főbb funkciókat valósítja meg az egyes moduljain keresztül. Az alábbi táblázat az információs rendszer moduljait sorolja fel:

|  |  |
| --- | --- |
| **Modul megnevezése** | **A modul célja, fő funkciói** |
|  |  |
|  |  |

## A rendszer jelenlegi státusza

*[A rendszer működési állapotára vonatkozóan a következők közül egyet vagy többet jelezzen. Ha egynél több állapot van kiválasztva, sorolja fel, hogy az egyes állapotok a rendszer mely részeire vonatkoznak.]*

A rendszer jelenleg a következő táblázatban feltüntetett életciklus-fázisban van.

| A rendszer jelenlegi státusza |
| --- |
| [x]  | Üzemel | A rendszer élesüzemi használatban van |
| [ ]  | Fejlesztés alatt | A rendszer tervezése, fejlesztése vagy bevezetése folyamatban van. |
| [ ]  | Jelentős változtatás alatt | A rendszer jelentős változás, fejlesztés vagy átalakítás alatt áll. |
| [ ]  | Egyéb | Kérjük írja le részeletesen a fázist: |

## A rendszer típusa

Azok a rendszerek, alkalmazások, amelyek az általuk tartalmazott, feldolgozott, tárolt vagy továbbított információk miatt, vagy az szervezet küldetése szempontjából kiemelt fontosságúak, különleges irányítási felügyeletet igényelnek fő alkalmazásnak tekinthetők. A fő alkalmazások olyan rendszerek, amelyek egyértelműen meghatározott funkciókat látnak el, és amelyeknél a biztonsági megfontolások és igények könnyen azonosíthatók (pl. pénzügyi tranzakciók kezelése). Egy fő alkalmazás számos egyedi programból, valamint hardver-, szoftver- és távközlési komponensből állhat.

Az általános támogató rendszer közös funkciókkal rendelkező azonos közvetlen irányítás alatt álló informatikai erőforrások összekapcsolt halmaza. Ilyenek lehetnek a közösen használt feldolgozó infrastruktúra beleértve annak operációs rendszerét és segédprogramjait is, valamint a kommunikációs hálózat. Egy fő alkalmazást futtathat egy általános támogató rendszer. Az általános támogató rendszer rendszerbiztonsági terve ilyen esetben referenciaként szolgálhat a fő alkalmazási rendszer biztonsági tervében. Egy általános támogató rendszer akkor tekinthető fő alkalmazásnak, ha különleges vezetői figyelmet igényel, magasak a fejlesztési, üzemeltetési vagy karbantartási költségei; és az általa kezelt adatok jelentős szerepet játszanak az szervezeti működésben.

*[Jelölje meg, hogy a rendszer egy fő alkalmazás vagy egy általános támogató rendszer. Ha a rendszer kisebb alkalmazásokat is tartalmaz, azokat a 2.1 pontban kell felsorolni.]*

|  |  |
| --- | --- |
| [x]  Főalkalmazás | [ ]  Általános támogató rendszer |

# Szervezeti feladatok és felelősségek elhatárolása

[*A Rendszerrel kapcsolatosan nem alkalmazható szerepkörök törölhetők a felsorolásokból, illetve szükség esetén a lista bővíthető*]

## Engedélyezésért felelős vezető

Az engedélyezésért felelős vezető a szervezeti felsővezetés azon tagja, aki jogosult hivatalosan felelősséget vállalni egy információs rendszer a szervezet számára elfogadható kockázati szinten történő működtetéséért a szervezeti működés, a vagyonelemek vagy a személyek tekintetében.

Az engedélyezésért felelő vezetőnek a rendszerbiztonsági tervekkel kapcsolatban a következő feladatai vannak:

* jóváhagyja a rendszerbiztonsági terveket,
* engedélyezi az információs rendszer üzembehelyezését és működtetését, esetleg (felvállalható) kockázatok felvállalása mellett engedélyezi az üzembehelyezést, vagy
* megtagadja az információs rendszer üzemeltetésének engedélyezését (vagy ha a rendszer már működik, leállítja az üzemeltetését), ha elfogadhatatlan biztonsági kockázatok állnak fenn.

|  |  |
| --- | --- |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Rendszertulajdonos

A rendszertulajdonos az információs rendszer beszerzéséért, fejlesztéséért, integrálásáért, módosításáért, üzemeltetéséért és karbantartásáért teljeskörűen felelős szervezeti tisztségviselő.

A rendszer tulajdonosa a rendszerbiztonsági tervekkel kapcsolatban a következő felelősséggel rendelkezik:

* kidolgozza a rendszerbiztonsági tervet az adatgazdákkal, az információbiztonsági felelőssel, a rendszergazdával és a kulcsfelhasználókkal együttműködve,
* biztosítja a rendszerbiztonsági terv karbantartását, és hogy a rendszert az elfogadott biztonsági követelményeknek megfelelően telepítik és üzemeltetik,
* biztosítja, hogy a rendszer felhasználói és a támogató személyzet megkapják a szükséges biztonsági képzést (pl. a viselkedési szabályokra vonatkozó oktatás).

|  |  |
| --- | --- |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Adatgazda

Az adatgazda a szervezet olyan tisztviselője, aki jogszabályi vagy műszaki szempontú rendelkezési jogkörrel rendelkezik az érintett adatokkal kapcsolatban és felelős az információk létrehozásának, begyűjtésének, feldolgozásának, terjesztésének és megsemmisítésének ellenőrzéséért.

Az adatgazda rendszerbiztonsági tervekhez kapcsolódó feladatai a következőket jelentik:

* meghatározza az adatok megfelelő használatára és védelmére vonatkozó szabályokat,
* biztosítja a biztonsági követelményekre és a védelmi intézkedésekre vonatkozó információkat a rendszertulajdonos számára,
* eldönti, hogy kinek lehet hozzáférése az információs rendszerhez, és milyen típusú jogosultságok vagy hozzáférési jogok kerüljenek meghatározásra,
* támogatja a rendszerrel kapcsolatos védelmi intézkedések azonosítását és értékelését.

*[Amennyiben a rendszernek több adatgazdája van, mindegyiket fel kell sorolni az irányítása alá tartozó adatkörökkel együtt. Ilyen esetben adatgazdánkként egy táblázatot kell kitölteni]*

|  |  |
| --- | --- |
| Adatkörök | pl. számlázási adatok, vevő/ügyféladatok, termékadatok |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Informatikai vezető

Az informatikai vezető az szervezet szintjén felelős az információ biztonsági program kialakításáért és fenntartásáért, illetve a következő biztonság tervezési felelősségekkel rendelkezik:

* kijelöli a rendszer biztonságtervezési felelősét,
* biztosítja a rendszerbiztonság tervezésének kezelésére vonatkozó szabályzatok, eljárások és ellenőrzési módszerek kialakítását és karbantartását,
* biztosítja az általános, minden rendszerre érvényes védelmi intézkedések azonosítását, megvalósítását, értékelését és folyamatos fejlesztését,
* biztosítja a rendszerbiztonsági tervekkel kapcsolatosan felelősséggel rendelkező személyek képzését,
* támogatja a szervezet vezetőit a rendszer biztonsági terveivel kapcsolatos felelősségük ellátásában.

|  |  |
| --- | --- |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Információbiztonsági felelős

Az információbiztonsági felelős az a személy, aki a szervezeten belül felelős a szervezet információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséért és fenntartásáért, és elvégzi vagy irányítja ezen tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.

Az információbiztonsági felelős feladatai a rendszerbiztonsági tervezéssel kapcsolatban:

* átveszi az informatikai vezető felelősségét a rendszerek biztonsági tervezésével kapcsolatban,
* a rendszerbiztonsági tervek kialakításának, felülvizsgálatának és elfogadásának összehangolása az információs rendszer tulajdonosaival és az engedélyező vezetővel,
* az általános biztonsági ellenőrzések azonosításának, végrehajtásának és értékelésének összehangolása,
* a rendszerbiztonsági tervek kialakításához és felülvizsgálathoz szükséges szakmai kompetenciák kialakításának, fejlesztésének támogatása vagy oktatása.

|  |  |
| --- | --- |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Üzemeltetésbiztonsági felelős

Az üzemeltetésbiztonsági felelős olyan személy, akit a megfelelő jogkörrel rendelkező vezető (pl. informatikai vezető, rendszertulajdonos, információbiztonsági felelős) jelöl ki annak biztosítása érdekében, hogy a megfelelő üzemeltetésbiztonsági tevékenységeket végrehajtsák és folyamatosan fenntartsák az üzemeltetés biztonságát.

Az üzemeltetésbiztonsági felelős feladatai a biztonságtervezéssel kapcsolatban a következők:

* segítségnyújtás az információbiztonsági felelősnek a közös biztonsági ellenőrzések meghatározásában, végrehajtásában és értékelésében,
* a rendszerbiztonsági terv fejlesztésének és karbantartásának aktív támogatása, a rendszerváltoztatások összehangolása az információs rendszer tulajdonosával és a változtatások biztonsági hatásának felmérése.

|  |  |
| --- | --- |
| Név |  |
| Beosztás |  |
| Szervezeti egység |  |
| Telefonszám |  |
| Email |  |

## Rendszer üzemeltetési felelősségek

|  |  |
| --- | --- |
| **Üzemeltetési feladat** | **Szervezeti egység/személyek** |
| Alkalmazásüzemeltetés |  |
| Szerver operációs rendszer üzemeltetés |  |
| Hardver infrastruktúra |  |
| Hálózatüzemeltetés |  |
| Adatközponti infrastruktúra elemek üzemeltetése |  |
| Rendszerfelügyelet |  |

## Végfelhasználók és privilegizált felhasználók száma

*[Az alábbi táblázatban adja meg a rendszer felhasználóinak és rendszergazdáinak hozzávetőleges számát. Tartalmazza az összes privilegizált hozzáféréssel rendelkező személyt, például rendszergazdákat, adatbázis-adminisztrátorokat, alkalmazás-adminisztrátorokat stb. Szükség szerint adjon hozzá sorokat a különböző szerepkörök meghatározásához.* *Itt érdemes feltüntetni a technikai felhasználókat is, különösen, azokat, amelyek privilegizált jogosultságokkal is rendelkeznek, vagy a rendszer működése, üzemeltetése szempontjából nélkülözhetetlenek, alapértelmezettek.]*

Az alábbi táblázat <Rendszer neve> felhasználóinak hozzávetőleges számát mutatja.

| Szerep | Külső/belső | Privilégiumok és betöltött szerepkörök  | Felhasználószám  |
| --- | --- | --- | --- |
| pl. Rendszergazda | Belső | Adatbázis adminisztrátor | 5 |
| pl. Felhasználó | Külső/Belső | Felhasználó | 100 |
|  |  |  |  |

# Biztonsági osztályba sorolás

## A rendszer által kezelt és tárolt adatok osztályozása

[*Az alábbiakban megadott adatosztályozási módszertan, amelynek részleteit a 418/2024. (XII. 23.) Korm. rendelet 1. melléklete írja le, a Kiberbiztonsági tv.* *9. § (1) és (2) bekezdésben meghatározott szervezetek számára* *kötelező az ott előírt esetekben, a többi szervezet számára opcionális.]*

Az elektronikus információs rendszer által kezelt, vagy feldolgozott adatokat az alábbi táblázat foglalja össze. A táblázatban szerepeltetni kell a rendszer által kezelt összes adatkört. A kezelés alatt értendő az adatok keletkezése, feldolgozása, megjelenítése, átadása és tárolása is. A táblázat egyes mezőit az alábbiak szerint kell kitölteni:

* **Adatcsoport megnevezése**: az adatkör megnevezése.
* **Kezelt adatok fajtája**: az adott adatkört kezelő rendszer modul(ok) neve/azonosítója. Minden olyan modult fel kell sorolni, ahol az adott adatkör adatai keletkeznek, tárolódnak, feldolgozásra kerülnek.
* **Bizalmasság szerinti besorolás**: 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 2. pont szerint
* **Sértetlenség és rendelkezésre állás szerinti besorolás**: 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 3. pont szerint.
* **Adatosztályozás eredménye:** 418/2024. (XII. 23.) Korm. rendelet 1. melléklet 4. pont szerint.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Adatcsoport megnevezése** | **Kezelt adatok fajtája** | **Bizalmasság szerinti besorolás** | **Sértetlenség és rendelkezésre állás szerinti besorolás** | **Adatosztályozás eredménye** |
|  |  | ***[B1; B2; B3; B4]*** | ***[SR1; SR2]*** | ***[F1; F2; F3; F4]*** |
|  |  |  |  |  |
|  |  |  |  |  |

## A rendszer biztonsági osztálya

Szervezet elvégezte a Rendszer által kezelt vagy feldolgozott adatok azonosítását, a releváns fenyegetettségek meghatározását és ehhez kapcsolódóan a lehetséges kárértékek beazonosítását. A biztonsági osztályba sorolás 7/2024. (VI. 24.) MK rendelet szerinti szempontrendszerét az alábbi táblázat mutatja.

[*Kérjük tegyen X-et a táblázat Igen/Nem oszlopaiba, attól függően, hogy az adott sorban igaz (Igen) vagy hamis (Nem) a rendszerre vonatkozó állítás.]*

|  |  |  |  |
| --- | --- | --- | --- |
| Pont. | Besorolási kritérium | Igen | Nem |
| 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 |  |  |
| 2.2.3.1. | 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 |  |  |
| 2.2.4.1. | 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 |  |  |

[Amennyiben a szervezet a fentitől eltérő módszert alkalmaz a biztonsági osztályba sorolásra, akkor kérjük írja le a besorolás módszerét! *Az alábbiakban adja meg az előzetes biztonsági osztályba sorolás eredményét.]*

|  |  |
| --- | --- |
|  | **<Rendszer neve>** **biztonsági osztálya** |
|  A rendszer biztonsági osztálya | **[*Alap; Jelentős; Magas]*** |

# A <Rendszer neve> műszaki megoldásainak bemutatása

Ez a fejezet a rendszert olyan mélységben ismerteti, ami a rendszerrel kapcsolatos védelmi szabályozások és folyamatok megértéséhez szükséges. Az alábbi alfejezetek mellett további információk is szerepeltethetők.

## A <Rendszer neve> főbb elemei és adatkapcsolatai

### A rendszer főbb moduljai, alrendszerei

A rendszer modul, alrendszer az információs rendszer olyan fő egysége vagy összetevője, amely egy vagy több konkrét funkciót lát el.

|  |  |
| --- | --- |
| Rendszer modul /alrendszer megnevezése | Funkció |
|  |  |
|  |  |
|  |  |

### Rendszer környezete és határai

## Rendszer logikai felépítésének bemutatása

*[Ebben a fejezetben adjon részletes topológiai leírást és ábrát, amely világosan ábrázolja a rendszer határait, a rendszer összeköttetéseit és a kulcsfontosságú eszközöket. (Megjegyzés: ehhez nem kell minden munkaállomást vagy asztali számítógépet ábrázolni, de minden egyes használt operációs rendszerhez, a hordozható komponensekhez (ha van ilyen), az összes virtuális és fizikai szerverhez (pl. fájl, nyomtatás, web, adatbázis, alkalmazás), valamint a hálózatba kapcsolt munkaállomásokhoz tűzfalakhoz, útválasztókhoz, kapcsolókhoz, másolókhoz, nyomtatókhoz, laboreszközökhöz, kézi számítógépekhez tartozik egy példány.) Ha a diagramon más rendszerek olyan komponenseit is fel kell tüntetni, amelyek összekapcsolódnak/interfésznek ezzel a rendszerrel, akkor a rendszerhatárokat a biztonsági tervekre vagy a többi rendszer(ek) nevére és tulajdonosára való hivatkozással kell jelölni a diagramon.]*

### A rendszer topológiája

*[Az alábbiakban illesszen be egy rendszertopológia ábrát! Adjon az ábrával összhangban lévő leírást, amely egyértelműen felsorolja és leírja az egyes rendszerelemeket!]*

### A rendszer hardver környezetének összefoglaló bemutatása

*[Írja le a rendszert kiszolgáló hardver elemeket vagy hivatkozásként adja meg a rendszerelemek nyilvántartásának helyét!]*

### A rendszer szoftver környezetének összefoglaló bemutatása

*[Írja le vagy hivatkozzon az összes szoftver (rendszerszoftver és alkalmazási szoftver) komponens teljes és pontos felsorolására, beleértve a gyártmányt/OEM-et, modellt, verziót, szervizcsomagokat!]*

| Hoszt | Funkció | Verzió | Patch szint | IP cím | Virtualizált (Igen / Nem) |
| --- | --- | --- | --- | --- | --- |
|  | Operációs rendszer | Windows Server 2022 |  | 255.255.255.255 | Igen |
|  | IIS | ASP .Net 4.5 |  | 255.255.255.255 | Igen |
|  | Alkalmazás |  |  | 255.255.255.255 | Igen |
|  | Database SQL Server | MS SQL 2016 |  | 123.45.678 | Igen |

### A rendszer kapcsolatainak összefoglaló bemutatása

*[Sorolja fel az összekapcsolt rendszereket és rendszerazonosítókat (adott esetben), adja meg a rendszert, a nevet, a szervezetet, a rendszer típusát (fő alkalmazás vagy általános támogató rendszer)!]*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Megnevezés** | **Forrás rendszer** | **Cél rendszer** | **Interfész technológia típus** | **Interfész funkcionalitás összefoglaló leírása** |
|  |  |  |  |  |
|  |  |  |  |  |

## Portok, protokollok és szolgáltatások

| **Portok****(TCP/UDP)** | **Protokollok** | **Szolgáltatások** | **Szolgáltatás kliens** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## A rendszer fizikai környezete

*[Ismertesse az egyes rendszerelemek fizikai elhelyezését, a fizikai környezet védelem jellemzőit. Ide tartozik például a szerverek elhelyezése, a géptermek megközelíthetősége, beléptető rendszere, videokamerás megfigyelése stb.]*

# Alapvető biztonsági események meghatározása

*[Kérjük sorolja fel a rendszer szempontjából releváns biztonsági eseményeket és azok azonosítási és felügyeleti megoldását! Releváns események lehetnek pl.:*

* *Felhasználói bejelentkezések és kijelentkezések*
* *Rendszerkonfiguráció változások*
* *Hozzáférési kísérletek (sikertelen bejelentkezések, jogosulatlan hozzáférési kísérletek, például sikertelen fájlhozzáférések vagy adatbázis-lekérdezések)*
* *Rendszerhibák és figyelmeztetések*
* *Hálózati forgalom anomália (szokatlan vagy gyanús hálózati tevékenységek, például nagy mennyiségű adatforgalom vagy ismeretlen IP-címekről érkező kérések)*
* *Adatmanipuláció (adatok létrehozása, módosítása vagy törlése, különösen érzékeny vagy bizalmas adatok esetén)*
* *Fájlhozzáférések (pl. rendszerfájlok, érzékeny dokumentumok)*
* *Felhasználói jogosultságok módosítása*
* *Rendszerindítások és leállások*

*]*

# Kapcsolódó dokumentumok

## Kapcsolódó jogszabályok, megfelelés elvárások

*[Sorolja fel azokat a jogszabályokat vagy rendeleteket, amelyek a rendszerben lévő adatok bizalmasságára, sértetlenségére vagy rendelkezésre állására vonatkozó különleges követelményeket állapítanak meg!]*

|  |  |  |
| --- | --- | --- |
| **Dokumentum címe** | **Típusa** | **Kiadás dátuma** |
|  |  |  |
|  |  |  |

## Kapcsolódó szabályzatok és dokumentumok

*[Sorolja fel azokat a szervezeti dokumentumokat, amelyek a rendszer tervezési, implementációs vagy üzemeltetési fázisában meghatározza a rendszerrel kapcsolatos viselkedési szabályokat!]*

|  |  |  |
| --- | --- | --- |
| **Dokumentum címe** | **Típusa** | **Kiadás dátuma** |
|  |  |  |
|  |  |  |

# Védelmi intézkedések megvalósítása

[*A Rendszer kialakítása és üzembehelyezése során implementálni kell a biztonsági osztályhoz tartozó, 7/24 (VI. 24.) MK rendelet védelmi intézkedés katalógusban meghatározott, a rendszer biztonsági osztályához tartozó követelményeket.]*

Az elektronikus információs rendszerre vonatkozó biztonsági elvárások meghatározásának célja az elektronikus információs rendszer és az általa kezelt adatok kockázatokkal arányos védelmének kialakítása, a jogosulatlan hozzáférés elkerülése, az elvárt rendelkezésre állási követelmények teljesítése.

Ez a szakasz a rendszer biztonsági osztályához tartozó 7/24 (VI. 24.) MK rendelet 2. melléklet szerinti védelmi intézkedés katalógusban meghatározott minimálisan elvárt védelmi intézkedéseket tartalmazza. Eltérő rendelkezés hiányában minden egyes védelmi intézkedés esetében az információs rendszer tulajdonosa felelős az védelmi intézkedések megvalósításáért. A jogszabály által meghatározott védelmi intézkedésektől való egyedi eltéréseket indokolni kell.

*[Az alábbi védelmi intézkedések kiegészítése szükséges abban az esetben, ha a 7/24 (VI. 24.) MK rendelet 2. melléklet szerinti kiegészítő kontrollok, vagy egyéb intézkedések alkalmazását a szervezet, akár helyettesítő intézkedésként, akár más okból szükségesnek ítéli meg.]*

*[Az egyes követelményeknél szükséges megadni, hogy általános, rendszer specifikus, hibrid követelményről van-e szó. Általános követelményről döntően akkor beszélünk, ha követelmény szervezeti szintű és a megvalósítása alapvetően szervezeti feladatként jelentkezik. Rendszerspecifikus a követelmény, ha alapvetően az érintett rendszerre vonatkozik és a megvalósítása fejlesztői feladat. A követelmény akkor hibrid, ha a megvalósításban szerepe van vagy lehet a szervezetnek és a fejlesztőnek egyaránt. Nem alkalmazható követelményről akkor beszélhetünk, ha az adott követelményt valamilyen oknál fogva teljességgel kizárjuk az érintett rendszer kapcsán (pl. a biometrikus azonosításra vonatkozó követelményt kizárhatjuk, ha a rendszerben ilyen típusú azonosítási/hitelesítési eljárást nem alkalmazunk)]*

## HOZZÁFÉRÉS-FELÜGYELET

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint - a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó hozzáférés-felügyeleti szabályzatot, amely - meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá - összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. - a hozzáférés-felügyeleti eljárásrendet, amely a hozzáférés-felügyeleti szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Fiókkezelés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.2. |
| A szervezet:Meghatározza és dokumentálja a rendszerben engedélyezett és kifejezetten tiltott fióktípusokat.Kijelöli a fiókkezelőket.Kialakítja a csoport- és szerepkör tagsági feltételeket és kritériumokat.Meghatározza: - a rendszerben engedélyezett felhasználókat. - a csoport- és szerepkör tagságokat. - a hozzáférési jogosultságokat és a felhasználói fiókokhoz tartozó szükséges jellemzőket minden egyes felhasználói fiókra.A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén.Létrehozza, engedélyezi, módosítja, letiltja és törli a fiókokat a meghatározott irányelvek, eljárások, előfeltételek és kritériumok alapján.Nyomon követi a fiókok használatát.Értesíti a fiókkezelőket és a meghatározott személyeket vagy szerepköröket a következő esetekben: - meghatározott időn belül, amikor a fiókok már nem szükségesek. - meghatározott időn belül, amikor a felhasználók jogviszonya megszűnik. - meghatározott időn belül, amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak.Engedélyezi a rendszerhez való hozzáférést a következők alapján: - érvényes hozzáférési engedély; - tervezett rendszerhasználat; - egyéb, a szervezet által meghatározott jellemzők.Ellenőrzi a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából, a meghatározott gyakorisággal.Létrehoz és végrehajt egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére.Összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszűntetési folyamataival. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Hozzáférési szabályok érvényesítése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.15. |
| Az EIR a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott logikai hozzáférési jogosultságokat az információkhoz és a rendszer erőforrásaihoz. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Sikertelen bejelentkezési kísérletek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.71. |
| A szervezet:Az általa meghatározott esetszám korlátot alkalmazza a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A rendszerhasználat jelzése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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: - a felhasználók a szervezet EIR-ét használják. - a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják. - a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár. - a rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti.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.Nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza: - a felhasználók a szervezet EIR-ét használják. - a rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják. - a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.88. |
| A szervezet:Azonosítja azon felhasználói tevékenységeket, amelyek - a szervezeti célokkal és üzleti funkciókkal összhangban - az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatók.A rendszerbiztonsági tervben dokumentálja és megindokolja azokat a felhasználói tevékenységeket, amelyek azonosítás vagy hitelesítés nélkül is végrehajthatók. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Távoli hozzáférés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.100. |
| A szervezet:Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Vezeték nélküli hozzáférés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.108. |
| A szervezet:A vezeték nélküli hozzáférés minden egyes típusára vonatkozóan konfigurációs követelményeket, kapcsolódási követelményeket és alkalmazási útmutatást alakít ki.Engedélyezési eljárást folytat le a rendszerhez való vezeték nélküli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Mobil eszközök hozzáférés-ellenőrzése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.113. |
| A szervezet: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.Engedélykötelessé teszi a szervezet rendszereihez mobil eszközökkel történő kapcsolódást. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Külső elektronikus információs rendszerek használata

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.115. |
| A szervezet: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: - hozzáférjenek a rendszerhez külső rendszerekből; és - feldolgozzák, tárolják vagy továbbítsák a szervezet által ellenőrzött információkat külső rendszerek használatával; vagymegtiltja a meghatározott típusú külső rendszerek használatát. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Nyilvánosan elérhető tartalom

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 2.124. |
| A szervezet:Kijelöli azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé.Képzést biztosít a jogosult személyek számára, hogy biztosítsa, hogy a nyilvánosan hozzáférhető információk nem tartalmaznak nem nyilvános információkat.Áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy nem tartalmaznak nem nyilvános információkat.Meghatározott gyakorisággal áttekinti a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából, és eltávolítja az ilyen információkat, ha felfedezik őket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó naplózásra és elszámoltathatóságra vonatkozó szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.a naplózási és elszámoltathatósági eljárásrendet, amely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki a naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplózható események

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.2. |
| A szervezet:Meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az EIR-t.Egyezteti a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy iránymutatással és információkkal segítse a naplózandó események kiválasztását.Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket.Indokolja, hogy a kiválasztott eseménytípusok, miért alkalmasak a biztonsági események utólagos kivizsgálásának támogatására;Meghatározott gyakorisággal felülvizsgálja és frissíti a naplózásra kiválasztott eseménytípusokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplóbejegyzések tartalma

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.3. |
| A szervezet biztosítja, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek:milyen típusú esemény történt;mikor történt az esemény;hol történt az esemény;miből származott az esemény; ésmi volt az eseménynek a kimenetele, valamintaz eseményhez kapcsolódó személyek, alanyok, objektumok. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplózás tárkapacitása

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.5. |
| A szervezet elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplózási hiba kezelése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.7. |
| A szervezet naplózási hiba esetén:Riasztja a meghatározott személyeket vagy szerepköröket a szervezet által meghatározott időn belül.További meghatározott intézkedéseket hajt végre. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.13. |
| A szervezet:Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából.Jelenti ezeket a szervezet által meghatározott személyeknek vagy szerepköröknek.Módosítja a naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének szintjét, amennyiben hiteles információk és információforrások alapján a kockázat változik. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Időbélyegek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.24. |
| A szervezet:Belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához.Időbélyegeket rögzít a naplóbejegyzésekben, amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplóinformációk védelme

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.25. |
| Az EIR:Megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor értesíti a meghatározott személyeket vagy szerepköröket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A naplóbejegyzések megőrzése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Naplóbejegyzések létrehozása

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 4.40. |
| Az EIR:Biztosítja a naplóbejegyzés generálási képességet a "Naplózható események" pontban meghatározott naplózható eseményekre.Lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az EIR egyes elemei által.Naplóbejegyzéseket állít elő a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságértékelési szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal.A biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonságértékelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonsági értékelések

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.2. |
| A szervezet:Kiválasztja az elvégzendő értékelés típusának megfelelő értékelő személyt vagy csoportot.Biztonságértékelési tervet készít, amely leírja az értékelés hatókörét, beleértve:az értékelendő védelmi intézkedéseket, azok kiterjesztését és továbbfejlesztését;a védelmi intézkedések hatékonyságának megállapításához használt értékelési eljárásokat;az értékelési környezetet, az értékelő csoportot, az értékelő szerepköröket és feladataikat.Biztosítja, hogy a biztonságértékelési tervet az engedélyezésre jogosult felelős vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálja és jóváhagyja.Meghatározott gyakorisággal értékeli az EIR és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.Elkészíti a biztonságértékelés eredményét összefoglaló jelentést.Gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek a szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonsági értékelések – Kiberbiztonsági audit

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.4. |
| A 1. § (2) bekezdés hatálya alá tartozó szervezet független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Információcsere

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.7. |
| A szervezet: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.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.Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Az intézkedési terv és mérföldkövei

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.10. |
| A szervezet: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.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Engedélyezés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.12. |
| A szervezet:Kijelöl egy engedélyezésért felelős személyt, aki az EIR-ért felel.Kijelöl egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.Biztosítja, hogy az engedélyezésért felelős személy az EIR használatbavételét megelőzően:elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; ésa szervezet vezetőjével engedélyezteti a rendszer működését.Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.Rendszeresen felülvizsgálja az engedélyeket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Folyamatos felügyelet

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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:A rendszerszintű metrikák meghatározását.Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére.A védelmi intézkedések folyamatos értékelését.Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését.A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését.A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket.az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Folyamatos felügyelet – Kockázatmonitorozás

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.18. |
| A szervezet biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:a hatékonyság ellenőrzését;a megfelelés ellenőrzését; ésa változások nyomon követését. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Belső rendszerkapcsolatok

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 5.25. |
| A szervezet:Engedélyezi a szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását.Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét.Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat.Meghatározott gyakorisággal felülvizsgálja minden belső kapcsolat további szükségességét. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## KONFIGURÁCIÓKEZELÉS

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó konfigurációkezelési szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.A konfigurációkezelési eljárásrendet, amely a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki a konfigurációkezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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 |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Alapkonfiguráció

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.2. |
| A szervezet:Kifejleszti, dokumentálja és karbantartja az EIR alapkonfigurációját.Elvégzi az EIR alapkonfigurációjának felülvizsgálatát és frissítését:meghatározott időközönként;ha azt a meghatározott körülmények indokolják, vagyaz EIR vagy rendszerelemek telepítésekor vagy frissítésekor. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonsági hatásvizsgálatok

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.15. |
| A szervezet még a változtatások bevezetése előtt megvizsgálja az EIR-ben tervezett változtatásoknak az információbiztonsági hatásait. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A változtatásokra vonatkozó hozzáférés korlátozások

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.18. |
| A szervezet meghatározza, dokumentálja, jóváhagyja és érvényesíti azokat a fizikai és logikai hozzáférési korlátozásokat, amelyek az EIR változtatásaihoz kapcsolódnak. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Konfigurációs beállítások

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.23. |
| A szervezetKialakítja és dokumentálja a rendszerelemekben alkalmazott egységes biztonsági konfigurációs beállításokat, amelyek az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot képviselik.Elvégzi a konfigurációs beállításokat az EIR valamennyi elemében.Azonosítja, dokumentálja és elfogadja a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.Figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait a szervezeti szabályzatokkal és eljárásokkal összhangban. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Legszűkebb funkcionalitás

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.26. |
| A szervezet:Az EIR-t úgy konfigurálja, hogy az csak az ügy- és üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa.Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Rendszerelem leltár

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.36. |
| A szervezet:Leltárt készít az EIR elemeiről.A leltár pontosan tükrözi az EIR-t.A leltár tartalmazza a rendszeren belül található összes elemet.Megakadályozza az elemek kettős elszámolását.A leltár a nyomon követés és a jelentéstétel szempontjából a szükséges részletességet biztosítja.A leltárban szereplő információk lehetővé teszik a rendszerelemekkel történő hatékony elszámolást.Meghatározott gyakorisággal felülvizsgálja és frissíti a rendszerelemek leltárát. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A szoftverhasználat korlátozásai

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.47. |
| A szervezet:Kizárólag olyan szoftvereket és olyan kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, valamint a szerzői jogi vagy más jogszabályi előírásoknak.A másolatok és megosztások ellenőrzésére nyomon követi a mennyiségi licenc alá eső szoftverek és a kapcsolódó dokumentációk használatát.Ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett művek jogosulatlan terjesztésére, megjelenítésére, előadására vagy sokszorosítására. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Felhasználó által telepített szoftver

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 6.49. |
| A szervezet:Megfogalmazza az EIR vonatkozásában a szervezetre érvényes követelményeket, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségeit.Érvényesíti a szoftvertelepítésre vonatkozó szabályokat a szervezet által meghatározott módszerek szerint.Meghatározott gyakorisággal ellenőrzi a szabályok betartását |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## KÉSZENLÉTI TERVEZÉS

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 7.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó üzletmenet-folytonosságra vonatkozó szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.az üzletmenet-folytonosságra vonatkozó eljárásrendet, amely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Üzletmenet-folytonossági terv

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 7.2. |
| A szervezet:Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely:meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;kijelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket és azok elérhetőségeit;meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat;tartalmazza az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek;szabályozza az üzletmenet-folytonossági információk megosztását; ésa szervezet által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott.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.Összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;Meghatározott gyakorisággal felülvizsgálja az EIR-hez kapcsolódó üzletmenet-folytonossági tervet.Az EIR vagy a működési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet.Tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.Az üzletmenet-folytonossági terv tesztelése, gyakorlata vagy tényleges alkalmazása során levont tanulságokat beépíti a tesztelési és gyakorlati folyamatokba.Gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető és módosítható. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A folyamatos működésre felkészítő képzés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 7.10. |
| A szervezet:Az EIR felhasználói számára szerepkörüknek vagy felelősségi körüknek megfelelő folyamatos működésre felkészítő képzést tart:szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;amikor az EIR változásai ezt szükségessé teszik;a szervezet által meghatározott gyakorisággal.Meghatározott gyakorisággal vagy meghatározott eseményeket követően felülvizsgálja és frissíti a folyamatos működésre felkészítő képzés tartalmát. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Az elektronikus információs rendszer mentései

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 7.35. |
| A szervezet:Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.Meghatározott gyakorisággal mentést készít az EIR-ben tárolt rendszerszintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.Meghatározott gyakorisággal mentést készít az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a biztonsági tárolási helyszínen. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Az elektronikus információs rendszer helyreállítása és újraindítása

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## AZONOSÍTÁS ÉS HITELESÍTÉS

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal.az azonosítási és hitelesítési eljárásrendet, amely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás és hitelesítés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.2. |
| A szervezet egyedileg azonosítja és hitelesíti a felhasználókat, és egyedi azonosítóhoz kapcsolja a felhasználók által végzett tevékenységeket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.3. |
| A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.7. |
| A szervezet visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált és a nem privilegizált fiókokhoz való hozzáféréshez. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosító kezelés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.14. |
| A szervezet:Az egyéni, csoport, szerepkör vagy eszköz azonosítók kiosztását a szervezet által meghatározott személyek vagy szerepkörök engedélyéhez köti.Kiválaszt egy azonosítót, amely azonosítja az egyént, csoportot, szerepkört, szolgáltatást vagy eszközt.Hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz.Meghatározott ideig megakadályozza az azonosítók újbóli felhasználását. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A hitelesítésre szolgáló eszközök kezelése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.21. |
| A szervezet a hitelesítő eszközöket az alábbiak szerint kezeli:A kezdeti hitelesítő eszköz kiosztásának részeként ellenőrzi a hitelesítő eszközt megkapó egyén, csoport, szerepkör, szolgáltatás vagy eszköz identitását.Meghatározza a szervezet által kiadott hitelesítő eszköz kezdeti tartalmát.Biztosítja, hogy a hitelesítő eszközök a tervezett felhasználáshoz megfelelő erősségű mechanizmussal rendelkezzenek.Adminisztratív eljárásokat alakít ki és hajt végre a kezdeti hitelesítő eszközök kiosztásához, az elveszett, kompromittált vagy sérült hitelesítő eszközökhöz, valamint a hitelesítő eszközök visszavonásához.Gondoskodik a hitelesítő eszközök kezdeti tartalmának megváltoztatásáról az első használat előtt.Gondoskodik a hitelesítő eszközök tartalmának megváltoztatásáról vagy frissítéséről meghatározott gyakorisággal, vagy amikor meghatározott események bekövetkeznek.Megvédi a hitelesítő eszközök tartalmát az illetéktelen nyilvánosságra hozatal és módosítás ellen.Megköveteli, hogy az egyének és eszközök konkrét védelmi intézkedéseket alkalmazzanak, illetve hajtsanak végre a hitelesítő eszközök védelme érdekében.Megváltoztatja a csoporthoz vagy szerepkörhöz rendelt fiókok hitelesítő eszközeinek tartalmát, amikor a fiókokhoz tartozó tagok közül valaki eltávolításra kerül. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.22. |
| A szervezet: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.Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján.A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja.A jelszavakat egy jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva tárolja.Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén.Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a nyomtatható karaktereket.Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában.A jelszavakra a szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Hitelesítési információk visszajelzésének elrejtése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.36. |
| Az EIR fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt a jogosulatlan személyek általi felfedésétől és felhasználásától. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Hitelesítés kriptográfiai modul esetén

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.38. |
| Az EIR egyedileg azonosítja és hitelesíti a szervezeten kívüli felhasználókat, tevékenységüket, valamint a nevükben futó folyamatokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.39. |
| A szervezet meghatározott profilokat alkalmaz az azonosítási folyamat során. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Újrahitelesítés

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 8.43. |
| A szervezet meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az újrahitelesítést. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## KOCKÁZATKEZELÉS

### Sérülékenységek ellenőrzése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 15.9. |
| A szervezet: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.Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Sérülékenységmenedzsment – Sérülékenységi információk fogadása

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 15.18. |
| A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Kockázatokra adott válasz

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 15.20. |
| A szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

### Beszerzések

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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:A funkcionális biztonsági követelményeket.A mechanizmusok erősségére vonatkozó követelményeket.A biztonság garanciális követelményeit.Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.A biztonsággal kapcsolatos dokumentációs követelményeket.A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket.Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.A teljesítési kritériumokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 16.8. |
| A szervezet megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Az elektronikus információs rendszerre vonatkozó dokumentáció

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 16.15. |
| A szervezet:Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;a biztonsági funkciók hatékony használatát és karbantartását; valamintaz ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;a felhasználói interakció biztonságos módját;a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.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; ésa dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Támogatással nem rendelkező rendszerelemek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 16.99. |
| A szervezet:lecseréli a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetvea támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a szervezet által meghatározott külső szolgáltatók bevonásával valósít meg. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és kommunikációvédelmi szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.a rendszer- és kommunikációvédelmi eljárásrendet, amely a rendszer- és kommunikációvédelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy, a szervezet által meghatározott személyt, aki a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Szolgáltatásmegtagadással járó támadások elleni védelem

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.12. |
| A szervezet:védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait; ésalkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A határok védelme

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.17. |
| A szervezet:Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein.A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól.Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Kriptográfiai kulcs előállítása és kezelése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.49. |
| A szervezet előállítja és kezeli a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Kriptográfiai védelem

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.53. |
| A szervezet:meghatározza a kriptográfia szervezeten belüli felhasználási területeit; ésmegvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Együttműködésen alapuló informatikai eszközök

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.54. |
| A szervezet:tiltja az együttműködésen alapuló számítástechnikai eszközök (például: kamerák, mikrofonok) és alkalmazások távoli aktiválását, a szervezet által meghatározott kivételekkel; ésegyértelmű visszajelzést ad a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.69. |
| Az EIR:A név- és címfeloldási kérésekre a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosít.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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.71. |
| Az EIR eredet-hitelesítést és adatsértetlenség-ellenőrzést kér és hajt végre a hiteles forrásból származó név- és címfeloldó válaszokon. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### A folyamatok elkülönítése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 17.108. |
| Az EIR elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

## RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

### Szabályzat és eljárásrendek

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 18.1. |
| A szervezet:Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerinta szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és információsértetlenségi szabályzatot, amelymeghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbáösszhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.a rendszer- és információsértetlenségi eljárásrendet, amely a rendszer- és információsértetlenségi szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.Kijelöl egy meghatározott személyt, aki a rendszer- és információsértetlenségi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.Felülvizsgálja és frissíti az aktuális rendszer- és információsértetlenségi szabályzatot és a rendszer- és információsértetlenségi eljárásokat a meghatározott gyakorisággal és a meghatározott események bekövetkezését követően. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Hibajavítás

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 18.2. |
| A szervezet:Azonosítja, jelenti és kijavítja az EIR hibáit.A hibajavítással kapcsolatos szoftverfrissítéseket telepítés előtt teszteli a hatékonyság és a potenciális mellékhatások szempontjából.A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti.A hibajavítást beépíti a szervezet konfigurációkezelési folyamatába. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Kártékony kódok elleni védelem

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 18.8. |
| A szervezet:Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat.A védelmi mechanizmusokat automatikusan frissíti minden olyan esetben, amikor új verziók jelennek meg összhangban a szervezet konfigurációkezelési szabályaival.A kártékony kódok elleni védelmi mechanizmusokat úgy konfigurálja, hogy: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.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.Ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az EIR rendelkezésre állására. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Az EIR monitorozása

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 18.13. |
| A szervezet:Monitorozza a rendszert, hogy észlelje:A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal;Az engedély nélküli helyi, hálózati és távoli kapcsolatokat.Azonosítja a rendszer jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával.Aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket:az egész rendszerre kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetvea rendszeren belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében.Elemzi az észlelt eseményeket és rendellenességeket.Módosítja a rendszerfelügyeleti tevékenység szintjét, amikor változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szint.Jogi állásfoglalást kér a rendszerfelügyeleti tevékenységekről.Biztosítja a szervezet által meghatározott rendszerfelügyeleti információkat a meghatározott személyeknek vagy szerepköröknek a szervezet által meghatározott gyakorisággal. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Biztonsági riasztások és tájékoztatások

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 18.37. |
| A szervezet:Folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat.Szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat készít.Biztonsági riasztásokat, tanácsokat és iránymutatásokat ad ki a meghatározott személyeknek vagy szerepkörökben dolgozóknak, a kijelölt szervezeti egységeknek és a kijelölt külső szervezeteknek.A biztonsági iránymutatásokat az azokban foglaltak szerint alkalmazza. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

### Információ kezelése és megőrzése

|  |  |  |
| --- | --- | --- |
| Követelmény:  | Biztonsági osztály: | **Alap** |
| [ ]  Rendszer specifikus  [ ]  Általános [ ]  Hibrid [ ]  Nem alkalmazható  | Referencia (7/2024 MK):  | 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. |
| A védelmi intézkedés státusza (csak egy választható):[ ]  Megvalósítva    [ ]  Részben megvalósítva    [ ]  Nincs megvalósítva |
| **Védelmi intézkedés** (tervezett) **megvalósításának részletei** |
|  |

Jóváhagyta:

|  |
| --- |
| Név: |
| Beosztás: |
|  |

Kelt: <város>, <dátum>