**Információbiztonsági terv**

**-**

**DIMOP pályázat keretében fejlesztendő informatikai rendszerek tervezéséhez**

**A Dokumentum Adatai**

|  |  |
| --- | --- |
| **Cím** | Információbiztonsági terv |
| **Leírás** | Jelen dokumentum támogatást kíván adni az új elektronikus információs rendszer bevezetési projektek során szállítandó rendszerek előzetes biztonsági követelményeinek meghatározásához. |
| **Biztonsági besorolás** | Nyilvános |

**Változatok**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kiadás dátuma** | **Szerző** | **Cégnév** | **Verzió** | **Leírás** |
|  |  |  |  |  |

Tartalomjegyzék

[Információbiztonsági terv célja és hatóköre 4](#_Toc128811435)

[Információbiztonsági terv készítésének szempontjai 4](#_Toc128811436)

[Információbiztonsági terv felülvizsgálata 4](#_Toc128811437)

[Az EIR biztonsági követelményei 5](#_Toc128811438)

[Biztonsági osztályba sorolás 5](#_Toc128811439)

[Adatok azonosítása, adatvagyon felmérése 5](#_Toc128811440)

[Fenyegetettség meghatározása 6](#_Toc128811441)

[Biztonsági osztályba sorolás eredménye 6](#_Toc128811442)

[Vonatkozó jogszabályok 7](#_Toc128811443)

[Az EIR feladata és környezete 8](#_Toc128811444)

[Rendszer (alap)feladata, szolgáltatásai 8](#_Toc128811445)

[Rendszer funkciói 8](#_Toc128811446)

[Az EIR felépítése, fizikai és logikai környezete 8](#_Toc128811447)

[Felhasználói szerepek és felelősségek 9](#_Toc128811448)

[Biztonsági célok és vonatkozó követelmények 11](#_Toc128811449)

[Adminisztratív védelmi intézkedések - 1. számú melléklet 11](#_Toc128811450)

[Fizikai védelmi intézkedések - 2. számú melléklet 12](#_Toc128811451)

[Logikai védelmi intézkedések - 3. számú melléklet 12](#_Toc128811452)

[Fogalmak és rövidítések 12](#_Toc128811453)

[1. számú melléklet – Adminisztratív védelem 14](#_Toc128811454)

[2. számú melléklet – Fizikai védelem 24](#_Toc128811455)

[3. számú melléklet – Logikai védelem 28](#_Toc128811456)

Információbiztonsági terv célja és hatóköre

Az Információbiztonsági terv célja a Projektgazda szervezet (továbbiakban: Szervezet) számára elősegíteni a 2013. évi L. törvény 11. §-ának (1) bekezdés a) pontja alapján biztosítja az elektronikus információs rendszerre (továbbiakban: EIR) irányadó biztonsági osztály tekintetében meghatározott követelmények teljesülését, valamint a 41/2015. (VII. 15.) BM rendelet (az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről) alapján, támogatást nyújtani az EIR tervezése során előzetesen (azaz a követelmények specifikálási fázisában) megállapított biztonsági osztálynak megfelelő követelmények megvalósításához, továbbá az EIR-re és az EIR fejlesztőire, valamint az EIR dokumentációjára értelmezhető követelmények meghatározása.

Az Információbiztonsági terv célja továbbá az EIR tervezéséhez kapcsolódó, a fejlesztéssel kapcsolatos biztonsági előírások és funkciók bemutatása, a rendszerbiztonsági terv elkészítésének elősegítése, összhangban a Műszaki Kiírásban, a hatályos jogszabályokban és a Szervezet belső szabályzataiban foglaltakkal.

Az Információbiztonsági terv hatóköre kiterjed az EIR fejlesztéséhez kapcsolódó védelmi intézkedések megvalósítására és az EIR oldali interfészek fejlesztésére. Az Információbiztonsági terv tartalmazza a fejlesztéshez kapcsolódó azon információkat, melyek az EIR információbiztonsági követelményeknek megfelelő tervezéséhez, fejlesztéséhez és üzemeltetéséhez szükségesek.

Információbiztonsági terv készítésének szempontjai

A dokumentum tartalmában meg kell feleljen a Szervezetre vonatkozó belső és külső szabályozások elvárásainak.

A dokumentum tartalmazza EIR-rel kapcsolatos alap információkat, annak folyamatait, feladatait oly módon, hogy ezek betartása esetén az EIR biztonságosan, az érvényes szabályozásoknak megfelelő módon használható legyen.

Az Információbiztonsági terv tartalmazza az EIR informatikai biztonsági implementációjának műszaki elvárásait.

Információbiztonsági terv felülvizsgálata

A Információbiztonsági terv rendszeres felülvizsgálata és naprakészen tartása szükséges az EIR-ben vagy annak üzemeltetési környezetében, a tervezési fázisban meghatározott állapothoz képest bekövetkező változások esetén, valamint az EIR fejlesztése vagy a tervezett védelmi intézkedések implementálása és értékelése kapcsán szükséges változtatások alapján.

Az EIR biztonsági követelményei

Annak érdekében, hogy a Szervezet által használt és az Ibtv. hatálya alá tartozó Rendszer, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az EIR-t biztonsági osztályba kell sorolni a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjait figyelembe véve.

Az Információbiztonsági terv alapul veszi és rögzíti a szervezet által előzetesen meghatározott biztonsági osztályt, valamint a kapcsolódó biztonsági elvárásokat.

Az előzetes biztonsági osztályba sorolás elvégzéséhez NBSZ NKI ajánlás „Biztonsági osztályba sorolási útmutató DIMOP pályázat keretében fejlesztendő informatikai rendszerek előzetes besorolásához” érhető el:(https://nki.gov.hu/it-biztonsag/tudastar).

Biztonsági osztályba sorolás

Annak érdekében, hogy az EIR-ek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az EIR-eket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.

Az EIR biztonsági osztálya az EIR védelmének elvárt erőssége. A biztonsági osztályba sorolással a releváns kockázatok alapján meghatározásra kerül az EIR védelmének elvárt erőssége.

A biztonsági osztályba sorolás alkalmával - az érintett EIR vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig kerül számozásra. Minél magasabb biztonsági osztályba kerül besorolásra egy EIR, annál szigorúbb védelmi követelmények meghatározása szükséges.

Figyelembe véve a Szervezet, EIR által kezelt adatainak jellegét, azok mennyiségét, az EIR sértetlenségre és rendelkezésre állásra vonatkozó Szervezeti igényt, továbbá a 41/2015. (VII. 15.) BM rendelet szempontrendszerét, az EIR fejlesztéshez kapcsolódóan meg kell határozni az EIR biztonsági osztályát (lsd.: Biztonsági osztályba sorolási útmutató, A biztonsági osztályba sorolás folyamata fejezet).

Adatok azonosítása, adatvagyon felmérése

Az EIR-ben szükséges a kezelt, tárolt, feldolgozott és továbbított adatok meghatározása és kategorizálása annak érdekében, hogy azok fontosságuknak megfelelő védelmet kaphassanak.

A biztonsági osztályba sorolás első lépéseként azonosított, az EIR által kezelt adatok kategóriáit, mennyiségét és a várható megőrzési időt, az Információbiztonsági tervben rögzíteni szükséges.

Az EIR által kezelt, vagy feldolgozott adatok (szükség szerint az adatkategóriák bővíthetőek):

|  |  |  |
| --- | --- | --- |
| Adat kategóriák | Adatok mennyisége  (csekély, közepes, nagy, jelentős mennyiség) | Adatmegőrzési idő  (min/max) |
| nyilvános adat |  |  |
| belső használatú adat |  |  |
| számlázási adat |  |  |
| ügyféladat |  |  |
| bizalmas adat |  |  |
| személyes adat |  |  |
| különleges adat |  |  |
| bűnügyi személyes adat |  |  |
| közérdekű adat |  |  |
| közérdekből nyilvános adat |  |  |
| minősített adat |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Adatmegőrzési idő az adott adatkategóriára meghatározott szervezeti, jogszabályi vagy egyéb szabályok szerint meghatározott adat kezelési/megőrzési idő.

Fenyegetettség meghatározása

A fenyegetés olyan lehetséges külső vagy belső irányultságú tényező, művelet vagy esemény, amely sértheti az EIR elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az EIR védettségét, biztonságát. A fenyegetettségek feltárása az eddigi tapasztalatok felhasználásával, illetve az EIR elemzéséből felderített hiányosságok számbavételével történhet (ld.: Biztonsági osztályba sorolási útmutató, Fenyegetettségek meghatározása fejezet), melynek eredményét az Információbiztonsági tervben rögzíteni szükséges.

A szervezet által az EIR-re vonatkozóan értelmezett releváns fenyegetések:

|  |  |
| --- | --- |
| **Fenyegető tényezők** | **Megjegyzések** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Biztonsági osztályba sorolás eredménye

A Szervezet elvégezte az EIR által kezelt vagy feldolgozott adatok azonosítását, az adatvagyon felmérését, az adatokkal kapcsolatos kárértékek beazonosítását, valamint a releváns fenyegetések meghatározását. A 41/2015. (VII. 15.) BM rendelet szempontrendszerét figyelembe véve, az EIR fejlesztéshez kapcsolódóan az:

alábbi biztonsági osztályba került besorolásra:

* Bizalmasság: (2-5)
* Sértetlenség: (2-5)
* Rendelkezésre állás: (2-5).

Vonatkozó jogszabályok

A Szervezet a tervezett EIR fejlesztéséhez kapcsolódóan az alábbi vonatkozó belső és külső szabályokat (például jogszabályokat) azonosította:

* Szervezeti belső szabályozás
* Külső szabályok

Az EIR feladata és környezete

Az Információbiztonsági tervben az EIR olyan mélységben kerül bemutatásra, ami az EIR-rel kapcsolatos védelmi szabályozások és folyamatok megértéséhez szükséges. Ismertetésre kell kerüljön az EIR célja, feladata, szolgáltatásai, moduljai, fő funkciói és információbiztonsági szempontjából releváns tulajdonságai.

Dokumentálni kell továbbá az EIR-rel szemben támasztott alapvető üzleti követelményeket, a támogatott üzleti folyamatokat, a folyamatokkal szemben támasztott követelményeket.

Az EIR főbb funkcionális elemeit kell felsorolni, illetve célszerű ábrázolni az azok közötti főbb kapcsolatokat és adatáramlásokat. Szerepeltetni kell a központi biztonsági infrastruktúrával (például tűzfal rendszer, LDAP stb.) való kapcsolatokat is.

Rendszer (alap)feladata, szolgáltatásai

A fejezet céljaz EIR feladatának, biztosított szolgáltatásainak meghatározása, valamint az EIR-rel szemben támasztott alapvető üzleti követelmények, a támogatott üzleti folyamatok, a folyamatokkal szemben támasztott követelmények.

Rendszer funkciói

A fejezet tartalmazza az EIR által támogatott feladatokhoz kapcsolódó főbb funkciók meghatározását, például:

* adatgyűjtés,
* adattárolás,
* adattovábbítás,
* adatbázis kezelés,
* digitális aláírás,
* titkosítás,
* felhasználó kezelés,
* naplózás,
* távoli elérés.

Az EIR felépítése, fizikai és logikai környezete

A fejezet célja (amennyiben a projekt jelenlegi fázisában ismertek) az EIR tervezett elérhetőségének, működési környezetének bemutatása, az engedélyezett hálózati kapcsolatainak, biztonsági zónáinak, a futtató környezetének meghatározása (amennyiben a fejlesztéshez kapcsolódóan releváns).

Fizikai környezet ismertetése tartalmazza az EIR és a rendszerelemek fizikai elhelyezését, a fizikai védelmi megoldásokat. (például x adatközpont, beléptető és kamera rendszer, biztonsági őrség stb.).

* Infrastruktúra típusa,
* Támogató rendszerek,
* Hálózati védelem (például tűzfal, proxy, IDS/IPS stb.),
* Rendszer platform,
* Fejlesztési programnyelv és komponenskészletek,
* Operációs rendszer,
* Alkalmazásszerver,
* Adatbáziskezelő(k),
* Alapvető biztonsági beállítások (rendszer, operációs rendszer szervezet által elvárt alap biztonsági beállításai).

Architektúra ábra és az EIR kapcsolatai

Az Információbiztonsági tervnek tartalmaznia kell az EIR külső és belső kapcsolatainak, a felhasználói, üzemeltetői és egyéb hozzáférési kapcsolatainak ismertetését. Cél annak biztosítása, hogy a Szervezet jelenlegi vagy jövőbeli rendszereihez történő kapcsolódás illeszkedjen a Szervezet üzemeltetési gyakorlatához, a működő szolgáltatások működése és működtetése zavartalan legyen.

Külön ki kell térni azokra az esetekre, amikor az EIR-t nem a Szervezet belső informatikai hálózatából érik el (például távoli elérés, távmunka, internet kapcsolat, más informatikai hálózatokkal kialakított kapcsolat stb.). Az egyes kapcsolatok esetén jelölni kell a kialakítandó authentikációs megoldást, valamint az elvárt titkosítási megoldást. Meg kell határozni, hogy az adott kapcsolatot melyik rendszer kezdeményezi, és milyen módon (a kapcsolatokat javasolt ábrázolni).

* Belső kapcsolatok (egyéb szervezeti vagy fejlesztett rendszerek, szervezeti belső hálózat, VLAN-ok)
* Külső kapcsolatok (NTG, internet szolgáltató)
* Publikus kapcsolatok (webes felületek)

Felhasználói szerepek és felelősségek

A fejezet célja az EIR meghatározott funkcióiban elérhető adat kategóriák összerendelése az egyes felhasználói szerepekkel és felelősségekkel.

Meg kell határozni az EIR-hez kapcsolódóan kialakítandó szerepköröket, például:

* Belső felhasználók
* Külső felhasználók (például szupport, külső fejlesztő, külső szakértő stb.)
* Privilegizált felhasználók (például alkalmazás üzemeltető, szerver üzemeltető, infrastruktúra üzemeltető, fejlesztő stb.)
* Technikai felhasználók
* Információbiztonsági felhasználó (például auditor, biztonsági manager, biztonsági adminisztrátor stb.)

Táblázatos formában fel kell sorolni az EIR meghatározott funkcióit és adatkategóriáit mely szerepkörök érhetik el.

|  |  |  |
| --- | --- | --- |
| **Funkció** | **Adat kategória** | **Szerepkör** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Biztonsági célok és vonatkozó követelmények

Az EIR-re vonatkozó biztonsági elvárások meghatározásának célja az EIR és az általa kezelt adatok kockázatokkal arányos védelmének kialakítása, a jogosulatlan hozzáférés elkerülése, az elvárt rendelkezésre állási követelmények teljesítése. Valamint a jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedések meghatározása.

Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény hatálya alá tartozó EIR-ek teljes életciklusában meg kell valósítani és biztosítani kell az EIR-ben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az EIR és elemeinek sértetlenségét és rendelkezésre állását, valamint a poszt-kvantumtitkosítás alkalmazásra kötelezett szervezetek esetén a fizikailag elkülönített helyszíneik közötti kormányzati célú hálózaton, továbbá a publikus internet felületen zajló, az elektronikus hírközlési törvény szerinti szolgáltató igénybevételével vagy egyéb információs társadalommal összefüggő szolgáltatásaik igénybevétele során a hagyományos kriptográfiai alkalmazáson felüli biztonságot nyújtó poszt-kvantum titkosítási alkalmazással történő zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

A meghatározott logikai, fizikai és adminisztratív védelmi intézkedések támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, valamint a biztonsági események kezelését.

Az alábbi melléketek (1., 2., 3., mellékletek) alapján meg kell adni a fejlesztés, valamint a meghatározott biztonsági osztály szempontjából releváns, válogatott kontrollokat. Amennyiben egyes kontrollok nem értelmezettek, értelmezhetőek az adott Rendszer vonatkozásában, megfelelő indoklás mellett kizárhatók.

Adminisztratív védelmi intézkedések - 1. számú melléklet

Adminisztratív védelem az EIR védelme érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás összessége. Ide tartoznak például az EIR biztonságával kapcsolatos dokumentumok és a Szervezet által kialakított folyamatok, például:

* Szabályzatok, utasítások és eljárásrendek,
* Üzemeltetési dokumentumok (operációs rendszer, adatbázis üzemeltetési leírásai, telepítési útmutatók stb.),
* Felhasználói dokumentumok (felhasználói kézikönyvek, oktatási dokumentumok stb.)
* Fejlesztői dokumentumok (fejlesztői módszertan, fizikai-, logikai- adatmodell, rendszerterv, tesztelési terv stb.)

Fizikai védelmi intézkedések - 2. számú melléklet

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. Cél a jogosulatlan fizikai hozzáférés, károkozás és zavarás megelőzése. Ide tartozik a fizikai határok meghatározása, a beléptetési intézkedések, a helyiségek felügyelete, külső és környezeti fenyegetésekkel szembeni védelem.

Logikai védelmi intézkedések - 3. számú melléklet

Logikai védelem, az EIR-ben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. Célja a Szervezeti információkhoz és rendszerekhez és alkalmazásokhoz történő hozzáférés korlátozása, a jogosult hozzáférés biztosítása, a jogosulatlan hozzáférés megakadályozása, alkalmas és hatásos titkosítási megoldások kialakítása, észlelő, megelőző és helyreállító védelmi intézkedések megvalósítása a kártékony kódok ellen, nyilvántartani a felhasználói tevékenységeket, rendellenességeket, hibákat, biztonsági eseményeket.

A 41/2015. (VII. 15.) BM rendelet 4. melléklete alapján meghatározott követelménycsoportok:

* Általános védelmi intézkedések,
* Tervezés,
* Rendszer és szolgáltatás beszerzés,
* Biztonsági elemzés,
* Tesztelés, képzés és felügyelet,
* Konfigurációkezelés,
* Karbantartás,
* Adathordozók védelme,
* Azonosítás és hitelesítés,
* Hozzáférés ellenőrzése,
* Rendszer- és információsértetlenség,
* Naplózás és elszámoltathatóság,
* Rendszer- és kommunikációvédelem.

Fogalmak és rövidítések

Releváns fogalmak, rövidítések és a kapcsolódó magyarázatok, melyek az Információbiztonsági tervben használt tartalom megértését és értelmezését segítik.

|  |  |
| --- | --- |
| adminisztratív védelem | a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás |
| bizalmasság | az EIR 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 EIR-ben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az EIR által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül |
| biztonsági esemény kezelése | az EIR-ben 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 EIR védelmének elvárt erőssége |
| biztonsági osztályba sorolás | a kockázatok alapján az EIR védelme elvárt erősségének meghatározása |
| EIR | - az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat,  - minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi |
| EIR biztonsága | az EIR olyan állapota, amelyben annak védelme az EIR-ben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az EIR elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos |
| 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 |
| logikai védelem | az EIR-ben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem |
| rendelkezésre állás | annak biztosítása, hogy az EIR-ek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek |
| 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 EIR elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az EIR eleme rendeltetésének megfelelően használható |

1. számú melléklet – Adminisztratív védelem

Az adminisztratív védelem, a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás. (A 2. biztonsági osztályhoz tartozó adminisztratív követelmények ebben a relációban külön nem értelmezhetők a fejlesztőre, ezeket az 1. biztonsági osztályhoz tartozó követelmények tartalmazzák.)

**1. biztonsági osztályú Rendszer követelményei**

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.1.1.1.3. gondoskodik arról, hogy az informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható; | | 1 |
| Szervezeti feladat: | | |
| A Szervezet gondoskodik róla, hogy az Informatikai biztonsági szabályzat vagy annak a fejlesztő számára releváns része megismerhető legyen. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő megismeri a rá vonatkozó elvárásokat és annak megfelelően végzi fejlesztési feladatát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.1.1.2.4. Az érintett szervezet meghatározza a tevékenységhez kapcsolódó felelősséget; | | 1 |
| Szervezeti feladat: | | |
| A Szervezet gondoskodik róla, hogy meghatározza a fejlesztési tevékenységhez kapcsolódó felelősségeket. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő megismeri a fejlesztéshez kapcsolódó felelősségeket és annak megfelelően végzi fejlesztési feladatát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.1.1.3.8. Az informatikai biztonsági szabályzat szabályozza az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatokat, elvárásokat, jogokat (ha az érintett szervezetnél ez értelmezhető); | | 1 |
| Szervezeti feladat: | | |
| A Szervezet gondoskodik róla, hogy a fejlesztő megismerje rendszer biztonsági beállításával kapcsolatos feladatokat, elvárásokat, jogokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő megvalósítja a rendszer biztonsági beállításával kapcsolatos feladatokat, teljesíti elvárásokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.4.1.2. Az érintett szervezet megszünteti vagy visszaveszi a személy egyéni hitelesítő eszközeit; | | 1 |
| Szervezeti feladat: | | |
| A szervezet megszünteti vagy visszaveszi a Fejlesztő egyéni hitelesítő eszközeit. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő visszaszolgáltatja a részére átadott egyéni hitelesítő eszközöket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.4.1.3. Az érintett szervezet tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről; | | 1 |
| Szervezeti feladat: | | |
| A Szervezet tájékoztatja a Fejlesztőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségeiről. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő tudomásul veszi és megfelel a reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségeknek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.9.1.1. Az érintett szervezet tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét; | | 1 |
| Szervezeti feladat: | | |
| A Szervezet tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a Szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét megelőzi. | | |

**3. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 3. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 1. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.1.1. Az érintett szervezet, ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti az adminisztrátori dokumentációt, amely tartalmazza a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.1.2. Az érintett szervezet, ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza a biztonsági funkciók hatékony alkalmazását és fenntartását. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti az adminisztrátori dokumentációt, amely tartalmazza a biztonsági funkciók hatékony alkalmazását és fenntartását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.1.3. Az érintett szervezet, ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti az adminisztrátori dokumentációt, amely tartalmazza a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.2.1. Az érintett szervezet megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti a felhasználói dokumentációt, amely tartalmazza a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.2.2. Az érintett szervezet megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti a felhasználói dokumentációt, amely tartalmazza a Rendszer biztonságos használatának módszereit. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.2.3. Az érintett szervezet megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elkészíti a felhasználói dokumentációt, amely tartalmazza a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.3. Az érintett szervezet gondoskodik arról, hogy az információs rendszerre vonatkozó - különösen az adminisztrátori és fejlesztői - dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható; | | 3 |
| Szervezeti feladat: | | |
| A szervezet gondoskodik arról, hogy az információs rendszerre vonatkozó dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő gondoskodik arról, hogy az információs rendszerre vonatkozó dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.4.1.4. Az érintett szervezet gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet gondoskodik a Rendszer dokumentációknak meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő gondoskodik a Rendszer dokumentációknak meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.5.6.1.1. Az érintett szervezet mindenkitől, aki az elektronikus információs rendszerrel, vagy azok elhelyezésére szolgáló objektummal kapcsolatban áll megköveteli, hogy jelentsék a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet megköveteli, hogy a Fejlesztők jelentsék a fejlesztéshez kapcsolódó, esetleges biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlelnek, melyhez meghatározott csatornát biztosít. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a fejlesztéshez kapcsolódó, esetleges a biztonsági esemény bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlel jelenti a Szervezet által meghatározott csatornán keresztül. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.2.1.2. Az érintett szervezet felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet felméri, hogy a Rendszer fejlesztés jelent-e nemzetbiztonsági ellenőrzés alá eső feladatot, ellenőrzi, hogy a Fejlesztő rendelkezik-e megfelelő feltételekkel. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő teljesíti a nemzetbiztonsági ellenőrzést igénylő feladat elvégzéséhez szükséges feltételeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.6.1.1. Az érintett szervezet a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg az érintett szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározza a Szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, valamint a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.6.1.2. Az érintett szervezet szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg az érintett szervezet által meghatározott személybiztonsági követelményeknek; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza és megköveteli a Fejlesztőre vonatkozó személybiztonsági követelményeket. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő teljesíti a vonatkozó személybiztonsági követelményeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.6.1.3. Az érintett szervezet a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza és megköveteli a Fejlesztőre vonatkozó személybiztonsági követelményeket. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő dokumentálja a vonatkozó személybiztonsági követelményeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.6.1.4. Az érintett szervezet előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett szervezetnek; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor a meghatározott csatornán, soron kívül küldjön róla értesítést. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő értesítést küld a meghatározott csatornán, a Szervezet kijelölt kapcsolattartójának, a szervezetében történt, fejlesztéshez kapcsolódóan releváns személyi változásokról. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.6.6.1.5. Az érintett szervezet folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet folyamatosan ellenőrzi a szerződő fél személybiztonsági követelményeknek való megfelelését. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő igazolja a személybiztonsági követelményeknek való megfelelését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.7.5.1.1. Az érintett szervezet szerepkör vagy feladat alapú biztonsági képzést nyújt az egyes szerepkörök szerinti, azért felelős személyeknek az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően; | | 3 |
| Szervezeti feladat: | | |
| A Szervezet belső szabályai szerint biztonsági képzést nyújt a Fejlesztő részére, a fejlesztési feladat végrehajtását megelőzően. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő részt vesz a Szervezet által nyújtott biztonsági képzésen. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.7.6.1.2. Az érintett szervezet a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő, a Szervezet által nyújtott biztonsági képzés megtörténtét dokumentált módon elismeri. | | |

**4-es biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 4. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 1. és 3. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.3.2.2. Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő az Információbiztonsági terv részeként, a logikai védelmi intézkedések között meghatározza az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak leírását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.3.3. Az érintett szervezet szerződéses követelményként meghatározza a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő létre hozza és rendelkezésére bocsátja az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas és alacsony szintű biztonsági tervet, - ha azzal a szállító rendelkezik - a forráskódot és futtatókörnyezetet. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.3.4. Az érintett szervezet szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy már a fejlesztési életciklus korai szakaszában meghatározza a használatra tervezett funkciókat, protokollokat és szolgáltatásokat. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő az Információbiztonsági terv, Rendszer funkciói pontban meghatározott, tervezett funkciókban, protokollokban és szolgáltatásokban történt módosulásokat naprakészen tartja. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.3.8.2 Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmazhat az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi független értékelők vagy értékelő csoportok alkalmazhatóságát az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.4.9.2. Az érintett szervezet tranzakció alapú elektronikus információs rendszerek esetén tranzakció helyreállítást hajt végre. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a tranzakció alapú elektronikus információs rendszerek esetén a tranzakció helyreállítás lehetőségét. | | |

**5. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 5. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 1.; 3. és 4. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.1.4.2.5. Meg kell tervezni a folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást. | | 5 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő közreműködik a Rendszer folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitás tervezésében. | | |

2. számú melléklet – Fizikai védelem

A 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.

**2-es biztonsági osztályú Rendszer követelményei**

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.2.1.1 Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti az elektronikus információs rendszerek szempontjából érintett létesítményekre vagy helyiségekre érvényes fizikai védelmi eljárásrendet, amely az érintett szervezet elektronikus információbiztonsági, vagy egyéb szabályzatának részét képező fizikai védelmi szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet, a Fejlesztő részére elérhetővé teszi a fizikai védelmi eljárásrendet, vagy annak vonatkozó részeit. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő betartja a Szervezet fizikai védelmi eljárásrendjében foglaltakat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.3.1.1. Az érintett szervezet összeállítja, jóváhagyja, és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját; | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározza a belépési jogosultsági igényeket, kezdeményezi azok Szervezet általi jóváhagyását. | | |

**3. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 3-as biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 2-es biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.12.1. Az érintett szervezet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint biztosítja a Rendszer tűzészlelő képességét és a megfelelő tűzelfojtó berendezéseket. | | |

**4. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 4.biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 1. és 3. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.9. Az érintett szervezet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint gondoskodik a Rendszert árammal ellátó berendezéseinek és a kábelezésének sérüléssel és rongálással szembeni védelméről. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.9.1. Az érintett szervezet az elsődleges áramforrás kiesése esetére, a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint gondoskodik a Rendszer szünetmentes áramellátásáról. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.10.1.3. Az érintett szervezet megakadályozza a jogosulatlan vészkikapcsolást. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint lehetővé teszi a Rendszer védelmét, a jogosulatlan vészkikapcsolás ellen. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.12.2. Az érintett szervezet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint biztosítja a Rendszer automatikus tűzelfojtási képességét. | | |

**5. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 5. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 2. és 4. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.4.2. Az érintett szervezet a létesítménybe történő fizikai belépés ellenőrzésén túl külön engedélyhez köti a fizikai belépést az elektronikus információs rendszereknek helyt adó helyiségekbe is. | | 5 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározza az elektronikus információs rendszereknek helyt adó helyiségekbe történő belépési jogosultsági igényeket, kezdeményezi azok Szervezet általi engedélyezését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.2.1.9.2. Az érintett szervezet az elsődleges áramforrás kiesése esetén biztosítja a hosszútávú tartalék áramellátást az elektronikus információs rendszer minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására. | | 5 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint biztosítja a Rendszer hosszútávú tartalék áramellátását. | | |

3. számú melléklet – Logikai védelem

A logikai védelem az EIR-ben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

**2. biztonsági osztályú Rendszer követelményei**

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.2.2.1. Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít […] | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő közreműködik az elektronikus információs rendszerhez rendszerbiztonsági terv elkészítésében, a rá vonatkozó tartalmat a Szervezet által meghatározott módon és formában elkészíti. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.2.4.1.2. Az érintett szervezet az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.10.1.1. Az érintett szervezet kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a Rendszer vonatkozásában kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi vagy más jogszabályoknak. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.7.1.1.1. Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározza a Rendszer vonatkozásában releváns karbantartási feladatokat, rendszerességét és elvégzési módját. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.8.7.1. Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő figyelembe veszi és betartja a Szervezet adathordozók használatára vonatkozó szabályait. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer konfigurációját a követelménypont szerint. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi, hogy a Rendszerben a felhasználók és az általuk végzett tevékenységek egyedileg azonosíthatóak és hitelesíthetőek legyenek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.1. Az érintett szervezet az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a Rendszerben használni kívánt egyéni-, csoport-, szerepkör- vagy eszközazonosítókat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a Szervezet által meghatározott egyéni-, csoport-, szerepkör- vagy eszközazonosítók használatát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.3. Az érintett szervezet meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az azonosítók ismételt felhasználására vonatkozó időtartamot. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben az azonosítók ismételt felhasználására vonatkozó időtartam beállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.4. Az érintett szervezet meghatározott időtartamú inaktivitás esetén letiltja az azonosítót. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az azonosítók letiltás előtti inaktivitási idejét. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben az inaktív azonosítók letiltását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.10.1.1. Az érintett szervezet kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak. | | 2 |
| Szervezeti feladat: | | |
| A szervezet kizárólag a követelménypont szerinti szoftvereket használ. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a Rendszer vonatkozásában kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi vagy más jogszabályoknak. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.7.1.1.1. Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely a rendszer karbantartási kezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározza a Rendszer vonatkozásában releváns karbantartási feladatokat, rendszerességét és elvégzési módját. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.8.7.1. Az érintett szervezet engedélyezi, korlátozza, vagy tiltja egyes, vagy bármely adathordozó típusok használatát a meghatározott elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő figyelembe veszi és betartja a Szervezet adathordozók használatára vonatkozó szabályait. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi, hogy a Rendszerben a felhasználók és az általuk végzett tevékenységek egyedileg azonosíthatóak és hitelesíthetőek legyenek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.1. Az érintett szervezet az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a Rendszerben használni kívánt egyéni-, csoport-, szerepkör- vagy eszközazonosítókat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a Szervezet által meghatározott egyéni-, csoport-, szerepkör- vagy eszközazonosítók használatát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.3. Az érintett szervezet meghatározott időtartamig megakadályozza az azonosítók ismételt felhasználását. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az azonosítók ismételt felhasználására vonatkozó időtartamot. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben az azonosítók ismételt felhasználására vonatkozó időtartam beállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.4.1.4. Az érintett szervezet meghatározott időtartamú inaktivitás esetén letiltja az azonosítót. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az azonosítók letiltás előtti inaktivitási idejét. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben az inaktív azonosítók letiltását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.2. Az érintett szervezet meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatot. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a hitelesítésre szolgáló eszköz kezdeti tartalmának beállítását az iparági jó gyakorlatok alapján. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.3. Az érintett szervezet biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatot. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben, a Szervezet által meghatározott a hitelesítésre szolgáló eszközök használatát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.4. Az érintett szervezet dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközök letiltását, vagy kialakítja a Rendszer központi címtárral vagy KAÜ-vel való együttműködését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.5. Az érintett szervezet megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékének módosítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.6. Az érintett szervezet meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a hitelesítésre szolgáló eszközök használati idejének beállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.7. Az érintett szervezet a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a hitelesítésre szolgáló eszközök megváltoztatásának kikényszerítését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.1.8. Az érintett szervezet megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben, a hitelesítésre szolgáló eszközök bizalmas, titkosított tárolását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.6. Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a hitelesítési folyamatban a fedett visszacsatolást. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.8.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett szervezeten kívüli felhasználókat és tevékenységüket. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a szervezeten kívüli felhasználók és tevékenységük egyedi azonosítását és hitelesítését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.8.2. Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez. | | 2 |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványok elfogadását, szervezeten kívüli felhasználók hitelesítéséhez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.1.1. Az érintett szervezet meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő megvalósítja a Rendszerben a meghatározott fiók típusokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.3. Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a jóváhagyott jogosultságok szerinti logikai hozzáféréseket. Gondoskodik róla, hogy a jogosultságok engedély nélkül ne legyenek kiterjeszthetőek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.12.1.1. Az érintett szervezet kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani. | | 2 |
| Szervezeti feladat: | | |
| A Szervezet meg kell határozza azokat a felhasználói tevékenységeket, amelyeket a Rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a meghatározott azonosítás vagy hitelesítés nélkül is végrehajtható tevékenységek elvégzését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.3.1.1. Az érintett szervezet azonosítja, belső eljárásrendje alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit. | | 2 |
| Fejlesztői feladat: | | |
| A Fejlesztő kijavítja a Szervezet által azonosított és jelzett hibáit. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.4.1.1. Az érintett szervezet az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat. | | 2 |
| Fejlesztői feladat: | | |
| A Fejlesztő, amennyiben hatáskörébe tartozik gondoskodik a Rendszer kártékony kódok elleni védelméről. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.2.1.1. Az érintett szervezet meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a naplózható és naplózandó események beállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.3.1. Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a naplózandó események tartalmának beállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.8.1.1. Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben belső rendszerórák használatát a naplóbejegyzések időbélyegeinek előállításához. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.8.1.2. Az elektronikus információs rendszer időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben időbélyegek rögzítését a naplóbejegyzésekben, a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.9.1. Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a naplóinformációk védelmét a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.12.1.1. Az elektronikus információs rendszer biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott naplózható eseményekre. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a szükséges naplóbejegyzések generálását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.12.1.2. Az elektronikus információs rendszer lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározott személyeknek vagy szerepköröknek biztosítja a Rendszerben, a naplózható események kiválasztását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.12.1.3. Az elektronikus információs rendszer naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a szükséges naplóbejegyzések előállítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.1.1. Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját és elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszer belső és külső kommunikációinak felügyeletét és ellenőrzését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.1.2. Az elektronikus információs rendszer a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól. | | 2 |
| Fejlesztői feladat: | | |
| A Fejlesztő gondoskodik a nyilvánosan hozzáférhető rendszerelemek fizikailag szeparált vagy logikailag elkülönített alhálózatokban történő elhelyezéséről. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.10.1. Az érintett szervezet előállítja és kezeli az elektronikus információs rendszerben alkalmazott kriptográfiához szükséges kriptográfiai kulcsokat a kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó belső szabályozásnak megfelelően. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben kriptográfiai kulcsok kezelését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.11. Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveletek végrehajtását. | | |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.12. Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél. | | 2 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (például kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett szervezet engedélyezte azt. Biztosítja továbbá, hogy a Rendszer közvetlen kijelzést nyújtson ezen eszközök távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél. | | |

**3. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 3. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 2. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.3 Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő az Információbiztonsági terv Rendszer funkciói pontban pontjában meghatározott, tervezett funkciókban, protokollokban és szolgáltatásokban történt módosulásokat naprakészen tartja. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.5.3.1.1. Az érintett szervezet az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő támogatja a sérülékenység tesztet elvégzését, a feltárt hibák javítását a Rendszer átadását megelőzően elvégzi. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.7.1.1. Az érintett szervezet az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszer szolgáltatásainak konfigurálását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.7.1.2. Az érintett szervezet meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet a Fejlesztő részére átadja a meghatározott tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatára vonatkozó követelményeket. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő figyelembe veszi a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatára vonatkozó követelményeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.2. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi, hogy a Rendszer többtényezős hitelesítést alkalmazzon a különleges jogosultsághoz kötött felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.7. Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.7.1.1. Az elektronikus információs rendszer az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben, a felhasználók meghatározott időtartamon belüli, egymást követő sikertelen bejelentkezési kísérleteinek korlátozását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.7.1.2. Az elektronikus információs rendszer, ha a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a sikertelen bejelentkezési kísérletekre felállított esetszám korlát elérése esetén a felhasználói fiók automatikusan zárolását vagy meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.8.1.1. Az érintett szervezet az elektronikus információs rendszer felhasználásával az érintett szervezet által meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt […]. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a használatra vonatkozó figyelmeztető üzenet vagy jelzés megjelenítését a rendszerhez való hozzáférés engedélyezése előtt. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.8.2. Az elektronikus információs rendszer a figyelmeztető üzenetet vagy jelzést mindaddig a képernyőn tartja, amíg a felhasználó közvetlen műveletet nem végez az elektronikus információs rendszerbe való bejelentkezéshez vagy további rendszer hozzáféréshez. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a használatra vonatkozó figyelmeztető üzenet vagy jelzés megjelenítését, amíg a felhasználó közvetlen műveletet (például tudomásul vétel gomb megnyomása) nem végez bejelentkezéshez vagy további rendszer hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.8.3.1. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén kijelzi a rendszer használat feltételeit, mielőtt további hozzáférést biztosít. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a rendszer használat feltételeit. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a nyilvánosan elérhető Rendszerben a rendszer használat feltételeinek megjelenítését a hozzáférés biztosítása előtt. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.8.3.2. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén, ha felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a rendszer adatvédelmi szabályait. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a nyilvánosan elérhető Rendszerben, a rendszer adatvédelmi szabályoknak való megfelelés kijelzését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.8.3.3. Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén leírást biztosít a rendszer engedélyezett felhasználásáról. | | 3 |
| Szervezeti feladat: | | |
| A Szervezet elkészíti a rendszer engedélyezett felhasználásának leírását. | | |
| Fejlesztői feladat: | | |
| A nyilvánosan elérhető Rendszerben, a Fejlesztő lehetővé teszi a rendszer engedélyezett felhasználási leírásának megjelenítését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.13.1.1. Az érintett szervezet kidolgozza és dokumentálja minden engedélyezett távoli hozzáférés típusra a felhasználásra vonatkozó korlátozásokat, a konfigurálási vagy a kapcsolódási követelményeket és a megvalósítási útmutatókat. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a távoli hozzáférésre vonatkozó korlátozások megvalósítását, a konfigurálási vagy a kapcsolódási követelmények érvényesítését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.5.1.1. Az elektronikus információs rendszer naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő meghatározott csatornán (például e-mail, sms stb.) biztosítja riasztás küldését naplózási hiba esetén. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.5. Az elektronikus információs rendszer véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével. | | 3 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszer túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelmi megoldásait. | | |

**4. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 4. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 2. és 3. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.2.5.1.1. Az érintett szervezet (ha a hatókörébe tartozik, és ha más dokumentumban nem kerül meghatározásra, vagy azokból nem következik) elkészíti az elektronikus információs rendszer információbiztonsági architektúra leírását. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő közreműködik a Rendszer információbiztonsági architektúra leírásának elkészítésében, a szükséges információt biztosítja a Szervezet számára. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.4.1.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a fejlesztőtől a követelménypont szerinti dokumentumok átadását. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a változtatásokat végig vezeti a rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.4.1.2. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a fejlesztőtől a követelménypont szerinti dokumentumok átadását. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a változtatásokat dokumentálja, kezeli és ellenőrzi, valamint biztosítja ezek sértetlenségét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.4.1.3. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson. | | 4 |
| Szervezeti feladat: | | |
| A szervezet folyamatosan egyeztet a fejlesztővel a változtatásokról. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a változtatásokat kizárólag jóváhagyás után hajthatja végre. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.4.1.4. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a követelménypont szerinti dokumentumok átadását a fejlesztőtől. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő elvégzi a jóváhagyott változtatások és lehetséges biztonsági hatásaik dokumentálását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.4.1.5. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az érintett szervezet által meghatározott személyeknek. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő nyomon követi a Rendszer biztonsági hibáit és azok javításait, valamint meghatározott csatornán jelenti észrevételeit Szervezet által meghatározott személyeknek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.5.1.1. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a követelménypont szerinti dokumentumok átadását a fejlesztőtől. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztonságértékelési tervet készít és végrehajtja az abban meghatározott feladatokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.5.1.2. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az érintett szervezet által meghatározott lefedettség és mélység mellett. | | 4 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az egység-, integrációs-, rendszer-, vagy regressziós tesztelés kiértékelésének lefedettségét és mélységét. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a fejlesztéshez illeszkedő módon végrehajtja az egység-, integrációs-, rendszer-, vagy regressziós tesztelést. A Fejlesztő a Szervezet által meghatározott lefedettség és mélység mellett kiértékeli a teszteket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.5.1.3. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a követelménypont szerinti dokumentumok átadását a fejlesztőtől. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő dokumentálja a biztonságértékelési terv végrehajtását és ismerteti a biztonsági tesztelés és értékelés eredményeit. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.5.1.4. Az érintett szervezet megköveteli, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat. | | 4 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a követelménypont szerinti dokumentumok átadását, valamint a feltárt hiányosságok javítását a fejlesztőtől. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő kijavítja a biztonsági tesztelés és értékelés során feltárt hiányosságokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.7.3. Az érintett szervezet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját és megtiltja ezek futtatását. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő figyelembe veszi a Rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját és nem alkalmazza ezeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.3. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a többtényezős hitelesítést alkalmazását, a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.4. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a többtényezős hitelesítést alkalmazását, a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.5. Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat, a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.6. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a többtényezős hitelesítést, a felhasználói fiókokhoz való távoli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.7. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a többtényezős hitelesítést, a felhasználói fiókokhoz való távoli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.2.8. Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat a Rendszerben, a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.3. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi, vagy távoli hálózati kapcsolatot létesítene velük. | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszerben a meghatározott eszközök vagy eszköz típusok egyedi azonosítási és hitelesítési megoldását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.2.1.3. Az érintett szervezet a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást) és nem továbbítja. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő a Rendszert úgy alakítja ki, hogy abban jelszavak nem kerülnek tárolásra és továbbításra. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.2.1.4. Az érintett szervezet a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben, hogy a jelszavakra minimális és maximális élettartam korlátozás érvényre jusson, továbbá a Rendszerbe történő első lépést lehetővé tevő ideiglenes jelszó lecserélését kikényszeríti. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.3.1.2.1. Az érintett szervezet az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a tanúsítványok érvényességének ellenőrzését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.9.5.4. Az érintett szervezet a felhasználó egyedi (biometrikus) azonosítást lehetővé tevő tulajdonságai alapján végzi el az azonosítást (pl.: ujjlenyomat, retina letapogatás, és más hasonló). | | 4 |
| Szervezeti feladat: | | |
| A szervezet elvégzi az elektronikus információs rendszer követelménypont szerinti konfigurációját. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi a Rendszerben a felhasználó egyedi (biometrikus) azonosítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.2. Az elektronikus információs rendszer automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer fiókjainak kezeléséhez. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a fiókok automatizált mechanizmusokkal történő kezelését. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.3. Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja, vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, vagy egyes kijelölt felhasználói fiók típusokat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott időtartam letelte után automatikusan eltávolítsa, vagy letiltsa az egyes fiók típusokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.4. Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott időtartam letelte után automatikusan letiltsa az inaktív fiókokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.5. Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket. Ezekről meghatározott csatornán, meghatározott személyek vagy szerepkörök részére értesítést küldjön. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.5.1.3. Az érintett szervezet meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő érvényesíti a Szervezet által meghatározott hozzáférés jogosultságokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.6.1. Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáférések legyenek engedélyezettek. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.6.2. Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a hozzáférési jogosultságokat a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.6.5. Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer naplózza a privilegizált funkciók végrehajtását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.6.6. Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését vagy megváltoztatását. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben a nem privilegizált felhasználók privilegizált funkciókat ne hajthassanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését vagy megváltoztatását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.10.1.1. Az érintett szervezet meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben meghatározott időtartamú inaktivitás után vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásra kerüljön. | | |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.10.1.2. Az érintett szervezet megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben a munkaszakasz zárolás fenntartásra kerüljön mindaddig, amíg a felhasználó újra nem azonosítja és hitelesíti magát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.10.2. A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben a munkaszakasz zároláskor a képernyőn korábban látható információ elrejtésre kerüljön. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.11. Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben az automatikus munkaszakasz zárolást, valamint a zároláshoz szükséges feltételek beállíthatóságát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.13.3. Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben a távoli hozzáférés biztonságos titkosítással történő kialakítását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.13.4. Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer távoli hozzáférése felügyelt hozzáférés ellenőrzési ponton keresztül kerüljön kialakításra. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.15.2. Az érintett szervezet teljes eszköztitkosítást, tároló alapú titkosítást vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő a kiírás szerint gondoskodik a Rendszer mobil eszközeinek titkosításáról. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.4.2. Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő kialakítja a Rendszer kártékony kódok elleni védelmét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.4.3. Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszer kártékony kódok elleni védelmének automatikus frissítési képességét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.4.2. Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben kezelhető legyen a kártékony kódok elleni védelem központi kezelése. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.4.3. Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer automatikusan frissítse a kártékony kódok elleni védelmi mechanizmusokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.5.3. Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.5.4. Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott csatornán riasztást tudjon küldeni, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.9.3. Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer képes legyen automatikusan frissíteni a levélszemét elleni védelmi mechanizmusokat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.10. Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer képes legyen ellenőrizni a meghatározott információ belépési pontok érvényességét (például egyes bemeneti mezők inputvalidációja). | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.11.1.1. Az elektronikus információs rendszer hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer képes legyen hibajelzéseket generálni a hibajavításhoz szükséges információkat biztosítva. Ugyanakkor ezt olyan tartalommal tegye, ami nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.11.1.2. Az elektronikus információs rendszer a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer a hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára tegye elérhetővé. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.11.13. Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a szükséges biztonsági beállításokat a Rendszerben, a memória védelme érdekében. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.3.2. Az elektronikus információs rendszer a naplóbejegyzésekben további, az érintett szervezet által meghatározott kiegészítő, részletesebb információkat is rögzít. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő lehetővé teszi, hogy a Rendszer a naplóbejegyzésekben további, a Szervezet által meghatározott kiegészítő, részletesebb információkat is rögzítsen. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.7.1.2. Az elektronikus információs rendszer nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer nem változtathassa meg a naplóbejegyzések eredeti tartalmát és időrendjét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.7.2. Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszer fontos naplóbejegyzéseinek automatikusan feldolgozhatóságát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.8.2. Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott gyakorisággal összehasonlítsa a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.2. Az elektronikus információs rendszer elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben elkülönítésre kerüljön a felhasználók által elérhető funkcionalitás és a Rendszer irányítási funkcionalitása. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.4. Az elektronikus információs rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.4. Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer a felügyelt kapcsolódási pontjain alapértelmezetten tiltja és csak kivételként engedélyezi egyes hálózati forgalmakat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.5. A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a távoli készülékkel/eszközzel kapcsolatban álló Rendszer meggátolja, hogy a készülék/eszköz egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel. | | |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.7.1. Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer védje meg a továbbított információk bizalmasságát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.7.2. Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer kriptográfiai mechanizmusokat alkalmazzon az adatátvitel során az információk jogosulatlan felfedése ellen -kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.8.1. Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer védje meg a továbbított információk sértetlenségét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.8.2. Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer kriptográfiai mechanizmusokat alkalmazzon az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.9. Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer megszakítsa a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, meghatározott időtartamú inaktivitás után. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.14.1.1. Az érintett szervezet meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat. | | 4 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben a szervezet által meghatározott elfogadható mobilkódok és mobilkód technológiák kerüljenek alkalmazásra. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.19. Az elektronikus információs rendszer védje meg a munkaszakaszok hitelességét. | | 4 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer megvédje a munkaszakaszok hitelességét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.21. Az elektronikus információs rendszer védi az érintett szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát; sértetlenségét. | | 4 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a védendő maradvány információkat, melyek bizalmasságát, sértetlenségét védeni szükséges. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer megvédje a Szervezet által meghatározott maradvány információk (pl.: átmeneti fájlok) bizalmasságát, sértetlenségét. | | |

**5. biztonsági osztályú Rendszer követelményei**

Amennyiben az EIR 5. biztonsági osztályba került besorolásra, abban az esetben alábbi követelményeken kívül a fenti 2.; 3. és 4. biztonsági osztály követelményeit is teljesíteni kell.

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.1.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy dokumentált fejlesztési folyamatot kövessen. | | 5 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő dokumentált fejlesztési folyamatot követ, melyet a Szervezet részére igazol. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.1.2. Az érintett szervezet előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat. | | 5 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a fejlesztői folyamat áttekintésének gyakoriságát. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő a Szervezet által meghatározott gyakorisággal áttekinti a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.2.1. A dokumentált fejlesztési folyamat kiemelten kezeli a biztonsági követelményeket. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő igazolja, hogy fejlesztési folyamata kiemelten kezeli a biztonsági követelményeket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.2.2. A dokumentált fejlesztési folyamat meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő igazolja, hogy fejlesztési folyamata meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.2.3. A dokumentált fejlesztési folyamat dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat; | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő igazolja, hogy fejlesztési folyamata tartalmazza a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.6.2.4. A dokumentált fejlesztési folyamat nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő igazolja, hogy fejlesztési folyamata nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.7. Az érintett szervezet oktatási kötelezettséget ír elő az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára, hogy az érintett szervezet által kijelölt személyek - elsősorban adminisztrátorok - és biztonsági felelősök a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák. | | 5 |
| Szervezeti feladat: | | |
| A szervezet elvégzi a követelménypont szerinti rá vonatkozó feladatokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő teljesíti oktatási kötelezettségét, a megvalósított biztonsági funkciók, intézkedések és mechanizmusok Szervezet általi helyes használatának és működésének megismerése és elsajátítása érdekében. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.8.1.1. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely illeszkedik a szervezet biztonsági architektúrájához és támogatja azt. | | 5 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a fejlesztőtől, hogy a számára testreszabott biztonsági architektúrát hozzon létre. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő olyan specifikációt és biztonsági architektúrát hoz létre, amely illeszkedik a Szervezet biztonsági architektúrájához és támogatja azt. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.8.1.2. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között. | | 5 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a fejlesztőtől, hogy a számára testreszabott biztonsági architektúrát hozzon létre. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő olyan specifikációt és biztonsági architektúrát hoz létre, amely leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.3.8.1.3. Az érintett szervezet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan specifikációt és biztonsági architektúrát hozzon létre, amely bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében. | | 5 |
| Szervezeti feladat: | | |
| A szervezet megköveteli a fejlesztőtől, hogy a számára testreszabott biztonsági architektúrát hozzon létre. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő olyan specifikációt és biztonsági architektúrát hoz létre, amely bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.2.3. Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját, és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszer alapkonfigurációját és szükség szerint annak további verzióit. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.5.2. Az érintett szervezet az elektronikus információs rendszerben automatikus mechanizmusokat alkalmaz a hozzáférési korlátozások érdekében, az ezzel kapcsolatos tevékenység naplózására. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben az automatikus hozzáférési korlátozások alkalmazhatóságát. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.5.4. A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő gondoskodik a szoftver és firmware elemek megfelelő digitális aláírással vagy tanúsítvánnyal történő validálásáról. | | |
| Követelmény: | Biztonsági osztály: | |
| 3.3.6.7.2.2. Az érintett szervezetnek a szoftver használatra meghatározott szabályzatainak vagy a szoftver használatára vonatkozó feltételeinek és kikötéseinek megfelelően az elektronikus információs rendszer megakadályozza a tiltott programok futtatását. | | 5 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a szoftver használatra vonatkozó szabályait vagy a szoftver használatára vonatkozó feltételeit és kikötéseit és átadja a fejlesztő részére. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszerben, a szoftver használatra vonatkozó szabályok szerint a tiltott programok futtatását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.2.6. Meghatározott időtartamú várható inaktivitás, vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót. | | 5 |
| Szervezeti feladat: | |  |
| A Szervezet határozza meg a felhasználó, inaktivitáson kívüli kiléptetésének esetleges eseteit. | |  |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott inaktivitás vagy időtartam letelte után kiléptesse a felhasználót. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.9. Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben meghatározott számra korlátozható legyen az egyidejű munkaszakaszok száma, a meghatározott fiókok vagy fiók típusok számára külön-külön. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.14.2. Az érintett szervezet az elektronikus információs rendszerben titkosítással és a felhasználók, vagy eszközök hitelesítésével védi a vezeték nélküli hozzáférést. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer vezeték nélküli hozzáférése titkosítással és a felhasználók, vagy eszközök hitelesítésével védetten kerüljön kialakításra. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.10.14.3. Az érintett szervezet azonosítja a felhasználókat, és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül teszi lehetővé számukra a vezeték nélküli hálózat független konfigurálását. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer azonosítsa a felhasználókat és csak közvetlen jogosultság birtokában, a védett hálózaton kialakított vezetékes kapcsolaton keresztül tegye lehetővé számukra a vezeték nélküli hálózat független konfigurálását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.3.3. Az elektronikus információs rendszer biztosítja a meghatározott rendszerelemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszer által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.5.2. Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott csatornán értesítést küldjön, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.5.3. Az elektronikus információs rendszer riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben beállíthatóak legyenek a valós idejű riasztást igénylő hibaesemények. Továbbá a Rendszer meghatározott csatornán riasztást küldjön, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.9.3. Az elektronikus információs rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmenti, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer a naplóbejegyzéseket meghatározott gyakorisággal elmentse, egy a keletkezési helyétől fizikailag elkülönülő rendszerre vagy rendszerelemre. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.9.4. Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére. | | 5 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére alkalmazandó kriptográfiai mechanizmusokat. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott kriptográfiai mechanizmusokat alkalmazzon a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.10. Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer képes legyen a tevékenységek elvégzésének letagadhatatlan módú igazolására. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.12.2. Az elektronikus információs rendszer a naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati naplót állít össze, amely - a felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli - időviszonyokat is tartalmazza. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer képes legyen a naplóbejegyzéseiből rendszerszintű (logikai vagy fizikai) felülvizsgálati napló összeállítására, amely - a felülvizsgálati napló egyedi bejegyzéseinek időbélyegei közötti kapcsolat tekintetében meghatározott tűréshatáron túli - időviszonyokat is tartalmazza. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.12.12.3. Az elektronikus információs rendszer biztosítja a lehetőséget a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszerelemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer lehetőséget biztosítson a meghatározott személyeknek vagy szerepköröknek arra, hogy megváltoztassák az egyes rendszerelemekre végrehajtandó naplózást a kiválasztott esemény kritériumok alapján, meghatározott időtartamon belül. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.3. Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszerben elkülönítésre kerüljenek a biztonsági funkciók a nem biztonsági funkcióktól. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.6. Az elektronikus információs rendszer hitelesített proxy - olyan szerver, számítógép vagy szerveralkalmazás, amely a kliensek kéréseit köztes elemként más szerverekhez továbbítja - kiszolgálók segítségével irányítja a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer hitelesített proxy kiszolgálók segítségével irányítsa a belső kommunikációs forgalmat a felügyelt interfészeken a meghatározott külső hálózatokhoz. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.6.7. Az elektronikus információs rendszer hibaállapotba kerül a határvédelmi eszköz működési hibája esetén. | | 5 |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja a Rendszer hibaállapotba kerülésének lehetőségét a határvédelmi eszköz működési hibája esetére. | | |

|  |  |  |
| --- | --- | --- |
| Követelmény: | Biztonsági osztály: | |
| 3.3.13.20. Meghatározott hibatípusokhoz tartozó hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerül, amely a hiba esetén is megőrzi a rendszerállapot információkat. | | 5 |
| Szervezeti feladat: | | |
| A Szervezet meghatározza azon hibatípusokat, melyeket követően a Rendszernek a kijelölt, vagy utolsó ismert állapotba kell kerülnie. | | |
| Fejlesztői feladat: | | |
| A Fejlesztő biztosítja, hogy a Rendszer meghatározott hibát követően az elektronikus információs rendszer a kijelölt, vagy utolsó ismert állapotba kerüljön. | | |