Vácduka Község Önkormányzata

N01 INFORMÁCIÓ BIZTONSÁGI SZABÁLYZATA

BIZALMAS

Készült	2025. 06. 19.
Készítette	Várfi András IBF
Jóváhagyta	Hegyi Ágnes Jegyző
Verziószám	2025 v1.0
Azonosító	N01 IBSZ
Oldalak száma	92

Verzióváltozások nyilvántartása

Verziószám	Módosítás dátuma	Módosítás leírása	Jóváhagyó neve	Megjegyzés
2025 v1.0	2025. 06. 19.	Első kiadás	Hegyi Ágnes Jegyző	–
1.1				–
1.2				–

Tartalom

1. Általános rendelkezések

1.1 A Szabályozás célja

Vácduka Község Önkormányzata (a továbbiakban: szervezet) Információbiztonsági Szabályzatának ***(„N01 Információ Biztonsági Szabályzat")*** a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal, a *2024. évi LXIX. törvény Magyarország kiberbiztonságáról (továbbiakban: Kibertv.) és végrehajtási rendeletei a 7/2024 (VI. 24.) MK rendelet, illetve 418/2024. (XII.23.) Kormányrendelet* (továbbiakban jogszabály), valamint a szervezet belső rendelkezéseivel összhangban meghatározza a szervezet informatikai rendszerei által kezelt információvagyon bizalmassága, hitelessége, sértetlensége, valamint rendelkezésre állásának biztosítása, funkcionalitása és üzembiztonsága megőrzése érdekében betartandó elveket. Az IBSZ meghatározza az informatikai vezető és az információbiztonságért felelős személy feladatait, valamint az információs rendszer működtetői és felhasználói számára kötelező szabályokat. Az IBSZ kiemelt célja, hogy a szervezet informatikai rendszereinek zavartalan működése biztosított legyen.

Jelen szabályzat a fentiek keretében védelmi eljárásokat határoz meg, intézkedési jogosultságot állapít meg, valamint ellenőrzési mechanizmusokat állít fel a szabálytalanságok felderítésére és a felelősség megállapítására.

1.2 A Szabályozás hatálya

1.1.1. Az IBSZ személyi hatálya

Az IBSZ személyi hatálya a kiterjed a szervezet valamennyi teljes- vagy részmunkaidős, valamint szerződéses foglalkoztatottjára (felhasználójára). Az IBSZ hatálya kiterjed továbbá a szervezet informatikai rendszerének üzemeltetésében és karbantartásában résztvevő cégekre, vállalkozókra, illetve magánszemélyekre ***(„N14.3.1 Külső felhasználó -személyi biztonsági szabályzat")***. Az érintettekkel az IBSZ megfelelő pontjait ismertetni kell ***(„N03.1 Információ Biztonsági Felhasználói Szabályzat")*** továbbá nyilatkozniuk kell az IBSZ rájuk vonatkozó előírásainak elfogadásáról és betartásáról az előírások szerinti munkavégzésükhöz ***(„N14.2.1 (EIR) felhasználási szabályok elfogadó nyilatkozat")*** vagy külső felhasználó esetén ***(„N14.3.1 Külső felhasználási szabályok elfogadó nyilatkozat").*** Az IBSZ hatálya kiterjed minden olyan magánszemélyre, illetve gazdasági szervezetre, aki/ami munkavégzése kapcsán bármilyen informatikai eszközzel a szervezet informatikai infrastruktúrájához csatlakozik, illetve azt igénybe veszi. A csatlakozás kizárólag szervezeti érdekből történhet.

1.1.2. Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

A szervezet Elektronikus Információs Rendszereire (a továbbiakban EIR). Az EIR olyan eszközök, folyamatok és adatok összessége, amely digitális adatok tárolására, kezelésére és továbbítására szolgál. Az EIR-nek vannak hardver összetevői (pl. számítógépek, szoftverek/programok, alkalmazások), hálózati elemei (internet, kommunikációs rendszerek) és elemei a benne kezelt adatok (pl. betegadatok, pénzügyi információk) is. Működési célja az automatizált adatfeldolgozás biztosítása a szervezet céljainak megfelelő szakterületeken. Az egyes EIR-ek információbiztonsági szempontból fontos tulajdonságait a szervezet az ***(„N13.1.1 EIR nyilvántartás és technikai-adatok-űrlap")*** tartja

frissen, a változásokat részletesen dokumentálja. A védelmet élvező adatok teljes körére, felmerülési és feldolgozási helyétől, idejétől és az adatok fizikai megjelenési formájától függetlenül;

- a szervezet tulajdonában lévő, illetve az általa bérelt, vagy használt valamennyi informatikai berendezésre (számítógépekre, azok tartozékaira és perifériáira);
- a különböző adathordozókra;
- a szervezet számítógépes hálózatára és annak elemeire;
- a számítógépes hálózathoz való kapcsolódást biztosító eszközökhöz tartozó modemekre (szolgáltatói modem, mobil adathordozók), hálózati útválasztókra (routerek), aktív elemekre és egyéb olyan speciális eszközökre, melyek az informatikai eszközökhöz, illetve a hálózathoz illeszthetők (pl. switch, hub, pendrive, mobil adathordozó, mobiltelefon, digitális fényképezőgép stb.) ;
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, üzemeltetési stb.);
- a rendszer- és felhasználói szoftver/programokra;
- az adatok felhasználására vonatkozó utasításokra;
- az adathordozók tárolására és felhasználására;
- tulajdonviszonytól függetlenül (tulajdonolt, bérelt stb.) a szervezet területén (állandóan vagy ideiglenes jelleggel) telepített informatikai eszközökre, az azokkal kapcsolatos tevékenységekre.
- Az IBSZ a tárgyi hatálya alá tartozó elemek teljes életciklusára kiterjed, amely az alábbi szakaszokból áll:
- tervezési szakasz: a rendszer iránti igény, a rendszer célja és a vele szemben támasztott követelményeknek a leírása;
- fejlesztési/beszerzési szakasz: a rendszer fejlesztése, programozása, létrehozása, beszerzése;
- megvalósítási szakasz: a rendszer tesztelése, telepítése, testreszabása;
- üzemeltetés/karbantartás: a rendszer üzemelése, üzemeltetése, hardver- és szoftver/program módosítások, karbantartás, események kezelése;
- visszavonás/selejtezés/megsemmisítés szakasz: információk, hardver és szoftver/program visszavonása az üzemelésből, törlése, megsemmisítése és hosszabb távú megőrzésre való felkészítése.

1.1.3. Az IBSZ időbeli hatálya

Az Információ Biztonsági Szabályzat (IBSZ), és annak kivonatolt, a felhasználók számára készült változata az ***(„N03.1 Információ Biztonsági Felhasználói Szabályzat")*** a szervezet vezetőjének elfogadásától (aláírás napja), illetve az dokumentum kiadásától, azaz a kihirdetésétől lép hatályba. Visszavonásig érvényes.

Az Információ Biztonsági Felhasználói Szabályzat fejezetszámai pontosan megegyeznek az IBSZ fejezetszámaival (még akkor is, ha a kivonatolás miatt kimaradnak komplett fejezetek) megkönnyítve ezzel a hivatkozások egységes használatát.

Az Információbiztonsági Szabályzatot évente vagy jelentősebb infrastrukturális-, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén módosítani, mind szervezeti, mind informatikai szakmai szempontok szerint.

Minden, a felhasználói szabályokat érintő változást az Információ Biztonsági Felhasználói Szabályzatban dokumentálni szükséges, a felhasználók számára ki kell hirdetni.

1.2. Az IBSZ alapelvei

A szervezet informatikai rendszereiben biztosítani kell informatikai és nem informatikai eszközök és módszerek kombinációjával az adatok biztonságát és az ilyen adatokat tároló, feldolgozó, továbbító rendszerek, azaz az EIR-ek üzembiztonságát. Az egyes EIR-ek tervezése és megvalósítása során – *a EIR-ben kezelt adatok biztonsági osztályba sorolásának megfelelően* – kell a konkrét IT biztonsági intézkedéseket meghatározni.

A bizalmasság biztosítása lehetővé teszi, hogy az információ a jogosulatlan informatikai szereplők (személyek, csoportok, programok, folyamatok stb.) számára ne legyen elérhető és ne kerüljön nyilvánosságra. Érvényesülnie kell a szervezet és szervezetei által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezelési folyamatoknál felhasznált adathordozók tekintetében, valamint a kommunikáció során.

Az egyedi elszámoltathatóságot az EIR-ekben a felhasználókat egyértelműen azonosító és hitelesítő mechanizmusok megvalósításával és az egyes rendszerekben naplózandó események, a naplórekordok tartalmának meghatározásával és rögzítésével kell biztosítani, amennyiben az adott alrendszer technikailag ezt lehetővé teszi. A naplókat védeni kell a jogosulatlan hozzáférés, módosítás és törlés ellen.

Az információ és a rendszerek rendelkezésre állása érdekében a szervezeti rendszerekben biztosítani kell a tárhelyek sértetlenségét, azonosítani kell a rendszerkomponenseket és rendszerkapcsolatokat. Eljárások és mechanizmusok akadályozzák meg a kártékony kódok rendszerbe jutását és az ottani károkozást. Mentési eljárásokat kell kidolgozni az adatokra, dokumentumtárakra, szoftver/program. Az eljárásokat tesztelni, dokumentálni kell. A mentéseknél a rendelkezésre állás biztosításán kívül a bizalmasság és sértetlenség követelményeit is biztosítani kell. Olyan alap szoftver/program és alkalmazásokat kell használni a szervezeti rendszerekben, amelyek biztosítják, hogy a rendszer működésének megszakadása után minimális veszteséggel álljon vissza biztonságos állapotba.

A dokumentáltság elve érvényre juttatása érdekében a rendszerek adminisztrátorai számára a biztonságos konfiguráláshoz, használathoz szükséges ismereteket (telepítési, üzemeltetési leírások) tartalmazó telepítési- és használati leírást kell rendelkezésre bocsátani. Felhasználói leírást kell biztosítani az átlagos/általános felhasználó számára. A leírásokat szervezeti fejlesztési erőforrások alkalmazása esetén az adott rendszer fejlesztését, kialakítását végző szervezeti egységnek kell elkészíteni. Külső fejlesztő közreműködése esetén a fejlesztést végző külső munkatárs készíti el, együttműködve a fejlesztésért felelős szervezeti egységgel.

A hitelesség biztosítása érdekében – ahol a hitelesség egy entitás (IT rendszeren belül elkülöníthető tulajdonsággal bíró személy, program, folyamat, adat stb.) olyan tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más egyed számára bizonyíthatóvá tesz - a szervezet belső kapcsolataiban a kommunikáló felek, szervezeti egységek kölcsönösen és kétségtelenül ismerjék fel egymást és ez az állapot a kapcsolat egész idejére változatlanul fenntartható legyen.

A szükséges és elégséges ismeret elve alapján a rendszer minden felhasználónak biztosítja azokat – de csak azokat – az információkat és funkciókat, amelyek az adott felhasználó feladatainak ellátáshoz szükségesek. A szervezeti rendszerekben a felhasználó csak azonosítás és hitelesítés után férhet hozzá a rendszerszolgáltatásokhoz.

Az információtartalom sértetlenségét biztosítani kell a szervezet rendszereiben az adattárolás, kezelés és továbbítás folyamán, azaz adatokat, dokumentumokat, programokat, hardvert és eszközöket, és ezek konfigurációit csak az arra jogosultak kezelhetik. Ezen elemek észrevétlenül nem módosulhatnak, törlődhetnek. Biztosítani kell, hogy a jogosultak a pontos és helyes információkat dolgozzák fel tevékenységük során.

1.2.1. Folyamatos ellenőrzés biztosítása

Az érintett szervezet folyamatba épített ellenőrzést vagy ellenőrzési tervet hajt végre, ***(„N08.2 Ellenőrzési terv")*** amely tartalmazza:

- az ellenőrizendő területeket;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságát;
- az érintett szervezet ellenőrzési stratégiájához illeszkedő folyamatos biztonsági értékeléseket;
- a mérőszámok megfelelőségét;
- az értékelések és az ellenőrzések által generált biztonsággal kapcsolatos adatok összehasonlító elemzését;
- az érintett szervezet reagálását a biztonsággal kapcsolatos adatok elemzésének eredményére;
- az érintett szervezet döntését arról, hogy milyen gyakorisággal kell az elemzési adatokat az általa meghatározott személyi- és szerepkörökkel megismertetni (ideértve azok változásait is).

A rendszer életciklus szakaszaiba épített biztonság elvének teljesítése céljából a rendszer teljes életciklusában érvényesülnie kell az információbiztonsági szempontoknak.

A feladatok elkülönítése elvének teljesítése érdekében a szerepkörök kialakítása során a feladatokat úgy kell szétosztani az érintettek között, hogy ne egyetlen személy kezében összpontosuljon a szervezet informatikai rendszereinek adminisztrálása és biztonsági ellenőrzése.

A szervezet elektronikus információs rendszerének kapcsolódása szempontjából szabályozza és belső engedélyhez köti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez, dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

A szervezet elektronikus információs rendszerének kapcsolódása szempontjából belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

A szervezet külső elektronikus információs rendszerekhez való kapcsolódásokhoz az információbiztonsági szabályzatában szabályrendszert állít fel és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

A szervezet cselekvési tervet készít, ebben mérföldköveket és felelősöket határoz meg. A kockázatkezelési stratégia és a kockázatokra adott választevékenységek prioritása alapján meghatározott időnként felülvizsgálja és karbantartja a cselekvési tervet. Ha az adott elektronikus információs rendszerére vonatkozó az alap biztonsági osztály meghatározásánál hiányosságot állapít meg, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni a hiányosság megszüntetése érdekében. Ha a meghatározott biztonsági osztály alacsonyabb, mint az érintett szervezetre érvényes biztonsági osztályra vonatkozó elvárt védelmi intézkedés, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni az előírt biztonsági osztály elérése érdekében.

1.2.2. Előzetes tesztelés és megerősítés

A szervezet kifejleszti, felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét.

Már a változtatási igény felmerülésekor rögzíteni kell a minimális tesztelési folyamatlépéseket, a felelősöket és az egyes vizsgálati szinteket (funkcionális, biztonsági), továbbá formálisan dokumentálni kell a teszteredményeket és a visszavonási tervet is. A tesztelés megtervezésekor a kockázati szempontokat például: sérülékenység, működésfolytonosság) be kell építeni, továbbá a megfelelő elkülönített tesztkörnyezet használata, illetve a tesztre engedélyezett időkeret

meghatározása is kötelező. Gondoskodni kell arról, hogy a dokumentált teszteredmények és a jóváhagyott változtatások nyilvántartása visszakövethető legyen, és a szervezet vezetői vagy az információbiztonságért felelős személy is ellenőrizhessék, hogy a kibocsátott új verzió minden minimális követelménynek megfelel. Ezzel biztosítható, hogy szabályozottan, nyomon követhetően és biztonságos módon történjen minden konfiguráció módosítás.

A konfiguráció megváltoztatása előtt az új verziót tesztelni kell, ezután dönteni kell annak megfelelőségéről, továbbá dokumentálni kell az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt.

A szervezet megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását még a változtatások megvalósítása előtt.

1.3. Szerepkörök, tevékenységek, felelősségek

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendeltek. A szerepkörök szerinti felelősök kijelölése elsősorban a munkaköri leírásokban történik. Az informatikai infrastruktúra) biztonságos működtetésében, illetve az informatikai rendszerekben kezelt adatok védelmének tárgykörében a következő szerepkörök kerülnek meghatározásra:

1.3.1. A szervezet vezetője

- A szervezet vezetője) felel az informatikai rendszerben tárolt adatok védelméért és az adatok biztonságáért. Hatáskörében jogosult a számítógépes adatvédelem és az adatbiztonság megszervezésére és ellenőrzésére.

Feladatai:

- Az irányadó biztonsági osztály tekintetében biztosítja a jogszabályban meghatározott követelmények teljesülését a szervezetre és információs rendszerre vonatkozóan is.
- Biztonságért felelős személyt nevez ki ***(„N01.2 Információ Biztonsági Felelős kinevezése„)*** erről a hatóságfelügyeleti jogot gyakorló szerv részére tájékoztatást nyújt.
- Meghatározza a szervezet elektronikus információs rendszereinek felhasználóira és üzemeltetőire vonatkozó szabályokat
- Meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira, és az ehhez szükséges hatáskörre vonatkozó szabályokat, illetve kiadja az információbiztonsági szabályzatot
- Gondoskodik az oktatásról, az információbiztonsági ismeretek szinten tartásáról ***(„N03.4 Információ Biztonsági oktatás terv és napló").***
- kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik a megfelelésről ***(„N15.1.1 Kockázatelemzés -kockázatértékelés")***
- Gondoskodik az események nyomonkövethetőségéről ***(„N09.1.2 Biztonsági események naplója")***
- Biztonsági esemény (incidens) bekövetkezésekor gondoskodik a gyors és hatékony reagálásról, ezt követően a biztonsági esemény kezeléséről ***(„N09.1.1 Biztonsági eseménykezelési terv")***
- az érintettek haladéktalan tájékoztatásáról
- Ha külsős erőforrást vesz igénybe, akkor szerződéses kötelemként gondoskodik a törvényben foglaltak teljesüléséről. A szervezet vezetője ebben az esetben is felelős a meghatározott feladatokért, kivéve, ha jogszabály által kijelölt központosított szolgáltatót kell igénybe venni. Ebben az esetben a szolgáltató felett felügyeletet gyakorló miniszter a felelős.

- Megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
- A hatóságfelügyeleti jogot gyakorló szerv részére az ellenőrzéshez lefolytatásához szükséges feltételeket ás adatokat biztosítja.
- Gondoskodik az információbiztonsági szabályzat felülvizsgálatáról évente, továbbá minden olyan esetben, amikor jogszabályváltozás lép hatályba, jelentős változás történik az informatikai infrastruktúrában, új elektronikus információs rendszer kerül bevezetésre, vagy bármely olyan körülmény következik be, amely érdemben befolyásolja a szervezet működését vagy az általa kezelt adatvagyon biztonságát.

1.3.2. Az elektronikus információs rendszerek biztonságáért felelős személy (IBF)

Az elektronikus információs rendszerek biztonságáért felelős személyt Információ Biztonsági Felelőst (továbbiakban: IBF) a szervezet vezetője nevezi ki. Az IBF felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

- A szervezet vezetőjének közvetlen adhat tájékoztatást, jelentést.
- Gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
- Elvégzi vagy irányítja a fenti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti a szervezet elektronikus információs rendszereire vonatkozó Információbiztonsági Szabályzatot (IBSZ).
- Meghatározza a rendszerek biztonsági beállításaival kapcsolatos elvárásokat, jogokat, feladatokat.
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet ezen tárgykört érintő szabályzatait és szerződéseit.
- Biztosítja a hatályos jogszabályok szerinti követelmények teljesülését.

Az elektronikus információs rendszer biztonságáért felelős személy a jogszabály alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről köteles tájékoztatni a szervezet vezetőjét és a jogszabályban meghatározott szervezet.

Az elektronikus információs rendszer biztonságáért felelős személy a szervezet vezetőjének támogatásával biztosítja az e szabályzatban meghatározott követelmények teljesülését. A szervezet valamennyi elektronikus információs rendszerének a tervezésében, auditállasában, vizsgálatában, kockázatelemzésében és kockázatkezelésében közreműködik.

Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor az elektronikus információs rendszer biztonságáért felelős személy jogosult a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatokat, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. Valamint figyelembe kell venni az Adatvédelmi Felelős (DPO) vonatkozó állásfoglalásait.

Az elektronikus információs rendszer biztonságáért felelős személy e szabályzat szerinti feladatai és felelőssége a jogszabálynak megfelelő módon átruházható.

1.3.3. Üzemeltető, informatikus/rendszergazda)

Feladata az informatikai infrastruktúra üzemeltetése, fejlesztése és biztonságos működésének elősegítése.

Felelős

- a szerverek és a rajtuk futó alap szoftver/program, operációs rendszerek, szolgáltatások, adatbáziskezelők, fájl- és nyomtatószerverek működtetéséért;
- a szervezet adatvagyona a ***(„N04.2 Mentési szabályzat")*** -ban foglaltak szerint, részletes, minden elemre kiterjedő adatmentések elvégzéséért, a mentett adatok biztonságos tárolásáért, a szükséges visszaállításokért;
- a standard felhasználói alkalmazáskörnyezet és az általa nyújtott szolgáltatások és segédalkalmazások, továbbá a ráépülő általános irodai alkalmazások komponensei, továbbá a szervezet felhasználói környezetében már megszokott általános alkalmazások és felhasználói segéd szoftver/program, valamint a hálózati nyomtatók működtetéséért;
- az aktív és passzív hálózati eszközök működtetéséért, rendelkezésre állásáért;

az adatbázisban tárolt adatok és szoftver/program rendelkezésre állásáért, a hozzáférők adminisztrálásért;

- az üzemeltetett infrastruktúra átlátható és aktuális állapotot tükröző dokumentálásáért kiemelten: ***(„N02.2 Informatikai leltár és topológia (szoftver, hardver, liszensz)")***

1.3.4. Adatgazda / EIR felelős

Az a személy (vagy szervezeti egység), amely a végső felelőse egy bizonyos adathalmaz jelentésének, tartalmának, minőségének és elérhetővé tételének – azaz az egyes EIR-eknek. Ide értendő az is, hogy az adatot hogyan definiálják, hogyan állítják elő, hogyan azonosítják, hogyan tartják karban, hogyan használják fel. A szervezeti egységeinél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat IBSZ-nek megfelelő kezelésért

- felelős a hozzá dedikált EIR-ben kezelt adatkörök és adatok számosságának meghatározásáért;
- ellátja a hatáskörébe rendelt EIR-ek esetén az adatkezelési feladatokat. E tekintetben további felelőssége az *EIR nyilvántartásiok naprakészen tartása* ***(„N13.1.1 EIR nyilvántartás és technikai-adatok-űrlap")*** kiemelt figyelemmel a dedikált EIR-ekre vonatkozó mezőinek adatokkal történő feltöltése majd az IBF-nek való megküldéséért;
- Az EIR adataiban történő változások esetén a frissített verziójú dokumentumokat megküldi az IBF-nek a frissítéstől számított 3 munkanapon belül;
- közreműködik a kockázatelemzésben, a cselekvési terv elkészítésében és a feltárt hiányosságok kezelésben - szakterületéről felelőst keres és időpontot rendel hozzá;
- közreműködik a cselekvési terv végrehajtásában és annak teljesülésének felügyeletében;
- tájékoztatást kérhet a cselekvési tervben megfogalmazott feladatok végrehajtásával kapcsolatban;
- meghatározza az összeférhetetlen szerep- és feladatköröket;
- kezeli a jogosultságigényeket (jóváhagy, felfüggeszt, zárol);
- részt vesz az éves BCP és DRP tesztelési terv kidolgozásában;
- részt vesz a BCP és DRP tesztelésekben;
- feladata a közreműködők szakmai szintű felügyelete;
- feladata a biztonsági események, incidensek jelentése;
- részt vesz az incidenskezelésben.

1.3.5. Felhasználó

A szervezeti rendszerek nem üzemeltető felhasználója.

- Ismernie kell az Információ Biztonsági Felhasználói Szabályzatban szereplő előírásokat, illetve azokat maradéktalanul be kell tartania.
- Rendelkeznie kell az általa használt berendezésekre és programhasználatra vonatkozó előírásokkal, valamit ismernie kell azok tartalmát.
- Tevékenysége megkezdésekor ellenőriznie kell, hogy az általa használt eszközök üzemképesek-e és azok beállítása az előírásoknak megfelelő-e.
- Köteles figyelemmel kísérni az általa használt berendezések és szoftver/program állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jeleznie kell a közvetlen vezetőnek.
- Munkája során figyelnie kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak az adat/információ feldolgozása során a helyiségben.
- Tevékenysége befejezésekor a használt programokból szabályszerűen ki kell lépjen.
- Hálózati információ igénybevételét követően a hálózatból szabályosan ki kell lépjen.
- A berendezéseket szükség esetén az előírásoknak megfelelően le kell állítania, illetve az áramellátásukat meg kell szüntetnie.
- A helyiségből utolsóként való távozáskor meg kell győződnie a helyiség biztonságos lezárásáról.

1.4. A vezetőség elkötelezettsége, a pénzügyi erőforrások biztosítása

A szervezet vezetősége elkötelezett az információbiztonság menedzselése iránt, és biztosítja, hogy az információbiztonsági követelmények teljesüljenek, különösen az alap biztonsági osztályba sorolt rendszerek esetében. Ennek megfelelően:

- Az információbiztonság ügyének szükséges mértékű publicitást biztosít a szervezet keretein belül, valamint gondoskodik a munkatársak megfelelő felvilágosításáról, tájékoztatásáról és oktatásáról. Az oktatás kiterjed az információbiztonsági szabályzat (IBSZ) alapvető előírásaira és a biztonságtudatosság növelésére.
- Az információbiztonsági szabályzatot (IBSZ) a szervezet vezetője) hirdeti ki a szerepköröknek megfelelően.
- Biztosítja a minimálisan szükséges anyagi, humán és technikai erőforrásokat az információbiztonsági követelmények teljesítéséhez:
- Gondoskodik arról, hogy az alapvető hozzáférés-védelmi és naplózási rendszerek működjenek.
- Biztosítja a szükséges szoftver/program és hardverfrissítésekhez szükséges forrásokat.
- Támogatja az alapvető adatmentési eljárások megvalósítását.
- A beruházások és beszerzések során tervezi az információbiztonsági stratégia megvalósításához szükséges forrásokat, különös tekintettel a védelemhez kapcsolódó minimális követelményekre (pl. jelszavas védelem, naplózás). Dokumentálja e követelmény alá eső kivételeket.
- Az információbiztonság irányítására felelőst (IBF) delegál és ruház fel a szükséges jogokkal. Az IBF felelős az EIR-ek biztonsági követelményeinek betartásáért is.
- Gondoskodik a biztonsági dokumentációkban található előírások betartásáról:
- Évente legalább egyszer belső auditot folytat le ***(„N05.3 Belső Audit jelentés") és („N05.3.1 Intézkedési terv")*** amely ellenőrzi az alapvető biztonsági intézkedések meglétét.

- Be nem tartás esetére szankciókat határoz meg, amelyeket a vonatkozó jogszabályok alapján foganatosít.
- Támogatja a rendszer használóinak az információbiztonságot fejlesztő törekvéseit:
- Ösztönzi az alkalmazottakat arra, hogy jelezzék a biztonsági hiányosságokat vagy fejlesztési lehetőségeket.
- Elérhetővé teszi számukra az alapvető biztonsági képzéseket és tájékoztató anyagokat.
- Mivel a szervezeti információvagyon biztonsága nem kizárólag az annak kezelésével megbízott személyek feladata és felelőssége, a vezetőség elvárja, hogy:

A szervezet minden felhasználója és szerződéses partnere sajátjának tekintse az információ biztonságának ügyét.

- Feladatán és hatáskörén belül külön utasítás nélkül támogassa azt.

1.5. Az IBSZ jogi háttere

Az IBSZ jogi háttere jelen verzió kihirdetésének napján naprakészen az alábbi, de évente vagy jelentős jogszabályváltozás esetén felülvizsgálatra szorul annak érdekében, hogy minden releváns előírásnak megfeleljen a szervezet működése és szabályozása.

- NIS2 irányelv - AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról
- 7/2024 (VI.24) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 270/2018. (XII. 20.) Korm. rendelet az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról.
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól.
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.
- 322/2024. (XI. 6.) Korm. rendelet: A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló rendelkezések, amelyek érintik a digitális szolgáltatásokat biztosító szervezetek működését, valamint az elektronikus dokumentumok hitelességének megőrzését.

2. Adminisztratív védelmi intézkedések

2.1. Információbiztonsági politika

A szervezet megfogalmazza és kihirdeti az ***„N01.4 Információ Biztonsági Politika"***-t (a továbbiakban: IBP), amely meghatározza:

- a szervezet kiberbiztonsági céljait,
- az alkalmazott biztonsági alapelveket,
- a megfelelőségi követelményeket,
- a vezetőség elkötelezettségét az információbiztonság irányítása és támogatása iránt.

Az IBP célja, hogy biztosítsa a szervezet által kezelt információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint támogassa az információbiztonsági szabályok betartását az alap biztonsági osztály követelményeinek megfelelően.

Az IBP-nek tartalmaznia kell a kockázatalapú megközelítés elvét, amelyet a követelmény rendelet előír. Ez biztosítja, hogy az információbiztonsági intézkedések arányosak legyenek a szervezet által kezelt adatok bizalmasságával és kritikus fontosságával.

Az IBP-ben ki kell térni a folyamatos ellenőrzés szükségességére, amely magában foglalja az ellenőrzési terv kidolgozását és végrehajtását.

Az IBP-ben szerepelnie kell annak is, hogy a szervezet vezetősége biztosítja az információbiztonsághoz szükséges pénzügyi, technikai és humán erőforrásokat.

Az IBP tartalmazza a tudatosságnövelő képzések fontosságát a felhasználók számára, különösen az alapvető biztonsági elvek betartására vonatkozóan.

Felülvizsgálat és frissítés

Az IBP-t szükséges évente frissíteni, vagy az alábbi esetekben:

- jelentős változások az elektronikus információs rendszerekben,
- új jogszabályi előírások megjelenése,
- kockázatelemzés) során feltárt hiányosságok.

Felelős

Az IBP kidolgozásáért, kihirdetéséért és rendszeres felülvizsgálatáért a szervezet vezetője felelős. A vezető biztosítja továbbá, hogy az IBP tartalmát minden érintett felhasználó és külső partner megismerje és betartsa.

2.2. Információbiztonsági stratégia

A szervezet megfogalmazza és kihirdeti az ***„N01.3 Információ Biztonsági Stratégia"*** -t (a továbbiakban: IBS), amely meghatározza:

- a biztonságpolitikai célok megvalósításának módszereit,
- az alkalmazandó eszközrendszert,
- az ütemezést és prioritásokat,
- a kockázatok kezelésének alapelveit.

Az IBS-nek tartalmaznia kell a kockázatalapú megközelítés elvét, amelyet a NIS2 irányelv és a 7/2024 MK rendelet is előír. Ez biztosítja, hogy az információbiztonsági intézkedések arányosak legyenek a szervezet által kezelt adatok bizalmasságával és kritikus fontosságával.

Az IBS keretében ki kell dolgozni egy cselekvési tervet, amely tartalmazza:

- a biztonsági fejlesztések ütemezését,
- a szükséges erőforrások biztosítását,
- a felelősök kijelölését.

Az IBS-ben ki kell térni a beszállítói lánc biztonságára, különös tekintettel arra, hogy a külső partnerek megfeleljenek az elvárt alap biztonsági osztály követelményeinek.

Az IBS-ben hangsúlyozni kell a szervezeti tudatosság növelését célzó képzések fontosságát.

Az IBS illeszkedik a szervezet más stratégiáihoz, így különösen:

- a költségvetési és humánerőforrás-tervezéshez,
- a szervezet jövőképéhez, fejlesztési terveihez,
- a működtetett minőségirányítási vagy információbiztonság-irányítási rendszerekhez.

Felülvizsgálat és frissítés

Az IBS felülvizsgálata évente szükséges, vagy az alábbi esetekben:

- jelentős változások az elektronikus információs rendszerekben,
- új jogszabályi előírások megjelenése,
- kockázatelemzés során feltárt hiányosságok kezelése érdekében.

A felülvizsgálat során biztosítani kell, hogy az IBS összhangban legyen a 7/2024 MK rendeletben meghatározott biztonsági osztályba sorolási követelményekkel és az alap biztonsági osztályba sorolt szervezett szerint meghatározott védelmi intézkedésekkel és követelményekkel.

Felelős

Az IBS kidolgozásáért, kihirdetéséért és rendszeres felülvizsgálatáért a szervezet vezetője felelős. A vezető gondoskodik arról is, hogy az IBS tartalmát minden érintett felhasználó megismerje és betartsa.

2.3. Az elektronikus információs rendszerek és rendszerelemek nyilvántartása

2.3.1. Az EIR nyilvántartás

A szervezet az elektronikus információs rendszereiről (EIR-ek) naprakész nyilvántartást vezet ***(„N08.1.2 EIR nyilvántartás")***, amely elektronikus formában kerül kezelésre.

A nyilvántartás célja, hogy biztosítsa az elektronikus információs rendszerek átláthatóságát, pontos állapotát, valamint támogassa a biztonsági intézkedések megfelelő végrehajtását.

Az egyes EIR-ek adatgazdáinak felelőssége az EIR nyilvántartás és technikai-adatok-űrlap elkészítése az EIR-ekre vonatkozó adatokkal történő feltöltése majd, amely alapján a rendszergazda összeállítja az EIR nyilvántartást, *a nyilvántartás alapján el kell készíteni az úgynevezett NBSZ-NKI OVI űrlapokat (táblázatokat) az azonosított Elektronikus Informatikai Rendszerekről.*

A nyilvántartásnak minden rendszerre vonatkozóan tartalmaznia kell:

- A rendszer alapfeladatait és célját.
- A rendszerek által biztosított szolgáltatásokat.

- Az érintett rendszerekhez tartozó licencszámokat (amennyiben azok a szervezet kezelésében vannak).
- A rendszer felett felügyeletet gyakorló személy nevét, beosztását, elérhetőségi adatait.
- A rendszert szállító, fejlesztő és karbantartó szervezetek azonosító- és elérhetőségi adatait, valamint az illetékes kapcsolattartók nevét és elérhetőségét.
- A rendszer biztonsági osztályba sorolását: ALAP, JELENTŐS, MAGAS.

2.3.2. Az hardver és szoftverlicensz (rendszerelemek) nyilvántartás

A szervezet az elektronikus információs rendszerek valamennyi hardver- és szoftvereleméről külön nyilvántartást vezet az ***„N02.2 Informatikai leltár és topológia (szoftver, hardver, liszensz)"*** dokumentumban, külön részletezve a hardver és licensz munkalapokon. Ez tartalmazza legalább az alábbiakat:

Hardver eszköz esetében

- Az eszközök funkcióját.
- Gyártót, modellt, sorozatszámot.
- Beszerzés dátumát és garanciaidőt.
- Az eszköz aktuális helyét és használóját.
- Az eszköz állapotát (aktív/inaktív/selejtezett)

Szoftver licensz esetében

- Az alkalmazás funkcióját.
- Gyártót, modellt, sorozatszámot.
- Beszerzés dátumát és garanciaidőt.
- A licensz típusát és érvényességét
- Az esetleges nem megfeleléseket (pl. licensz túlhasználat, vagy lejárat)
- Ha megfeleltethető a licensz aktuális telepítési helyét és használóját.
- Az eszköz állapotát (aktív/inaktív/selejtezett)

2.3.3. A nyilvántartások kezelése

Az adatok feltöltése és frissítése:

- Az adatok feltöltéséért az adott rendszerrel kapcsolatos feladatokat ellátó informatikus/rendszergazdaüzemeltető rendszergazda, vagy csoport a felelős.
- Minden új rendszer vagy rendszereszköz beszerzésével egyidejűleg fel kell venni azt a nyilvántartásba.
- A nyilvántartást rendszeresen ellenőrizni kell, és minden változást haladéktalanul át kell vezetni.

Az eszközök kivonása: Rendszereszközt a nyilvántartásból csak annak selejtezésekor vagy értékesítésekor lehet kivenni, a megfelelő dokumentáció elkészítésével ***(„N10.3 Selejtezési jegyzőkönyv").***

Az adatok tárolása: A nyilvántartás adatait biztonságos környezetben kell tárolni, amely biztosítja azok bizalmasságát, sértetlenségét és rendelkezésre állását.

Felelős

Az információs vagyonelemek nyilvántartásának naprakészségéről az üzemeltető rendszergazda, vagy csoport gondoskodik.

Felülvizsgálat

A nyilvántartást felülvizsgálata legalább évente egyszer szükséges annak érdekében, hogy pontosan tükrözze az elektronikus információs rendszer aktuális állapotát. Felülvizsgálat szükséges továbbá:

- Jelentős változás esetén (pl. új rendszer bevezetése vagy meglévő rendszer átalakítása).
- Jogszabályváltozás esetén.

Az éves felülvizsgálat eredményeiről jelentést kell készíteni az információbiztonságért felelős személy (IBF) részére, amelyet a belső audit során az IT biztonsági auditjelentés és az intézkedési tervben dokumentál.

2.4. Biztonsági osztályba sorolás

Adatbiztonság szempontjából a szervezet kezelésében lévő elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából ALAP, JELENTŐ, MAGAS – a kockázat növekedésével arányosan növekvő - biztonsági osztályokba kell sorolni. A besorolás eredményét rögzíteni kell az EIR nyilvántartásban, a kockázatelemzés alapján kapott eredményét.

Az osztályba sorolás eredményét az Információ Biztonsági szabályzat 1. számú mellékletében rögzíteni kell.

Az osztályba sorolás folyamatának részletes lépései, a jelentős osztály követelményeinek megfelelően:

1. Adatbiztonsági követelmények meghatározása

A szervezetnek először fel kell mérnie az elektronikus rendszerben kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását. A súlyozást a rendszer funkcióihoz kell igazítani, különös tekintettel az adatvesztés vagy sérülés következményeire.

2. Hatáselemzés végrehajtása

A besorolást kockázatelemzési módszertan alapján kell elvégezni:

- Kötelezően alkalmazni kell a felügyeleti hatóságfelügyeleti jogot gyakorló szerv által kiadott módszertant, ha a szervezetnek nincs sajátja.
- Az elemzésnek tartalmaznia kell az alábbiakat:
- Lehetséges káresemények azonosítását
- Kockázatok kvantitatív (számszerűsítő, matematikai vagy statisztikai értékelés) /qualitatív (szöveges kategóriákba sorolt leírás) értékelését
- A szervezetnek ki kell dolgoznia egy olyan költség-haszon elemzési módszertant, amely átfogóan értékeli az adatvagyon védelmére és visszaállíthatóságára fordított kiadásokat. A módszertan célja, hogy számszerűsíthető formában bemutassa azokat a költségtételeket, amelyek az adatvesztés megelőzésére, illetve bekövetkezése esetén a károk helyreállítására irányulnak. Ennek részeként elemezni kell, tartalmaznia kell az adatbiztonság megteremtésére és fenntartására fordított technikai és szervezeti kiadásokat, az esetleges adatvesztés bekövetkezése után szükséges helyreállítási tevékenységek költségeit, valamint a visszaállításban részt vevő humán erőforrás idő- és bérköltségeit.

A módszertan célja, hogy segítséget nyújtson a vezetés számára a döntéshozatalhoz, a kockázatok és erőforrásigények mérlegeléséhez, valamint az információbiztonsági beruházások megalapozott tervezéséhez az alap biztonsági osztály feltételeinek ellenőrzése

Az alap biztonsági osztályba csak olyan rendszerek kerülhetnek, ahol:

- Legfeljebb csekély kár keletkezhet a rendszer meghibásodásából
- A rendszer megszakadása nem fenyegeti:
- Az emberi életet vagy egészséget
- Közszolgáltatások folytonosságát
- Jelentős anyagi károkat

4. Jóváhagyás és dokumentálás

A besorolási döntést a szervezet vezetőjének kell hivatalosan jóváhagynia. A dokumentációban kötelezően szerepelnie kell:

- A hatáselemzés módszertanának leírása
- A kockázatértékelés részletes eredményei
- A választott biztonsági osztály indoklása

5. Folyamatos felülvizsgálat

A besorolást rendszeresen felül kell vizsgálni, különösen a következő esetekben:

- Rendszer-funkciók változásakor
- Új biztonsági fenyegetések megjelenésekor
- Szabályozási változások alkalmazásakor

Az alap biztonsági osztályba tartozó szervezetek esetében a konkrét védelmi intézkedések közé tartozik például alapvető hozzáférés-vezérlés, rendszeres biztonsági mentések, valamint alapvető incidenskezelési folyamatok kialakítása. A folyamat során különös figyelmet kell fordítani a szabályozási követelmények és a tényleges üzleti kockázatok közötti egyensúlyra.

2.4.1. Adatvagyon-nyilvántartás

A szervezet EIR-ek adatgazdái és információbiztonságért felelős személy közösen készíti el az információs rendszerekben kezelt adatok teljes körű nyilvántartását (***„N13.1.1 EIR nyilvántartás és technikai-adatok-űrlap”).***

- Az adatokat fel kell osztani a feldolgozásuk célja, tartalma, helye és felhasználási időhorizontja szerint.

2.4.2. Kockázatelemzés és kategorizálás

- Az információkat három fő szempont alapján kell besorolni:
- **Bizalmasság**: Kinek lehet joga megismerni az adatokat?
- **Sértetlenség**: Biztosítottak-e a változatlan adatállapotok?
- **Rendelkezésre állás**: Az adatok elérhetők-e a felhasználás céljából?
- Az alap biztonsági osztályba sorolt szervezet, az adatokhoz minimális védelmi elvárások tartoznak, amely megakadályozza az illetéktelen hozzáférést, véletlen törlést vagy adatvesztést.

2.4.3. Biztonsági osztályba sorolás szabályai és beosztása

A biztonsági osztályba sorolás a jogszabályban meghatározásra biztonsági osztályok a következő:

ALAP (korábban 1–2.) biztonsági osztály: Kevésbé kritikus adatok, alapszintű védelem (ideértve a *nyilvánosan elérhető információkat is*).

„legfeljebb csekély káresemény következhet be, mivel:

- *az elektronikus információs rendszerben jogszabály által nem védett adat vagy legfeljebb kis mennyiségű személyes adat sérülhet,*
- *a szervezet üzleti vagy ügymenete szempontjából csekély értékű, vagy csak belső (szervezeti) szabályzóval védett adat vagy rendszer sérülhet,*
- *a lehetséges társadalmi-politikai hatás a szervezeten belül kezelhető, vagy*
- *a közvetlen és közvetett anyagi kár a szervezet éves költségvetésének vagy nettó árbevételének 1%-át nem haladja meg."*

JELENTŐS (korábban 3-4.) biztonsági osztály: Az alapnál magasabb szintű, közepes védelemre szoruló adatok.

„közepes káresemény következhet be, mivel:

- *nagy mennyiségű személyes adat, illetve különleges személyes adat sérülhet,*
- *személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket),*
- *a szervezet üzleti vagy ügymenete szempontjából érzékeny folyamatokat kezelő rendszer, információt képező adat vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet,*
- *a káresemény lehetséges társadalmi-politikai hatásai a szervezettel szemben bizalomvesztést eredményezhetnek, a jogszabályok betartása vagy végrehajtása elmaradhat, vagy a szervezet vezetésében személyi felelősségre vonást kell alkalmazni, vagy*
- *a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 1%-át, de nem haladja meg annak 10%-át."*

MAGAS (korábban 5.) biztonsági osztály: Magasabb szintű védelmet igénylő adatok (*pl. üzleti titkok, nagy mennyiségű vagy különleges személyes adatok*).

„nagy káresemény következhet be, mivel:

- *különleges személyes adat nagy mennyiségben sérülhet,*
- *emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,*
- *nemzeti adatvagyon helyreállíthatatlanul megsérülhet,*
- *az ország, a társadalom működőképességének fenntartását biztosító kritikus infrastruktúra rendelkezésre állása nem biztosított,*
- *a szervezet üzleti vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer vagy információt képező adat tömegesen vagy jelentősen sérülhet,*
- *súlyos bizalomvesztés állhat elő a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok is sérülhetnek, vagy*
- *a közvetlen és közvetett anyagi kár meghaladja a szervezet éves költségvetésének vagy nettó árbevételének 10%-át."*

2.4.4. Dokumentáció és jóváhagyás

A biztonsági osztályba sorolás eredményeit dokumentálni kell az osztályozási lapokon. A végső besorolást az információbiztonságért felelős személy hagyja jóvá az adatgazda tájékoztatása mellett.

Az osztályba sorolás eredményei bekerülnek a szervezet információbiztonsági nyilvántartásába.

2.4.5. Felülvizsgálat és karbantartás

A besorolást évente, a belső audit keretében a belső auditjelentés és intézkedési tervben dokumentálva, valamint minden jelentős változás esetén (pl. adatvagyon bővülése, rendszerfrissítés) felül kell vizsgálni. Hiányosságok esetén 90 napon belül intézkedési tervet kell készíteni és végrehajtani az előírt biztonsági osztályra vonatkozó védelmi intézkedések megvalósítása érdekében.

2.4.6. Kivételek kezelése

A biztonsági osztályba sorolás során nem szükséges részletes külső audit vagy harmadik fél által végzett mélyreható kockázatelemzés). Nem szükséges az biztonsági osztályba sorolás teljes körű dokumentációjának egyeztetése jogi szakértőkkel.

2.4.7. Speciális figyelmeztetések

Az alap biztonsági osztályba sorolt szervezetek által kezelt rendszereket és adatokat mindig úgy kell kialakítani, hogy:

- A minimális biztonsági követelményeket (pl. jelszóvédelem, naplózás) teljesítsék.
- Az osztályozott adatokhoz kizárólag az arra jogosultak férhessenek hozzá.
- A rendszereken belüli változások azonnal frissítésre kerüljenek a nyilvántartásokban.

2.4.8. A biztonsági osztályba sorolás felülvizsgálata

A besorolást minimum kétévente, de minden, az elektronikus információs rendszereket érintő változás után, illetve jogszabályváltozás esetén felül kell vizsgálni és szükség esetén ismételten el kell végezni.

2.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

A Szervezetnek minden hozzáférési engedélyezési folyamatát dokumentálni kell, és auditálhatóvá kell tennie.

2.5.1. Új felhasználó hozzáférésének engedélyezése

Az új munkatársak csak a felhasználói szabályok megismerését és elfogadását követően ***(„N14.2.1 EIR felhasználási szabályok elfogadó nyilatkozat")*** aláírása után, valamint a biztonsági oktatási terv és naplóban regisztrált belépéskori IT biztonsági **oktatás** elvégzése és az ***(„N14.2.2 Titoktartási nyilatkozat")*** aláírása után kaphatnak egyedi hozzáférést az elektronikus információs rendszerekhez.

A belépő munkatárs hozzáférési jogköreit az érintett vezető határozza meg, aki a szükséges jogosultságokat az ***„N02.1.1 Fiók igénylő lap"***-on igényli, amely a megjelölt EIR-ekhez tartozó adatgazdák jóváhagyása után az jogosult által beállításra és felvezetésre kerül az ***„N14.2.3 EIR Hozzáférés engedélyezés"*** kiadása után, megfelelő mértékű dokumentálás mellett.

2.5.2. A jogosultságok jóváhagyása

Az igényelt jogosultságokat az érintett vezető írásban továbbítja jóváhagyásra a szervezet vezetőjének. A szervezet vezetője jogosult a hozzáférések kiadását megtagadni, de döntését indokolnia kell az igénylő felé. Az érintett vezető ilyen esetben kérheti az IBF állásfoglalását.

2.5.3. A jogosultságok beállítása

A jóváhagyott jogosultságigénylő lap formanyomtatvány alapján az érintett rendszer adminisztrátora állítja be a hozzáféréseket. Az adminisztrátornak tilos az engedélyben nem szereplő jogosultságokat beállítani. Az IBF szúrópróbaszerűen ellenőrzi a beállított jogosultságok megfelelőségét.

2.5.4. A változások kezelése

Amennyiben az információbiztonsági szabályozásban, feladat- vagy felelősségi körökben változás történik, azt vezetői jóváhagyás után át kell vezetni a munkaköri leírásban, amelyeket aláírással kell érvényesíttetni az érintettekkel.

Ha a változások vállalkozói szerződéseket érintenek, a szervezet vezetése kezdeményezi azok módosítását vagy kiegészítését a biztonsági követelményeknek megfelelően.

2.5.5. Új munkakörök kialakítása

Új munkakörök létrehozása esetén a szervezet vezetője tájékoztatja az IBF-et a munkakör feladatairól és tervezett jogosultságairól. Az IBF javaslatot tehet a munkakör biztonsági vonatkozásainak kialakítására.

2.5.6. Felülvizsgálat és naprakészség

A hozzáférési jogosultságokat évente felül kell vizsgálni annak biztosítása érdekében, hogy azok megfeleljenek az aktuális feladatköröknek és biztonsági követelményeknek. A nem indokolt jogosultságokat haladéktalanul vissza kell vonni.

2.5.7. Távoli hozzáférések szabályozása

Távoli -külső hozzáférést csak titkosított kapcsolaton keresztül lehet biztosítani (pl. VPN), és azt dokumentálni kell ***(„N14.3 Külső felhasználó -személyi biztonsági szabályzat").*** A távoli hozzáférések biztonságáért mind az adminisztrátor, mind a felhasználó felelős.

2.5.8. Külső partnerek hozzáférése

Külső szerződött partnerek csak külön engedéllyel és dokumentált módon kaphatnak jogot -férhetnek hozzá a rendszerekhez, ***„N14.3 Külső felhasználó -személyi biztonsági szabályzat"*** megismerése és elfogadása ***„N14.3.1 Külső felhasználási szabályok elfogadó nyilatkozat" és „N14.2.2 Titoktartási nyilatkozat"*** aláírása után. A külső partnerek számára kiadott jogosultságokat szigorúan kell nyilvántartani ***(„N14.3.1 Külső felhasználók nyilvántartása")*** kizárólag a szükséges ideig biztosítani a hozzáférést. Amennyiben a kiadott hozzáférés indokolatlanná válik, haladéktalanul vissza kell vonni.

2.5.9. Biztonsági események (incidensek) kezelése

Ha egy felhasználó hozzáférési jogaihoz kapcsolódóan biztonsági esemény történik ***(„N09.1.2 Biztonsági események naplója")*** dokumentálni szükséges (pl. jogosulatlan hozzáférés), azt haladéktalanul jelenteni kell az IBF-nek. Az esemény kivizsgálását követően döntést kell hozni, amennyiben a biztonsági esemény súlyossága indokolja a hatóság részére a bejelentést meg kell tenni. A felhasználó jogosultságait fel kell függeszteni, vagy módosítani kell az érintett jogosultságokat.

2.6. Biztonságtervezési eljárásrend

A szervezet megfogalmazza, dokumentálja, és a munka- és feladatkörük miatt érintettek számára kihirdeti a ***„N13 Biztonságtervezési szabályzat"***-ot, amely elősegíti a biztonságtervezési szabályzat és

az ehhez kapcsolódó ellenőrzések megvalósítását. A biztonságtervezési eljárásrend célja ***(„N13.1 Biztonságtervezési eljárásrend")***, hogy az információs rendszerek tervezésekor, fejlesztésekor, üzemeltetésekor és kivonásakor biztosítsa az információk bizalmasságát, sértetlenségét és rendelkezésre állását. A szervezet az Biztonságtervezési eljárásrendet vagy más belső szabályozását évente legalább egyszer, valamint az alábbi esetekben felülvizsgálja és frissíti:

- jelentős változások az elektronikus információs rendszerekben vagy azok környezetében,
- új jogszabályi előírások megjelenése,
- kockázatelemzés) során feltárt hiányosságok kezelése érdekében.

Életciklus-szemlélet

A szervezet az információs rendszerek életciklusának alábbi szakaszait határozza meg biztonságtervezési szempontból:

1. **Követelmény meghatározás:** Az információs rendszer céljainak, funkcióinak és biztonsági követelményeinek definiálása.
2. **Fejlesztés vagy beszerzés:** Az információbiztonsági követelmények figyelembevétele a rendszer fejlesztése vagy beszerzése során.
3. **Megvalósítás vagy értékelés:** A rendszer tesztelése, telepítése és biztonsági szempontú értékelése.
4. **Üzemeltetés és fenntartás:** Az információbiztonsági intézkedések folyamatos biztosítása az üzemeltetés során (pl. naprakész frissítések, naplózás).
5. **Kivonás (archiválás, megsemmisítés):** A rendszer biztonságos kivonása az üzemeltetésből, beleértve az adatok törlését vagy archiválását.

Kapcsolódó szabályzatok és előírások

A rendszerbiztonság tervezésekor a szervezet figyelembe veszi:

- az *Információbiztonsági Politikában* megfogalmazott célokat és követelményeket,
- a gyártói és iparági előírásokat, ajánlásokat (pl. ISO 27001 szabvány),
- a jogszabályban meghatározott biztonsági osztályba sorolási követelményeket.

Kockázatalapú megközelítés

A biztonságtervezés során minden életciklus-szakaszban kockázatelemzést kell végezni annak érdekében, hogy azonosítsák és kezeljék a potenciális fenyegetéseket. Az eredményeket dokumentálni kell.

Biztonsági ellenőrzések

A rendszer életciklusának minden szakaszában ellenőrizni kell a biztonsági intézkedések megfelelőségét. A tesztelési fázisban különösen fontos a sebezhetőségi vizsgálatok elvégzése.

Dokumentáció

Minden életciklus-szakaszhoz kapcsolódóan részletes dokumentációt kell készíteni (pl. rendszerbiztonsági terv, tesztelési jelentések-jegyzőkönyvek).

Személyi kompetenciák

A biztonságtervezésben részt vevő személyeknek megfelelő képzettséggel kell rendelkezniük; szükség esetén képzést kell biztosítani számukra.

Felelősök

- A biztonságtervezési eljárásrend kidolgozásáért és karbantartásáért az IBF felelős.
- Az éves felülvizsgálatot a szervezet vezetője hagyja jóvá.

2.7. Rendszerbiztonsági terv

A szervezet az elektronikus információs rendszereihez rendszerbiztonsági tervet terveket készít[1] ***(„N07.1.1 Üzletmenet-folytonossági terv rendszerelemekre")***, amely biztosítja a rendszerek biztonságos működését, valamint támogatja az információbiztonsági célok és követelmények teljesítését. A rendszerbiztonsági terv az alábbiakat tartalmazza:

- **Összhang a szervezeti felépítéssel és architektúrával:** A rendszerbiztonsági terv figyelembe veszi a szervezet felépítését és az informatikai architektúráját.
- **Hatókör és alapfeladatok meghatározása:** A terv pontosan meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait biztosítandó (szolgáltatásokat, biztonságkritikus elemeit és funkcióit.
- **Biztonsági osztály meghatározása:** A rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályba sorolását rögzíti, összhangban a rendelet előírásaival.
- **Működési körülmények és kapcsolatok:** A terv tartalmazza a rendszer működési környezetének leírását, valamint más rendszerekkel való kapcsolatait (pl. interfészek, adatáramlások).
- **Biztonsági követelmények dokumentálása:** A vonatkozó rendszerdokumentáció keretében meghatározza az elektronikus információs rendszer biztonsági követelményeit.
- **Védelmi intézkedések meghatározása:** Leírja a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, valamint ezek bővítési lehetőségeit. Ide tartozik a jogszabályok által előírt biztonsági feladatok végrehajtása is.
- **Védelmi intézkedések meghatározása:** Leírja a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, valamint ezek bővítési lehetőségeit. Ide tartozik a jogszabályok által előírt biztonsági feladatok végrehajtása is.
- **Ismertetés az érintettekkel:** Gondoskodik arról, hogy a tervet a meghatározott személyek és szerepkörök megismerjék, ideértve annak változásait is.
- **Felülvizsgálat és frissítés:** A rendszerbiztonsági tervet a belső szabályozásban vagy magában a tervben meghatározott gyakorisággal felül kell vizsgálni. Frissítés szükséges az alábbi esetekben:
- Az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások esetén.
- A védelmi intézkedések végrehajtása vagy értékelése során feltárt problémák alapján.
- **Belső egyeztetések elvégzése:** A terv elkészítése és frissítése során biztosítani kell a szükséges belső egyeztetéseket, különös tekintettel az érintett szerepkörökre (pl. IBF, adatgazda, rendszergazda).
- **Hozzáférés védelme:** Gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlan személyek számára ne legyen megismerhető vagy módosítható.

Kivételes esetek

[1] A Nemzeti Kibervédelmi Intézet által kiadott rendszerbiztonsági terv sablonok elérhetőek és letölthetőek a https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/a-7-2024-mk-rendelet-alapjan-aktualizalt-rendszerbiztonsagi-terv-sablonok/ oldalról.

Ha egy adott információs rendszer jelentősége nem indokolja, illetve a jogi-, szabályozási- és üzemeltetési körülmények nem teszik lehetővé, a szervezet vezetője az IBF egyetértésével eltekinthet az adott rendszerre vonatkozó rendszerbiztonsági terv készítésétől. E döntést dokumentálni kell.

Felelősök

A rendszerbiztonsági terv elkészítéséért, naprakészen tartásáért és felülvizsgálatáért az adott EIR adatgazdája felelős. A terv jóváhagyása és kihirdetése a szervezet vezetőjének feladata.

2.8. Személyi biztonság

Ez a fejezet biztosítja, hogy minden felhasználó tisztában legyen a rá vonatkozó szabályokkal és kötelezettségekkel, valamint garantálja a hozzáférések megfelelő kezelését az alap biztonsági osztály követelményeinek megfelelően. A nyilatkozatok és oktatások révén megelőzhetőek a jogosulatlan hozzáférések és egyéb biztonsági kockázatok.

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségeket, valamint az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen dokumentum és az adott rendszerdokumentáció tartalmazza. A rendszerbiztonság és a hozzáférési jogosultságok megfelelő kezelése érdekében a következő eljárásokat kell alkalmazni:

2.8.1. Hozzáférési jogosultság engedélyezése

A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek írásbeli nyilatkozatot kell tennie az ***„N14.2.1 EIR felhasználási szabályok elfogadó nyilatkozat"*** dokumentumon arról, hogy:

- az érintett rendszer használatához kapcsolódó biztonsági szabályokat és kötelezettségeket megismerte,
- azokat saját felelősségére betartja.
- Az új belépő munkatársak csak a belépéskori IT biztonsági oktatást követően és a nyilatkozatok aláírása után kaphatnak hozzáférést a rendszerekhez dokumentált formában.

2.8.2. Felhasználói elvárások és kötelezettségek

A felhasználók kötelesek:

- Betartani az Információbiztonsági Szabályzatban meghatározott előírásokat.
- Csak azokra az adatokra és funkciókra hozzáférést biztosítani, amelyek munkakörük ellátásához szükségesek.
- Gondoskodni arról, hogy jelszavaik és hitelesítő adataik biztonságban legyenek, és ne kerüljenek illetéktelen kezekbe.
- Az általuk használt rendszerekben kizárólag a jóváhagyott tevékenységeket végezni.
- Azonnal jelenteni minden gyanús eseményt vagy potenciális biztonsági incidenst az IBF-nek vagy közvetlen vezetőjüknek.

A felhasználók számára tilos:

- Más felhasználók azonosítóit vagy jelszavait használni.
- Jogosulatlanul hozzáférni olyan adatokhoz vagy rendszerekhez, amelyekhez nincs engedélyük.
- A rendszereken belüli bármilyen módosítást végrehajtani, amely nem tartozik munkakörükhöz.
- Olyan tevékenységet folytatni, amely veszélyezteti a rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

2.8.3. Felülvizsgálat és frissítés és felelősök

A hozzáférési jogosultságokkal kapcsolatos szabályokat évente felül kell vizsgálni, illetve minden jelentős változás esetén frissíteni kell. Ide tartoznak például:

- Munkakör-változások,
- Új rendszerek bevezetése,
- Jogszabályi változások.

Felelősök

- Az elektronikus információs rendszerek biztonságáért felelős személy (IBF) ellenőrzi a szabályok betartását és gondoskodik azok aktualizálásáról.
- A szervezet vezetője jóváhagyja a hozzáférési jogosultságokkal kapcsolatos szabályokat. Az érintett felelősökkel megismerteti annak tartalmát, a folyamat végrehajtására vonatkozó előírásokat és utasításokat.

2.9. Rendszer és szolgáltatás beszerzés

2.9.1. Beszerzési eljárásrend

A szervezet megfogalmazza, dokumentálja, és a szervezeten belül kihirdeti a beszerzési Informatikai Beszerzési Szabályzatot ***(„N16 Informatikai Beszerzési Szabályzat")***, amely az alábbiakat tartalmazza:

- Az elektronikus információs rendszerekre, az ezekhez kapcsolódó szolgáltatásokra és az információs rendszer biztonsági eszközök beszerzésére vonatkozó szabályokat.
- Az eljárásrend célja, hogy biztosítsa a beszerzések során az információbiztonsági követelmények érvényesülését, összhangban a szervezet általános beszerzési szabályzatával.
- A beszerzési folyamatokhoz kapcsolódó ellenőrzések megvalósítását és dokumentálását.

A beszerzési eljárásrendben ***(„N16.1 Informatika Beszerzési eljárásrend")***, vagy más belső szabályozásban meghatározott gyakorisággal felül kell vizsgálni és szükség esetén frissíteni kell az eljárásrendet annak érdekében, hogy megfeleljen a jogszabályi változásoknak vagy a szervezet működésében bekövetkező változásoknak.

2.9.2. A rendszer fejlesztési életciklusa

A szervezet az elektronikus információs rendszereinek teljes életútján figyelemmel kíséri azok információbiztonsági helyzetét, és minden életciklus-szakaszban biztosítja az információbiztonsági követelmények betartását. Az életciklus-szemlélet az alábbi szakaszokat foglalja magában:

Követelmény meghatározás:

- A rendszer céljainak, funkcióinak és biztonsági követelményeinek definiálása.
- Az információbiztonsági szempontok beépítése már a tervezési fázisba.

Fejlesztés vagy beszerzés:

- Az eszközök és rendszerek beszerzésénél biztosítani kell, hogy azok megfeleljenek a jelen szabályzatban rögzített információbiztonsági követelményeknek.
- A fejlesztési folyamat során figyelembe kell venni az iparági szabványokat és ajánlásokat.

Megvalósítás vagy értékelés:

- A rendszer telepítése, tesztelése és biztonsági szempontú értékelése.

- A biztonsági intézkedések hatékonyságának ellenőrzése.

Üzemeltetés és fenntartás:

- Az üzemeltetés során biztosítani kell a folyamatos megfelelőséget (pl. naprakész frissítések, naplózás).
- Az informatikai üzemeltetés naprakész nyilvántartást vezet az általa kiadott vagy telepített eszközökről szoftver/program, verziókövetés) az IT leltár dokumentumban.

Kivonás (archiválás, megsemmisítés):

- A rendszerek biztonságos kivonása az üzemeltetésből, beleértve az adatok törlését vagy archiválását.
- Gondoskodni kell arról, hogy a kivonás során ne sérüljenek az adatok bizalmasságára, sértetlenségére vagy rendelkezésre állására vonatkozó követelmények.

Információbiztonsági szerepkörök és felelősségek

A szervezet meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket a fejlesztési életciklus minden szakaszára vonatkozóan:

- Kijelöli a szerepköröket betöltő személyeket (pl. IBF, adatgazda), akik felelősek az adott szakaszban előírt biztonsági feladatok végrehajtásáért.
- Biztosítja, hogy minden érintett szerepkör tisztában legyen a rá háruló feladatokkal.

Felülvizsgálat

A rendszer fejlesztési életciklusát érintő szabályokat évente felül kell vizsgálni, valamint minden jelentős változás esetén frissíteni kell annak érdekében, hogy azok megfeleljenek a jogszabályi előírásoknak és a szervezet aktuális működési környezetének.

2.10. Biztonságelemzési eljárásrend

A szervezet megfogalmazza, dokumentálja és az érintett szervezeten belül kihirdeti a biztonságelemzési szabályzatot ***(„N05 Biztonságértékelési szabályzat")***, amely támogatja a biztonságértékelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását. Az eljárásrend célja ***(„N05.1 Biztonságértékelési eljárásrend")***, hogy biztosítsa az elektronikus információs rendszerek és azok működési környezetének folyamatos biztonsági megfelelőségét.

Biztonságértékelési terv

A szervezet biztonságértékelési tervet készít, amelyben meghatározza:

- Az elektronikus információs rendszerek és működési környezetük védelmi intézkedéseinek rendszeres értékelését.
- A bevezetett intézkedések működőképességének kontrollját.
- Az intézkedések tervezett működésének ellenőrzését.
- Az értékelés eredményének összefoglalását egy jelentésben Biztonságértékelési eljárásrend – 1.sz melléklet - értékelő táblázat.

A biztonságértékelési jelentést a szervezet által meghatározott szerepköröket betöltő személyek számára hozzáférhetővé kell tenni, figyelembe véve a jogosultságokat.

A biztonsági értékelés tartalma

A biztonsági értékelés az alábbiakat foglalja magában:

- **Értékelendő védelmi intézkedések:** Adminisztratív, fizikai és logikai védelmi intézkedések.

- **Ellenőrzések eredményessége:** Az ellenőrzések hatékonyságát meghatározó eljárásrendek.
- **Értékelési környezet:** Az értékelés célja, az értékelést végző csoport feladatai és az értékelési módszerek.

Biztonsági mérés és felügyelet

A szervezet kifejleszti és felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét. Ez magában foglalja:

- A biztonsági mérőszámok meghatározását és azok folyamatos ellenőrzését IT biztonsági mérőszámok.
- A mérések eredményeinek összehasonlító elemzését a korábbi adatokkal.
- A mérések alapján tett javaslatok megvalósítását.

Felülvizsgálat és frissítés

A biztonságelemzési eljárásrendet és a hozzá kapcsolódó terveket évente, vagy az alábbi esetekben kell felülvizsgálni:

- Jelentős változások az elektronikus információs rendszerekben vagy azok környezetében.
- Jogszabályi változások esetén.
- kockázatelemzés) során feltárt hiányosságok kezelése érdekében.

Felelősök

- Az elektronikus információs rendszerek biztonságáért felelős személy (IBF) felelős a biztonságelemzési eljárásrend kidolgozásáért és felülvizsgálatáért, végrehajtásáért szervezet vezetője a felelős.
- A szervezet vezetője jóváhagyja a biztonságelemzési tervet, valamint biztosítja annak végrehajtásához szükséges erőforrásokat.

2.11. Tesztelés, felügyelet

A szervezet megfogalmazza, dokumentálja és kihirdeti az elektronikus információs rendszerek tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat biztonsági mérések eljárásait. Ezek az eljárások támogatják a tesztelési, képzési és felügyeleti tevékenységek fejlesztését, fenntartását és folyamatos végrehajtását. A szervezet a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia, valamint a lehetséges vagy bekövetkezett biztonsági események súlya alapján rendszeresen felülvizsgálja.

2.11.1. Biztonsági mérés és felügyelet

A szervezet kifejleszti és felügyeli az elektronikus információs rendszerei biztonsági mérésének rendszerét, a biztonságértékelési eljárásrendet, (***„N13.1 Biztonságtervezési eljárásrend")*** amely magában foglalja:

- Mellékletként a biztonsági mérőszámok meghatározását és azok folyamatos ellenőrzését.
- A mérések eredményeinek összehasonlító elemzését a korábbi adatokkal.
- A mérések alapján tett javaslatok megvalósítását.

2.11.2. Sérülékenységvizsgálat

Rendszeres sérülékenységvizsgálatok

- A szervezet meghatározott rend szerint sérülékenységi tesztet végez - vagy végeztet - az elektronikus információs rendszerei és alkalmazásai tekintetében
- Sérülékenységi tesztet kell végezni/végeztetni akkor is, ha új sérülékenység kerül azonosításra és jelentésre az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban.
- a sérülékenységvizsgálatot lehetőség szerint az éles üzem megzavarása nélkül szükséges lefolytatni - ha azt a rendszer fejlesztési, üzemeltetési és használati körülményei lehetővé teszik.

Külső szervezet bevonása

- A sérülékenységi vizsgálatot külső szervezet is végezheti azon rendszerek esetében, amelyek az érintett szervezet felügyelete alatt állnak.
- a szervezet szükség esetén az elektronikus információs rendszer különleges jogosultsághoz kötött (privilegizált) hozzáférést biztosít a kijelölt rendszerelemekhez a vizsgálat végrehajtásához.

Tesztelési folyamat

- A tesztet lefuttatását követően kimutatás készül a feltárt hibákról és nem megfelelő beállításokról.
- Végrehajtásra kerülnek az ellenőrzési listák és tesztelési eljárások.
- Felmérik a sérülékenység lehetséges hatásait.
- Elemzik a sérülékenységi teszt eredményét, és megosztják azt a szervezet vezetőjével, illetve a rendszer üzemeltetésében résztvevőkkel (rendszergazdákkal).
- Meghatározásra kerül, hogy egy esetleges támadó milyen információkat képes elérni az elektronikus információs rendszerben - ennek elhárítására javítási javaslatokat tesz.

Eszközhasználat

- javasolt olyan sérülékenységi teszteszközt alkalmazása, amely könnyen bővíthető az ismertté váló új sérülékenységekkel.

A NIS2 irányelv és az ahhoz kapcsolódó magyar szabályozások lehetőséget biztosítanak arra, hogy NIS2 hatálya alá tartozó szervezetek külső szakértői (szolgáltatásokat vegyenek igénybe sérülékenységvizsgálatokhoz, feltéve, hogy ezek megfelelnek az előírt szabványoknak és minőségi követelményeknek (pl. ISO 27001 vagy más releváns tanúsítványok).

Állami szervezetek és az OKF nyilvántartásába tartozó szervezetek esetében a hatályos jogszabályok a sérülékenységvizsgálat lefolytatását külön engedélyhez kötik!

2.11.3. Eredmények kezelése

A sérülékenységi teszt eredményei alapján az informatikai vezetőutasításokat ad a rendszergazdának a feltárt hiányosságok megszüntetésére. Az eredmények dokumentálása kötelező, és azok alapján cselekvési tervet kell készíteni.

2.11.4. Felügyeleti tevékenységek

Folyamatos ellenőrzések

Az elektronikus információs rendszerek működésének folyamatos figyelemmel kísérése érdekében naplózásra és monitorozásra van szükség. A naplózott eseményeket rendszeresen értékelni kell, különösen biztonsági incidensek esetén.

Felhasználói oktatás

A felhasználóknak rendszeres képzésben kell részesülniük az informatikai biztonsági szabályok betartása érdekében.

Felülvizsgálat

A felügyeleti tevékenységeket évente legalább egyszer át kell tekinteni, hogy megfeleljenek az aktuális biztonsági követelményeknek.

2.12. Biztonsági eseménykezelési eljárásrend (Incidenskezelés)

A szervezet kidolgozza, dokumentálja és kihirdeti a biztonsági események kezelésére vonatkozó eljárásrendet azaz az eseménykezelési eljárásrend dokumentumot, amely biztosítja a biztonsági események hatékony kezelését és az információs rendszerek védelmét. Az eljárásrend az alábbiakat foglalja magában:

Eseménykezelési folyamat

A biztonsági események kezelése az alábbi szakaszokból áll:

Előkészület:

- Az eseménykezelési terv kidolgozása és kommunikálása az érintett szerepkörök felé.
- Az információbiztonsági képzések biztosítása a felhasználók számára.

Észlelés:

- A biztonsági események felismerése és azonnali jelentése.
- Az elektronikus információs rendszerek folyamatos monitorozása és naplózása.

Vizsgálat:

- Az esemény okainak, körülményeinek és hatásainak részletes elemzése.

Elszigetelés:

- Az érintett rendszerek vagy erőforrások izolálása a további károk megelőzése érdekében.

Megszüntetés:

- A biztonsági eseményt kiváltó okok megszüntetése, beleértve a sérülékenységek kijavítását.

Helyreállítás:

- Az érintett rendszerek eredeti állapotának visszaállítása, beleértve az adatok helyreállítását és a szolgáltatások újraindítását.

Tanulságok levonása:

- Az eseményből származó tapasztalatok beépítése a folyamatokba, szabályzatokba és képzésekbe.

Eseménykezelési (incidenskezelési) terv

A szervezet biztonsági eseménykezelési tervet dolgoz ki ***(„N09.1.1 Biztonsági eseménykezelési terv")*** amely:

- Iránymutatást nyújt a biztonsági események kezelésének módjaira.
- Meghatározza a bejelentésköteles biztonsági eseményeket.
- Leírja az események kategorizálásának és súlyosságuk értékelésének kritériumait.
- Meghatározza az erőforrásokat és vezetői támogatást, amelyek szükségesek az eseménykezelési lehetőségek bővítésére és fenntartására.
- Kihirdeti és tudomásul veteti a tervet az érintett személyekkel és szervezeti egységekkel.
- Rendszeresen felülvizsgálja és frissíti a tervet az információs rendszer változásainak vagy tapasztalatok alapján feltárt problémák figyelembevételével.

Dokumentáció és jelentéstétel

A szervezet:

- Nyomon követi és dokumentálja az összes biztonsági eseményt, incidenst ***(„N09.1.2 Biztonsági események naplója")***
- beleértve azok okait, kezelésének módját és eredményeit.

Jogszabályban meghatározott módon jelenti a releváns információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek (pl. GovCERT-Hungary) ***(„N09.1.3 Biztonsági esemény bejelentési űrlap").***

Felhasználói kötelezettségek

Minden felhasználótól megköveteli, hogy:

- Jelentsék a biztonsági eseményt vagy annak gyanúját közvetlen vezetőjüknek vagy az IBF-nek.
- Vegyenek részt az eseménykezelési képzéseken, amelyek biztosítják számukra a megfelelő ismereteket szerepkörükhöz igazítva.

Képzés

A szervezet rendszeres időközönként biztosítja:

- A felhasználók képzését a biztonsági események felismeréséről és kezeléséről.
- Új szerepkörök vagy felelősségi körök kijelölése esetén soron kívüli képzést.

Hozzáférésvédelem

Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlan személyek számára ne legyen hozzáférhető vagy módosítható.

2.13. Kockázatkezelés

A szervezet kockázatkezelési eljárásrendet alakít ki és alkalmaz az információbiztonsági kockázatok azonosítására, értékelésére és kezelésére. A kockázatkezelési folyamat célja, hogy biztosítsa az információbiztonsági célok elérését és a követelményeknek való megfelelést.

2.13.1. Kockázatkezelési eljárásrend

A szervezet kidolgozza és dokumentálja ***„N15 Kockázatmenedzsment szabályzat"-ot*** és a ***„N15.1 Kockázatelemzési és kockázatkezelési eljárásrend"*** -et, amely tartalmazza:

- A kockázatértékelés módszertanát
- A kockázatok azonosításának, elemzésének és értékelésének folyamatát
- A kockázatkezelési intézkedések meghatározásának és végrehajtásának módját
- A kockázatok nyomon követésének és felülvizsgálatának rendjét.

2.13.2. Kockázatértékelés

A szervezet évente legalább egyszer átfogó kockázatértékelést végez, amely kiterjed:

- Az információs rendszerek és adatok azonosítására
- A fenyegetések és sebezhetőségek feltárására
- A potenciális hatások elemzésére

- A kockázati szintek meghatározására

A kockázatértékelés eredményeit dokumentálni kell kockázatértékelési jelentés.

2.13.3. Kockázatkezelési stratégia

A szervezet a kockázatértékelés alapján kockázatkezelési stratégiát dolgoz ki, amely meghatározza:

- A kockázatok elfogadható szintjét
- A kockázatkezelés prioritásait
- A kockázatkezelési intézkedések típusait (elkerülés, csökkentés, áthárítás, elfogadás).

2.13.4. Kockázatkezelési intézkedések

A szervezet a kockázatkezelési stratégia alapján konkrét intézkedéseket határoz meg és hajt végre a kockázatok csökkentésére. Ezek lehetnek:

- Technikai kontrollok bevezetése vagy fejlesztése
- Adminisztratív szabályozások kialakítása vagy módosítása
- Képzések és tudatosító programok szervezése
- Biztonsági incidenskezelési képességek fejlesztése

2.13.5. Kockázatok nyomon követése és felülvizsgálata

A szervezet folyamatosan nyomon követi a kockázatokat és az alkalmazott kontrollok hatékonyságát. Évente felülvizsgálja a kockázatkezelési folyamatot és szükség esetén aktualizálja azt.

2.13.6. Jelentéstétel

Az IBF évente jelentést készít a szervezet vezetősége számára a kockázatkezelési tevékenységről és annak eredményeiről a kockázatkezelési jelentést.

2.14. Beszállítói lánc kezelése

A szervezet a követelményeknek megfelelően nyilvántartja az ***„N19.2 Ellátási lánc nyilvántartása"*** dokumentumban alvállalkozóit és beszállítóit. A szervezet az alábbi intézkedéseket alkalmazza a beszállítói lánc biztonságának kezelésére:

2.14.1. Beszállítói kockázatértékelés

- A szervezet évente legalább egyszer átfogó kockázatértékelést végez a kritikus beszállítókra vonatkozóan az Információbiztonsági kérdőív beszállítóknak -kérdőív kiküldésével és kiértékelésével.
- A szervezet megtervezi a beszállítói lánc kiesésére vonatkozó védelmi stratégiákat. Az ellátási lánc biztonságát kockázatalapú megközelítéssel kezeli, amely kiterjed a kulcsfontosságú beszállítókra, alvállalkozókra, valamint ezek informatikai kapcsolatainak ellenőrzésére is.

A kockázatértékelés kiterjed a beszállítók által nyújtott szolgáltatások és termékek biztonsági aspektusaira.

Az eredményeket dokumentálni kell az ***„N19.4 Ellátási lánc kockázatelemzés jelentés"-ben.***

Beszállítói szerződések biztonsági követelményei

- A kritikus beszállítókkal kötött szerződéseknek tartalmazniuk kell az információbiztonsági követelményeket.
- A szerződésekben ki kell térni az adatvédelmi, titoktartási és incidenskezelési kötelezettségekre.
- A beszállítóknak vállalniuk kell, hogy megfelelnek a szervezet információbiztonsági szabályzatának.

2.14.2. Beszállítói auditok

- A szervezet jogot formál arra, hogy évente legalább egyszer auditálja kritikus beszállítóit.
- Az auditok kiterjednek a beszállítók információbiztonsági gyakorlataira és folyamataira.

Az audit eredményeit dokumentálni kell ellátási lánc kockázatelemzés jelentés.

2.14.3. Incidenskezelés a beszállítói láncban

- A beszállítóknak kötelességük 24 órán belül jelenteni minden olyan biztonsági incidenst[2], amely érintheti a szervezet adatait vagy rendszereit.

A szervezet eljárásrendet dolgoz ki a beszállítói incidensek kezelésére ***(„N19 Ellátási lánc kockázatmenedzsment szabályzat")***

2.14.4. Beszállítói kapcsolattartás

- A szervezet kijelöl egy felelős személyt vagy csoportot a beszállítói kapcsolatok kezelésére.
- Rendszeres (legalább negyedéves) egyeztetéseket kell tartani a kritikus beszállítókkal a biztonsági kérdések megvitatására.

2.14.5. Beszállítói jogosultságok kezelése

- A beszállítók hozzáférését a szervezet rendszereihez szigorúan korlátozni és ellenőrizni kell.
- A hozzáféréseket rendszeresen felül kell vizsgálni és a már nem szükséges jogosultságokat azonnal vissza kell vonni.

2.14.6. Beszállítói lánc folyamatos monitorozása

- A szervezet folyamatosan figyelemmel kíséri a beszállítói láncot érintő fenyegetéseket és sebezhetőségeket.
- Szükség esetén azonnali intézkedéseket hoz a felmerülő kockázatok kezelésére.

2.14.7. Oktatás és tudatosítás

- A szervezet évente legalább egyszer oktatást tart a beszállítói lánc biztonságáért felelős felhasználók számára.
- A képzés kiterjed a legújabb fenyegetésekre és védelmi technikákra.

[2] Nemzeti Kíberbiztonsági Intézet (NKI); https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/ Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH); Hivatali kapu azonosító (KRID) 469506375

3. Adatok és IT rendszerek védelme, biztonsága

Jelen fejezet alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, vagyon- és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre, valamint arra, hogy e fejezet rendelkezései az adott létesítmény bárki által szabadon látogatható vagy igénybe vehető területeire nem vonatkoznak. Kiemelten kell kezelni a jogszabályban előírt, a vissza követhetőség elvének betartását. A fizikai védelmi intézkedéseknek biztosítaniuk kell, hogy minden hozzáférés, belépés és releváns tevékenység egyértelműen visszakövethető legyen, lehetővé téve az események utólagos vizsgálatát és azonosítását.

3.1. Fizikai védelmi intézkedések

Azon helyiségek kijelölése, illetve kialakítása során, amelyekben a szervezet kiemelt fontosságú kiszolgáló számítógépei (szerverei) kerülnek elhelyezésre, különös figyelmet kell fordítani a fokozott biztonságra.

A szerverhelyiség közelében nem üzemelhet tűz- és robbanásveszélyes raktár. A helyiségben független áramellátással működő tűzjelző rendszert kell kiépíteni, a bejárat közelében az informatikai eszközökhöz megfelelő oltóberendezést kell elhelyezni. A berendezések üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell.

A szerverszobában az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat (klímaberendezés), a folyamatos kontrol érdekében olyan védelmi eszközök beszerzése szükséges, amelyek a meghatározott paraméterektől eltérés esetén riasztást küldenek a meghatározott szerepkör részére.

3.1.1. Fizikai védelmi eljárásrend

A szervezet elkészíti az ***„N12 Fizikai védelmi szabályzat"-ot,*** amely a fizikai és környezeti biztonságra vonatkozó óvintézkedések a szervezeti rendszereknek helyet adó létesítmények, a rendszer-erőforrások és a működést biztosító alap(szolgáltatások védelmével kapcsolatban fogalmaz meg szabályokat annak érdekében, hogy:

- a számítástechnikai szolgáltatások megszakadását,
- eszközök ellopását,
- a fizikai károkozást,
- az információk jogosulatlan felfedését,
- a rendszer sértetlenségének elvesztését megakadályozzák.

A szervezet legalább éves gyakorisággal felülvizsgálja és frissíti az ***„N12.1 Fizikai védelemi eljárásrend"-et.***. A szervezeti számítógépek és adathordozók fizikai védelmét biztosítani kell a szervezetben lopás, rongálás és megsemmisülés ellen értékarányos módszerekkel és eljárásokkal (pl. élőerős védelem és fizikai védelem – rácsok, ajtók, riasztóberendezés). A hardverek és adatok részleges vagy teljes megsemmisülésével fenyegető tüzek megelőzése és elhárítása a Tűzvédelmi Szabályzat rendelkezései szerint történik.

Az infrastrukturális gyengeségek és hiányosságok kivédése érdekében az egyes rendszerek biztonsági osztályba sorolása után gondoskodni kell a megfelelő infrastruktúra biztosításáról. Ilyenek lehetnek:

- szünetmentes áramellátás,
- hőmérséklet- és páratartalom-szabályozó rendszer,

- beléptető rendszer stb.

A szervezet informatikai rendszeréhez nem a szervezeti infrastruktúrájához tartozó (pl. magántulajdonú) számítástechnikai, kommunikációs, multimédiás berendezést vagy adathordozót kapcsolni tilos! Amennyiben szervezeti érdekből szükséges ilyen eszköz használata, úgy az csak a szervezet vezetőjének vagy a rendszergazdának az engedélye alapján dokumentálási kötelezettség mellett végezhető el ***(„N11.1.3 Idegen adathordozó behozatali -használati engedély").*** A szervezet tulajdonában lévő vagy bérelt számítástechnikai berendezések behozatala, kivitele (javítás céljából, máshol történő használatra stb.) csak szervezeti céllal lehetséges, amelyet az IBF vagy a szervezet vezetője engedélyezhet ***(„N11.1.2 Adathordozó eszköz kiviteli engedély").*** Ezeket az eseteket dokumentálni kell. Nem kell alkalmanként dokumentálni a személyes használatra, név szerint, tartósan átadott eszközök mozgatását (pl. szervezeti laptopok, telefonok stb.) ***(„N11.1.1 Adathordozók nyilvántartása").*** A javítás céljából a szervezetből kikerülő eszközök esetében biztosítani kell, hogy a szervezet által kezelt adatok ne kerüljenek ki.

Olyan meghibásodott eszközök (PC, mobil eszköz, szerver stb.), amelyekben az adathordozók védendő adatokat tartalmazhatnak, nem kivihetők az adathordozó alkatrésszel. Ebben az esetben az adathordozót (merevlemez, statikus memória egység stb.) a javítás idejére cserealkatrésszel kell helyettesíteni, vagy ha nem szükséges ez az alkatrész a működéshez, akkor az eredeti adathordozó és cserealkatrész nélkül kell javítási célból kivinni a szervezetből. Az eredetileg használt adathordozót a javítás után vissza kell helyezni az eszközbe, vagy arról az adatokat az új eszközre át kell tenni. Amennyiben az eredeti adathordozó alkatrész nem kerül vissza az adott eszközbe, úgy az adathordozót a szabályzat „4.4 Adathordozók védelme" fejezetében meghatározottak szerint kell kezelni.

3.1.2. Fizikai belépés ellenőrzése, belépési engedélyek

A szervezet székhelyén négy biztonsági zóna van elkülönítve, amelyekhez különböző belépési szabályok tartoznak:

0. zóna

- Távoli rendszerek, felhők, amelyek üzemeltetése, védelme a szervezet által nem lehetséges és nem is a szervezet hatásköre.
- Szerződéses keretek között meg kell követelni az információbiztonsági megfelelőséget.

1. zóna:

- A bejutás ellenőrzötten lehetséges, látogató felügyelet nélkül tartózkodhat az adott területen.
- Informatikai eszköz nem lehet a zónában, amennyiben nyomtató található az adott területen, nyomtatás kizárólag jelszóval aktiválható módon történhet.
- A zónába tartozó helyiségek: folyosó, lépcsőház.

2. zóna:

- A bejutás kulccsal vagy beléptető rendszerrel lehetséges, látogató csak felügyelettel tartózkodhat a területen.
- Látogatói belépés kizárólag az ügyintéző jelenlétében történhet.
- A zónába tartozó helyiségek: iroda, tárgyaló.

3. zóna:

- A bejutás kulccsal vagy beléptető eszközzel, csak ideiglenesen, belépési naplót vezetve lehetséges.
- A kiemelt fontosságú informatikai eszközöket itt kell elhelyezni.

- Kizárólag az informatikus/rendszergazda tartózkodhat bent kíséret nélkül, minden más személy belépését dokumentálni és felügyelni kell.
- A zónába tartozó helyiségek: rendszergazdai iroda, szerver helyiség, irattár, anyakönyvi gép - dedikált gép működési környezete.

Belépési szabályok és jogosultságkezelés

A 2. és 3. zónába tartozó helyiségeket – amennyiben nem folyik bennük munkavégzés – kulcsra zárva kell tartani vagy elektronikus beléptetőrendszerrel kell védeni.

A helyiségek kulcsait elzárva kell tartani, és csak az arra jogosultaknak szabad kiadni az ***„N12.1.1 Belépésre jogosultak -nyilvántartása"*** kulcsfelvételi rend listáján szereplők részére a számukra írásban engedélyezett szobákra vonatkozóan. A kulcsok kiadását és visszavételét vagy manuálisan, vagy elektronikusan dokumentálni kell ***(„N12.1.3 Szerver helyiség belépés nyilvántartás").***

Új munkatársak belépési jogosultsága

Az új belépő munkatársak kulcsokat és/vagy kártyákat csak a belépést követő IT biztonsági oktatási terv és napló megtörténte és a titoktartási nyilatkozat ***(„N14.2.2 Titoktartási nyilatkozat")*** aláírása után kaphatnak.

A belépő munkatárs új belépési jogosultságait, illetve nem új belépő munkatárs belépési jogosultságainak változtatását az érintett terület vezetője határozza meg.

A meghatározás során a terület vezetője az ***„N08.1.3 Jogosultság kiadás -visszavonás nyilvántartás"*** formanyomtatványon összegzi az általa szükségesnek tartott belépési jogosultságokat, és azokat jóváhagyatja a szervezet vezetőjével.

Kulcsok és kódok kezelése

A jóváhagyott EIR jogosultságok nyilvántartása formanyomtatvány továbbításra kerül a kulcsok/azonosító kártyák/kódok kiosztásának felelőse felé.

Az illetékes személy felelőssége, hogy csak a vezetőség által jóváhagyott jogosultságokat állítsa be, illetve csak a megfelelő kulcsokat/kódokat adja ki.

Amennyiben felmerül a jóváhagyás hitelességének gyanúja, azt köteles a kulcskiadás előtt igazoltatni a vezetőség megkérdezésével.

A kulcsokat vagy kódokat évente cserélni kell, a jogosultságok és felülvizsgálatával együtt.

Szerverszoba-specifikus szabályok

A helyiség (szerverszoba) közelében nem üzemelhet tűz- és robbanásveszélyes raktár.

A helyiségben tűzjelző rendszert kell kiépíteni, amelynek üzembiztonságát az előírásoknak megfelelően időszakosan ellenőrizni kell.

A szerverhelyiségben biztosítani kell az automatikus tűzoltó képességet.

A szerverhelyiségben biztosítani kell az páratartalom szabályozásának képességét.

A szerverszobát mindig zárva kell tartani.

Munkaidőben csak az informatikai vezető), vagy az általa felhatalmazott informatikus/rendszergazda veheti fel a kulcsot; ezt minden esetben dokumentálni kell ***(„N12.1.3 Szerver helyiség belépés nyilvántartás").***

Munkaidőn kívül a kulcsokat elzártan kell tárolni.

Idegen személy felügyelet nélkül nem tartózkodhat a szerverszobában.

Elektronikus beléptetőrendszer

A belépések rögzíthetők elektronikus beléptetőrendszer használatával is. Ebben az esetben csak az informatikai vezető és az általa felhatalmazott informatikus/rendszergazdakártyája nyithatja az ajtót, illetve ők ismerhetik az ajtónyitó kódokat.

Belépési jogosultságok naprakészen tartása

A belépésre jogosultak listáját mindig naprakészen kell tartani ***(„N12.1.1 Belépésre jogosultak - nyilvántartása")***. Akinek a belépése már nem indokolt, azt el kell távolítani a listáról, és vissza kell vonni a belépési jogosultságot igazoló dokumentumait/eszközeit.

Látogatók kezelése

A látogatók (vendégek, ügyfelek) belépéseiről nyilvántartást kell vezetni ***(„N12.1.1 Belépésre jogosultak -nyilvántartása")*** amely tartalmazza:

- A látogató neve,
- hogy milyen ügyben érkezett
- és kihez érkezett.
- Látogatók csak kísérettel mozoghatnak a szervezet 2. és 3. zónába tartozó területein.
- Az adatvédelmi szabályoknak megfelelően a látogatói nyilvántartást egy hónap után meg kell semmisíteni.

Biztonsági intézkedések

A zónahatárokon biztonsági kamerát vagy elektronikus beléptetőrendszert kell üzemeltetni.

Az elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat legalább egy évig meg kell őrizni. Ha rendelkezésre álló információk alapján jogosulatlan belépés gyanúja merül fel, azonnal át kell vizsgálni a látogatói adatokkal kapcsolatos dokumentumokat vagy felvételeket.

3.2. Szervezeti és személyzeti szabályok

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás ***(„N14 Személyi biztonsági szabályzat")*** kiterjed a szervezet teljes személyi állományára, valamint minden olyan természetes személyre, aki a szervezet elektronikus információs rendszereivel kapcsolatba kerül vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszerrel tényleges vagy feltételezhető kapcsolatba kerülő személy nem a szervezet alkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötés során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.2.1. Felvételi eljárás során követendő szabályok, személyes követelmények

A szervezet meghatározza a felvételi eljárás során követendő szabályokat ***(„N14.2 Felvételi eljárásrend")***, valamint a munkakörökhöz kapcsolódó személyes követelményeket. A követelményeket a munkaköri leírásokban rögzíti, amelyek tartalmazzák:

- Az adott munkakörhöz szükséges információbiztonsági ismereteket.
- A titoktartási kötelezettségre vonatkozó előírásokat.
- Az informatikai rendszerekhez való hozzáférés feltételeit.

A felvételi eljárás során minden jelöltnek nyilatkoznia kell arról, hogy megismerte és elfogadja az információbiztonsági szabályzatot ***(„N14.2.1 EIR felhasználási szabályok elfogadó nyilatkozat").***

3.2.2. Képzési eljárásrend

A felhasználói állományt az informatikai biztonság megvalósítása érdekében munkakörüknek megfelelően képezni kell, a fejlesztői és üzemeltetői állománynak pedig folyamatosan szinten kell tartania és fejlesztenie kell az informatikával és információbiztonsággal kapcsolatos ismereteit. A felhasználói személyi állományt új rendszerek bevezetésekor szintén képezni kell. Az újonnan alkalmazott felhasználót – vezetője kérésére – soron kívül kell oktatni a rendszer használatáról *az „N03 Képzési szabályzat"* és *„N03.2 Képzési eljárásrend"-ben* meghatározottak szerint.

Éves oktatási terv

A követelmények és a ténylegesen rendelkezésre álló erőforrások összevetése alapján évente oktatási terv készül ***(" N03.3 Információ Biztonsági oktatás terv és napló „),*** amely tartalmazza:

- A szükséges oktatásban résztvevők körét.
- Az oktatás/képzés témaköreit és követelményeit.
- A minőségi, környezeti, munkahelyi egészségvédelmi és biztonsági, valamint információbiztonsági célok kapcsán megfogalmazott jövőbeni elvárt kompetenciákat.

Továbbképzési igények figyelembevétele

A szervezet nyitott a munkatársak egyéni teljesítményét javító igényekre, ezért – eseti elbírálás alapján – figyelembe veszi a vezetők és beosztottak saját továbbképzési igényeit is, amennyiben azok összhangban vannak a szervezet hosszú távú stratégiájával.

Oktatás és szabályzatismertetés

Az oktatás mellett a teljes felhasználói állománnyal ismertetni kell az IBSZ rájuk vonatkozó előírásait ***(„N03.1 Információ Biztonsági Felhasználói Szabályzat").*** A felhasználók nyilatkozatot adnak arról, hogy az ismertetés megtörtént, a szabályzatban foglaltakat megértették és azokat maradéktalanul betartják Nyilatkozat az IT biztonsági szabályok elfogadásáról.

3.2.3. Biztonságtudatosság képzés

A szervezet annak érdekében, hogy az érintett felhasználók felkészülhessenek a lehetséges belső és külső fenyegetések felismerésére, rendszeres tudatossági képzést nyújt a Személybiztonsági eljárásrend szerint. A képzés célja, hogy az elektronikus információs rendszer felhasználói megismerjék és alkalmazzák az alapvető biztonsági követelményeket.

A képzés időpontjai és helyzetei

A biztonságtudatossági képzés az alábbi esetekben kötelező:

Új felhasználók kezdeti képzése: Az új felhasználók számára az IT biztonsági oktatás részeként, a belépést követően IT biztonsági oktatási terv és napló.

Szerepkör vagy felelősség változásakor: Amikor egy felhasználó új szerepkörbe vagy felelősségi körbe kerül.

- Rendszerváltozás esetén: Amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi a felhasználók újra oktatását.

- Éves ismeret-felfrissítés: Legalább évente egyszer minden felhasználó számára kötelező informatikai és IT-biztonsági képzés.

A képzés tartalma

A tudatossági képzés során az alábbi témakörökre kell fókuszálni:

Alapvető biztonsági követelmények:

- Jelszókezelés szabályai.
- Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának alapelvei.
- A munkaállomások és eszközök biztonságos használata.

Fenyegetések felismerése:

- Adathalász támadások (phishing) elleni védekezés.
- Kártékony kódok (vírusok, malware) felismerése és elkerülése.
- Gyanús e-mailek és linkek kezelése.

Rendszerhasználati szabályok:

- Hozzáférési jogosultságok betartása.
- Adatok helyes tárolása és továbbítása.

Belső fenyegetések kezelése:

- Illetéktelen hozzáférések jelentése.
- Szabálytalan viselkedés felismerése a munkahelyen.

Képzési módszerek

- **Előadások és workshopok:** Az alapvető ismeretek átadása interaktív módon.
- **E-learning modulok:** Online tananyagok biztosítása a rugalmas tanulás érdekében.

Gyakorlati szimulációk: adathalász támadások szimulálása a felhasználói reakcióinak tesztelésére.

Nyilatkozat a képzésről

A képzés végén minden résztvevő köteles nyilatkozni arról, hogy:

- Az oktatás során ismertetett szabályokat megértette.
- Azokat maradéktalanul betartja. ***„N14.2.1 EIR felhasználási szabályok elfogadó nyilatkozat"***

3.2.4. Fegyelmi intézkedések

A biztonsági előírásokat megsértőkkel szemben fegyelmi eljárás indulhat. Az eljárás célja a szabályszegés körülményeinek feltárása, a felelősség megállapítása és szükség esetén szankciók alkalmazása. A fegyelmi eljárást az érintett felhasználó közvetlen vezetője, az IBF (Információbiztonságért Felelős személy), illetve a szervezet vezetője kezdeményezheti írásban.

A kezdeményezés tartalma

A fegyelmi eljárás kezdeményezésének tartalmaznia kell:

- A fegyelmi eljárást kezdeményező nevét és beosztását.
- A valószínűsíthető fegyelmi vétséget elkövető (érintett) nevét és beosztását.
- Az észlelés idejét és módját.

- A fegyelmi vétség elkövetésének idejét, módját és körülményeit.
- A keletkező károk és egyéb következmények kifejtését.
- A kezdeményezés idejét.

Az eljárás menete

A szervezet vezetője a kezdeményezést elbírálja, melyről értesítést küld a kezdeményezőnek és az IBF-nek. A vezető kitűzi a fegyelmi eljárás feltáró megbeszélésének időpontját, és meghatározza az azon résztvevő személyek körét.

Az eljárás szakaszai:

Feltáró megbeszélés:

- A megbeszélésen jelen van:
- A szervezet vezetője.
- Az eljárást kezdeményező személy.
- Az érintett személy.
- Az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó.
- Az eseményben érintett egyéb személyek.
- Azok, akiket erre a megbeszélésre a szervezet vezetője meghívott.
- A feltáró megbeszélést a szervezet vezetője vezeti.

A megbeszélés során:

- Az eljárást kezdeményező ismerteti az általa tapasztalt vélhető fegyelmi vétséget, bemutatja az eseményről begyűjtött bizonyítékokat, és megnevezi az érintetteket.
- Az érintett személy reagálhat az ismertetett információkra, megnevezve azon pontokat, amelyekkel egyetért vagy nem ért egyet.
- Jegyzőkönyv készül, amely tartalmazza:
    - A fegyelmi eljárás hivatkozási számát.
    - Az eljáráson jelenlévőket.
    - Az eljárás lefolytatásának idejét és helyét.
    - Az elhangzottakat, meghivatkozva a személyeket.

Adatgyűjtés és adatértékelés:

Amennyiben szükséges, további adatok begyűjtése történik tisztázatlan körülmények tisztázása érdekében.

Záró megbeszélés:

- Résztvevők:
- A szervezet vezetője.
- Az eljárást kezdeményező személy.
- Az érintett személy.
- Az IBF, amennyiben biztonságot érintő fegyelmi vétségről van szó.
- Azok, akiket erre a megbeszélésre a szervezet vezetője meghívott.

- Jegyzőkönyv készül, amely tartalmazza:
    - A fegyelmi eljárás hivatkozási számát.
    - Az eljáráson jelenlévőket.
    - Az eljárás lefolytatásának idejét és helyét.
    - A szervezet vezetőjének állásfoglalását.

Döntéshozatal

A rendelkezésre álló adatok alapján a szervezet vezetője döntést hoz arról, hogy:

- Megvalósult-e a fegyelmi vétség, ha igen, milyen formában nyilvánult meg.
- Kik érintettek a vétségben és milyen mértékben felelősek annak megvalósulásában.
- Milyen szankciókat kell alkalmazni (pl. figyelmeztetés, jogosultságok visszavonása).
- Szükséges-e büntetőjogi lépések megtétele.

Fegyelmi intézkedések érvényesítése

Az érvényesítés során:

- Meghatározzák a szükséges teendőket, kijelölik azok végrehajtásának felelőseit és határidejét.
- Ezen feladatokat rögzítik a jegyzőkönyvben

Nem alkalmazotti jogviszony esetén

Amennyiben az elektronikus információbiztonsági szabályokat nem a szervezet személyi állományába tartozó személy sérti meg:

- Érvényesíteni kell a vonatkozó szerződésben meghatározott következményeket.
- Meg kell vizsgálni az egyéb jogi lépések lehetőségét.
- Szükség szerint új eljárások kerülnek bevezetésre.

3.2.5. Eljárás a jogviszony megszűnésekor

Feladatok a jogviszony megszűnése előtt

A felhasználójogviszonyának megszűnése esetén a felhasználófelettes vezetője gondoskodik arról, hogy a kilépő munkavállaló elektronikus információs rendszerrel vagy annak biztonságával kapcsolatos feladatait a jogviszony megszűnését megelőzően teljesítse. Ez magában foglalja:

- A folyamatban lévő munkák lezárását vagy átadását.
- Az elektronikus információs rendszerekhez való hozzáférések megszüntetésének előkészítését.

Feladatok a jogviszony megszűnésekor

A jogviszonyt megszüntető személy gondoskodik arról, hogy a kilépő felhasználó ne sérthesse meg az elektronikus információbiztonsági szabályokat, különös tekintettel:

- **Hozzáférések megszüntetése:** Az összes hozzáférési jogosultságot törölni kell az elektronikus információs rendszerekből.

Jogosultságok visszavonása: A kilépő felhasználóhoz rendelt jogosultságokat vissza kell vonni.

- **Informatikai eszközök visszavétele:** az informatikai eszközök visszavételét és ellenőrzést dokumentálni kell.

A fentiekben meghatározottakon túlmenően a részletes eljárásokat az ***„N14.4 Eljárásrend munkaviszony -jogviszony megszűnése esetén"*** szabályozza.

Informatikai eszközök visszavétele

A szervezet ellenőrzi, hogy a kilépő felhasználó személyes használatában található-e informatikai eszköz, és gondoskodik ezek visszavételéről ***(„N14.4.1 Jogosultságok visszavonása, informatikai eszközök visszavétele")***

Az ellenőrzés során:

- Azonosítani kell az összes eszközt, amelyet a kilépő használt.
- Gondoskodni kell az eszközök fizikai visszaszolgáltatásáról és állapotuk dokumentálásáról.
- Az üzemeltető rendszergazda, vagy csoportnak ellenőriznie kell és szükség szerint törölnie kell az informatikai eszközön, vagy azok szolgáltatásaiban megtalálható személyes adatokat vagy nem publikus hozzáférési adatokat.

Elszámolás és tájékoztatás

- A szervezet igazolja a kilépő számára, hogy minden hozzáférési jog törlésre került és hogy a felhasználó elszámolt az összes eszközzel és adatokkal kapcsolatban.
- A kilépőt tájékoztatni kell az esetleg rá vonatkozó, jogi úton is kikényszeríthető kötelezettségekről, amelyek a jogviszony megszűnését követően is fennállnak (pl. titoktartási kötelezettség).

Hozzáférés fenntartása és személyes adatok kezelése

- A szervezet meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt elektronikus információs rendszerekhez és szervezeti információkhoz.

A kilépő felhasználó számára lehetőséget kell biztosítani arra, hogy ellenőrzött keretek között menthesse vagy törölhesse személyes jellegű adatait (pl. levelezések). Kiemelt figyelmet kell fordítani arra, hogy ez ne sértse az adatbiztonsági szabályokat.

Magáncélú adatok kezelése

Mivel a vonatkozó törvényi szabályozások és a jelen szabályzat egyértelműen megfogalmazza, hogy:

- A felhasználók nem használhatják magáncélra a szervezet informatikai rendszereit.
- Nem tárolhatnak magán adatokat munkaállomásokon vagy hivatalos levelezőfiókokban.

Amennyiben mégis ilyen személyes jellegű adatok kezelésére vonatkozó kérés merül fel, az jogsértő magatartás vélelmezésére adhat okot. A jogsértés tényének megállapításától függetlenül az üzemeltető rendszergazda, vagy csoport kötelessége, hogy az ilyen jellegű személyes adatokat haladéktalanul törölje az informatikai eszközről, eszközökről.

3.3. Azonosítás és hitelesítés

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, valamint nyomon követi a felhasználók által végzett tevékenységeket. Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött – úgynevezett privilegizált – felhasználói fiókokhoz való **hálózat**on keresztüli hozzáféréshez.

3.3.1. Azonosítási és hitelesítési eljárásrend

A szervezetben alkalmazott informatikai rendszerekben kötelező a felhasználói azonosítás és hitelesítés alkalmazása a jogosulatlan személyek tevékenységének megakadályozása és az

elszámoltathatóság biztosítása érdekében, az ***(„N08 Azonosítási és hitelesítési szabályzat")*** előírásainak megfelelően.

Az azonosítási és hitelesítési folyamat alapelvei

- **Azonosítás:** A felhasználó megadja azonosságát a rendszer felé, amelyet egyedi felhasználói azonosítóval végez.
- **Hitelesítés:** A felhasználó állítólagos azonosságának bizonyítására szolgál, amelyhez legalább tudás alapú (jelszavas) hitelesítés kell alkalmazni.
- **Adatvédelem:** Az **azonosítási** és hitelesítési adatokhoz való hozzáférést korlátozni kell a jogosulatlan megismerés, módosítás és törlés ellen.

Általános szabályok

- A szervezet kijelölt informatikus/rendszergazda gondoskodik arról, hogy minden felhasználói azonosító valós, engedélyezett felhasználóhoz tartozzon.
- A rendszergazdák számára külön azonosítót kell létrehozni adminisztratív és felhasználói feladatok ellátására. Az adminisztrátori azonosítót kizárólag rendszergazdai feladatokra szabad használni.
- Az új felhasználókat be kell vezetni a rendszerbe, míg a távozók jogait haladéktalanul vissza kell vonni.
- A hitelesítő eszközöket személyre szólóan kell kiadni és nyilvántartani. Ezek kezeléséért, használatáért és tárolásáért a felhasználók felelnek.
- Más felhasználók azonosítóinak használata tilos!
- A jelszavaknak legalább 10 karakter hosszúnak kell lenniük, tartalmazniuk kell számokat, kis- és nagybetűket és speciális karaktereket.
- Nem lehet szótári szó vagy egyszerű sorozat (pl. "1234567891011"; ABCDEF; qwertz).
- A jelszavakat legalább háromhavonta meg kell változtatni.
- Jelszóváltáskor nem lehet újra használni az utolsó három jelszót (jelszó-história).
- A jelszavakat tilos másnak átadni vagy leírni.

További követelmények

Munkaállomások használata:

- Többfelhasználós munkaállomások esetén minden munkamenet után ki kell jelentkezni.
- Egyéni munkaállomás időleges elhagyásakor gondoskodni kell a védelemről (pl. képernyő zárolása).

Megosztott fiókok kezelése:

- Megosztott vagy csoportfiókok esetén a felhasználók változása esetén a hozzáféréseket vissza kell vonni és újra generálni.

Távollét esetén hozzáférés biztosítása:

- Csak az IBF engedélyével történhet, dokumentált módon:
- Jelszó módosítása rendszergazda által.
- Engedélyezett feladat végrehajtása után a jelszó visszaállítása.

Sikertelen belépések kezelése

- Sikertelen bejelentkezési kísérletek meghatározott számának túllépése esetén a rendszer automatikusan zárolja a fiókot meghatározott időre.

Felhasználói felelősség

A felhasználóknak kötelességük:

- Az IBSZ előírásainak betartása.
- Jelszavaik bizalmas kezelése.
- Minden gyanús esemény vagy jogosulatlan hozzáférés kísérlet jelentése.

Többtényezős hitelesítés

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz minden privilegizált fiókhoz való hálózati hozzáférés esetén.

Ez magában foglalja:

- Tudás alapú (jelszó) hitelesítést.
- Tulajdon alapú hitelesítést (pl. token vagy mobilalkalmazás).
- Biometrikus adatok használatát, amennyiben technológiailag lehetséges.

Hozzáférések naplózása

Minden hozzáférési eseményt naplózni kell, beleértve:

- Sikeres és sikertelen belépéseket.
- Privilegizált fiókok használatát. A naplózott adatokat legalább 1 évig meg kell őrizni, védve a jogosulatlan hozzáférés ellen.

Adminisztrátori jelszavak tárolása

A rendszergazdai és bizonyos rendszereknél használt visszaállítási jelszavakat titkosított formában kell tárolni:

Redundánsan két külön adathordozón, megfelelő titkosítású jelszótároló programban rögzíteni.

A tárolt adatokat lezárt borítékban kell elhelyezni biztonsági szekrényben, amelyhez csak jogosult személyek férhetnek hozzá.

3.3.2. Azonosításra, hitelesítésre szolgáló eszközök kezelése

Az azonosításra, hitelesítésre szolgáló eszközök kiadása előtt az azt végző munkatárs vagy szervezet:

- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát (pl. kezdeti jelszó), melyet az adott rendszer telepítése során a végfelhasználónak meg kell változtatni;
- kiosztáskor ellenőrzi az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát, illetve biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- a hitelesítésre szolgáló eszköztípusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, kompromittálódott vagy a sérült eszközöket;
- megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

- megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;
- lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

Sikertelen belépés esetén a szervezet által meghatározott esetszámkorlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszámkorlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

A felhasználói azonosítók/jelszavak elvesztését/elfelejtését, illetve vélelmezett kompromittálódását azonnal jelezni kell a szervezet vezetője vagy az IBF felé. Elfelejtett jelszó esetében a rendszergazda új kezdeti jelszót állít be, amelyet az első bejelentkezéskor meg kell változtatni. Azonosító kompromittálódása esetén a kompromittált azonosítóhoz tartozó jogokat azonnal le kell tiltani és ki kell vizsgálni, hogy történt-e jogosulatlan hozzáférés az informatikai rendszerhez. Az IBF engedélyével a rendszergazda a kompromittálódott azonosító helyett az érintett felhasználónak a munkájához szükséges másik azonosítót biztosít.

A szerepköröknek megfelelő, leginkább az üzemeltetéshez köthető rendszergazdai és bizonyos rendszereknél a rendszer-visszaállítási jelszavakat tárolni kell a következő módon:

- Minden ilyen jogosultsági adatot (rendszer neve, hozzáférés módja, felhasználónév, jelszó) redundánsan, két darab külön adathordozóra mentve, megfelelő titkosítású jelszótárolóban rögzítetten, szerepkörönként külön adatbázisban, melynek mesterkulcsát (jelszavát) az adathordozó mellett, szerepkörönként lezárt, lepecsételt és legalább két jogosult személy által aláírt borítékban kell tárolni.
- A borítékba az adatokat úgy kell elhelyezni, hogy azok ne legyenek „átvilágíthatók", felbontás nélkül ne legyenek olvashatók. A borítékokra kívül rá kell írni az utolsó módosítás dátumát és a megbontás okát (pl. audit vagy jogosult távolléte miatti vezetői bontás), ilyen eseteket követően a szerepköri jogosultaknak célszerű a jelszavakat lecserélni.
- A jelszótárolóban a korábbi jelszavak a History alatt, időmegjelöléssel megtalálhatók. A változtatást végző jogosult köteles a hasonló szerepkörűeknek jelezni a változtatás tényét, adattartalmát. Ha a szerepkörhöz rendelt jogosult végez szabályzatban előírt kötelező jelszóváltást a tárolt adatokban, akkor nincs szükség borítékbontásra.
- A borítékot zárt biztonsági szekrényben kell tárolni az illetéktelen hozzáférés elkerülése érdekében.

3.3.3. Szervezeten kívüli felhasználók azonosítása és hitelesítése

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezeten kívüli felhasználókat és tevékenységeiket.

Tanúsítványok elfogadása

- Az elektronikus információs rendszer kizárólag a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el.

Hitelesség biztosítása

A szervezeten kívüli felhasználók számára biztosítani kell:

- Egyedi azonosítókat.

- Megbízható tanúsítvány-alapú hitelesítést.
- A rendszereknek naplózniuk kell minden hozzáférési eseményt (sikeres vagy sikertelen belépések).

3.4. Hozzáférés védelem, jogosultság kezelés

3.4.1. Hozzáférés ellenőrzési eljárásrend

A szervezet minden informatikai rendszerében, erőforrásaival és szolgáltatásaival kapcsolatban, az adott eszköz, erőforrás, adat, dokumentumtár stb. biztonsági osztályától függően, a „szükséges és elégséges ismeret elvének" betartásával kell alkalmazni a hozzáférés-védelmi és jogosultságkezelési intézkedéseket. Minden, az IBSZ hatálya alá eső adatot a központi informatikai rendszerben, a központi logikai és fizikai rendszerek védelme alatt, központi hozzáférés-védelmi és jogosultságkezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával. A hozzáférés-védelmi követelmények a szervezet informatikai rendszereiben alkalmazandó rendszertől függenek, amelyeket az ***„N08 Azonosítási és hitelesítési szabályzat"*** részletesen szabályoz.

Általános szabályok

- Az információkhoz való hozzáférési lehetőséget (jogosultságot) a felhasználó által betöltött munkakör (szerepkör) alapján kell meghatározni (szerepkör-alapú hozzáférés). A szerepkörök definiálása a szervezet munkafolyamatain, szervezeti struktúráján, valamint hierarchikus és funkcionális kapcsolatokon alapul.
- A hozzáférések biztosítása során érvényesíteni kell a minimális jogosultság elvét, amely szerint minden felhasználó csak azokat az erőforrásokat érheti el, amelyek munkájához feltétlenül szükségesek.
- A hozzáférések meghatározásánál figyelembe kell venni AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) rendelkezéseit is.

Hozzáférések engedélyezése

A szervezetbe újonnan belépő felhasználók informatikai rendszerhez történő hozzáférését az erre szolgáló igénylőlapon ***(„N02.1.1 Fiók igénylő lap")*** az érintett szervezeti egység vezetője kezdeményezi.

- A felhasználói hozzáférést és az indokoltan kért jogosultságokat a szervezet vezetőjének engedélye után a rendszergazda adja meg.
- A szolgáltatások (pl. megosztott könyvtárak) esetén a szolgáltatás indítását engedélyező dokumentumban meg kell jelölni:
- A szolgáltatásért felelős vezetőt.
- A szolgáltatás tulajdonosát.
- A szolgáltatás tulajdonosa által definiált hozzáférés-védelem elve szerint kell kialakítani a jogosultsági kört.

Hozzáférések technikai korlátozása

- A munkaállomásokon és szervergépeken technikailag is korlátozni kell az alternatív bootolási lehetőségeket (pl. DVD, USB, Ethernet). Ezeket az eszközöket csak karbantartási és javítási célból lehet olyan rendszerrel működtetni, amely nem az üzemszerűen rátelepített operációs rendszer.

- A munkaállomásokon és szervereken telepített szoftver/program esetében kiemelt figyelmet kell fordítani az automatikusan létrejövő felhasználókra (pl. administrator, guest). Ezek kezdeti jelszavát azonnal meg kell változtatni vagy zárolni kell használatukat.

Jogosultságok felülvizsgálata

- Az informatikai rendszerhez történő hozzáférési engedélyeket évente felül kell vizsgálni (pl. távoli hozzáférések, internetelérés).
- Az esetlegesen már nem indokolt jogosultságokat meg kell szüntetni.

Felhasználói szerepkör változás kezelése

- A felhasználó szerepkörének megváltozása esetén (pl. más osztályra kerül) a régi szerepkörhöz tartozó jogosultságokat vissza kell vonni, majd az új szerepkörnek megfelelő jogosultságokat megadni.

Jogviszony megszűnése esetén

- A kilépő felhasználó vezetője intézkedik a hozzáférési jogok törléséről.
- Az informatikus/rendszergazda az írásban beérkező igényt -hozzáférési jog visszavonását végrehajtja és dokumentálja.

Az elszámolást dokumentálni kell ***„N14.4.1 Jogosultságok visszavonása, informatikai eszközök visszavétele".***

Hozzáférési események naplózása

- Minden hozzáférési eseményt (sikeres/sikertelen belépések) naplózni kell.
- A naplókat legalább 1 évig meg kell őrizni. (Jogszabály ennél hosszabb megőrzési időt [3] is előírhat.)

3.4.2. A felhasználói fiókok kezelése

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságokat nem kaphatnak.

Kivételt képeznek e szabály alól azon alkalmazások munkaállomásai, ahol a szoftver/program működéséhez szükségesek az emelt szintű jogok. Ilyen esetekben a zavartalan munkavégzés érdekében ez engedélyezett, de az így rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra (pl. szoftver/program telepítése, leállítása stb.), csak és kizárólag a szakalkalmazás használata miatt birtokolhatja ezeket.

Hálózati szolgáltatások korlátozása

- A munkaállomásokon a felhasználóknak tilos hálózati szolgáltatásként mappákat vagy fájlokat megosztani.
- Amennyiben a megosztás szakmailag indokolt, úgy azt a közvetlen vezető kezdeményezésére, az IBF jóváhagyásával a munkaállomás adminisztrátora hozza létre.
- Valamennyi megosztás esetén szigorúan kell meghatározni a hozzáféréseket, és törekedni kell arra, hogy ne legyenek általános megosztások. Csak azok a felhasználók és munkaállomások kaphatnak jogot az erőforrások elérésére, amelyeknek ez munkájukhoz valóban szükséges.

Hálózati csatlakozás és jogosultságok

[3] a naplóállományok megőrzési idejét az adott rendszerben tárolt adatok esetleges sérülésének, az ebből következő kárhatás – beleértve egy esetleges a jogi eljárás lefolytatásnak követelményeit figyelembe véve szükséges megállapítani.

- A szervezet minden irodájában biztosítani kell a zárt hálózati csatlakozás lehetőségét.
- A hálózati erőforrásokhoz való hozzáférést különböző szintű hálózat jogosultságok biztosítják. Ezek az alábbi tevékenységek elvégzését tehetik lehetővé:
- **Hálózat** kezeléséhez szükséges szoftver/programok közös használata.
- Közös nyomtatók használata.
- Internet böngészés.
- Elektronikus levelezés.
- Adatbázisok elérésének biztosítása.
- Alkalmazások és adatok elérésének biztosítása.

Hálózaton található fájlokra és könyvtárakra kioszthatő jogosultságok

- Olvasási jog.
- Írási (módosítási, létrehozási) jog.
- Törlési jog.

Szoftveres védelmi eljárások korlátozása

A szervezeti informatikai rendszerben az egyes számítástechnikai rendszerek, szoftverek készítői által gyárilag biztosított védelmi eljárásokat (pl. Microsoft Word jelszavas védelme) a felhasználók – a szervezeti adatok rendelkezésre állásának biztosítása érdekében – nem használhatják!

Ettől eltérni csak a szervezet vezetőjének írásos utasítására vagy felhasználói kezdeményezés esetén, írásos engedéllyel szabad. Az eltérést dokumentálni kell, beleértve az eljárás okát és célját is. A titkosító kódot vagy jelszót lezárt borítékban át kell adni a szervezet vezetőjének.

Tiltott tevékenységek

- Tilos nem engedélyezett erőforrások, szolgáltatások vagy jogosultságok megszerzése vagy ennek kísérlete.
- Tilos más felhasználók munkájának zavarása, állományaikhoz történő bármilyen illetéktelen hozzáférés vagy annak kísérlete.

Naplózás és ellenőrzés

A hozzáférésvédelmi és jogosultságkezelési elemek adminisztrálása érdekében a felhasználói hozzáféréseket megvalósító rendszerek működtetését (ahol technológiailag lehetséges) naplózni[4] kell.

A naplótartalmat rendszeresen ellenőrizni kell az engedélyezett jogosultság-igénylések alapján.

Felhasználói fiókok kezelése és felülvizsgálata

- A munkaállomás adminisztrátorát értesíteni kell, ha:
- A felhasználói fiókokra már nincs szükség.
- A felhasználók kiléptek vagy áthelyezésre kerültek.
- Az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.
- A felhasználói fiókokat legalább évente felül kell vizsgálni.

---

[4] naplóállományokat olyan formában szükséges megőrizni, hogy azok egy esetleges peres eljárásban bizonyítékként felhasználhatóak legyenek. A Mentési- és archiválási eljárásrendben az adott rendszer adatainak mentéséhez a rendszer naplóállományainak mentéséről/archiválásáról is gondoskodni/rendelkezni szükséges.

A szervezet további feladatai

- Meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait.
- Kijelöli a felhasználói fiókok fiókkezelőit.
- Kialakítja a csoport- és szerepkör tagsági feltételeket.
- Meghatározza az elektronikus információs rendszer jogosult felhasználóit, valamint a csoport- és szerepkör tagságot.

3.4.3. Külső rendszerekből történő hozzáférés szabályozása

A szervezet az alábbi szabályokat és intézkedéseket alkalmazza a külső rendszerekből történő hozzáférések biztonságos szabályozására:

Felhasználói feladatok és kötelezettségek

A szervezet meghatározza és dokumentálja felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

- A külső rendszerekhez való hozzáférés során a felhasználóknak kötelességük:
- Az IBSZ előírásainak betartása.
- A jogosultságok kizárólag munkavégzés céljára történő használata.
- Az esetleges biztonsági események azonnali jelentése az IBF-nek.

Külső szolgáltatók ellenőrzése

- A szervezet külső és belső ellenőrzési eszközökkel biztosítja, hogy a külső elektronikus információs rendszer szolgáltatója megfelel az elvárt védelmi intézkedéseknek.
- A külső szolgáltatókat további minősítése szükségese, valamint meg kell határozni az adott külső szolgáltatás prioritását a hálózaton belül, és vagy a kötelező adatszolgáltatások teljesítése tekintetében.
- A külső szolgáltatások minősítését az üzemeltetői rendszergazdának, vagy az üzemeltető informatikai csoportnak kell elvégeznie és dokumentálnia.
- A Külső szolgáltatók számára biztosított, kiadott hozzáféréseket dokumentálni kell a külső felhasználók nyilvántartásában minden kiadás esetén.
- A hozzáférést azonnal vissza kell vonni, amennyiben a külső szolgáltató a szolgáltatáshoz kapcsolódó feladatait elvégezte, vagy a szolgáltatás tekintetében már nincs szükség a kiadott hozzáférésre.

Távoli hozzáférések kezelése

Külső cégek távoli hozzáférése:

- Külső cégek megbízott munkatársai állandó távoli hozzáférést kaphatnak az általuk felügyelt rendszerhez, például szerverek és szakalkalmazások karbantartása céljából.
- Ezeket a hozzáféréseket a cégeknek az IBSZ betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük.
- Külső felhasználók részére hozzáférések kiadása esetén, különös figyelmet kell fordítani a AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) rendelkezéseit is.

Szervezeti munkatársak távoli hozzáférése:

- Távoli hozzáférést kaphatnak azok a munkatársak, akik a szervezet által biztosított, távoli munkavégzésre alkalmas eszközzel rendelkeznek.

Az azonosítókat és jogosultságokat dokumentáltan kell kiadni ***(„N14.3.1 Külső felhasználók nyilvántartása")*** az azonosítóért felelős személy pontos meghatározásával. Az azonosítóért felelős személy ezt aláírásával igazolja.

Távoli gépek biztonsága:

- A távoli hozzáférésű munkaállomások biztonságáért minden esetben a távoli gép felhasználója és/vagy üzemeltetője felelős.
- A felhasználó felelőssége kiterjed a távoli gépről végrehajtott cselekményekre is.

Titkosított kapcsolatok használata:

- A szervezet informatikai infrastruktúrájához való távoli elérés kizárólag titkosított kapcsolaton (pl. VPN) keresztül történhet.
- A rendszerhez való csatlakozás csak a szükséges időre korlátozódhat; a munka végeztével a kapcsolatot bontani kell.

Biztonsági követelmények

Hozzáférési események naplózása:

- Minden külső hozzáférési eseményt (sikeres/sikertelen belépések) naplózni kell.
- A naplókat legalább 1 évig meg kell őrizni.

Többtényezős hitelesítés alkalmazása:

- Kötelező többtényezős hitelesítést alkalmazni minden privilegizált fiókhoz való hálózati hozzáférés esetén.

Távoli kapcsolatok időbeli korlátozása:

- A távoli kapcsolatok időtartamát minimalizálni kell; a kapcsolatot munka végeztével bontani szükséges.

Külső rendszerekkel való kapcsolódás szabályozása:

- Az elektronikus információs rendszer külső rendszerekkel való kapcsolódását dokumentálni kell, beleértve:
- Az interfészek paramétereit.
- A biztonsági követelményeket.
- Az átvitt adatok típusát.

3.4.4. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

A számítógépes munkahely kialakítását követően a számítógépen felhasználók azonosítására, valamint a jogosultságok meghatározására van szükség. A számítógép használatakor egyedi azonosítókat kell alkalmazni, melyek hiányában a munkaállomásra a belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

Engedélyezett tevékenységek az **azonosítás** és hitelesítés előtt:

3.4.4.1. Nyilvánosan elérhető tartalom

- Nyilvánosan hozzáférhető rendszerként definiálja a szervezet a publikus weboldalát.
- Az oldal üzemeltetéséért felelős szervezeti egység vezetőjének gondoskodnia kell:
- Az ott publikált információk törvényi megfelelőségéről és valódiságáról.
- Az információk sértetlenségéről.
- Tilos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni.
- A publikus weboldalt gondosan szegmentálni kell a szervezet belső hálózatától arra alkalmas eszközzel.

3.4.4.2. Rendszerhasználat jelzése

A rendszerhez való hozzáférés előtt figyelmeztető üzenetet vagy jelzést kell biztosítani, amely tájékoztatja a felhasználót arról, hogy:

- Az érintett szervezet elektronikus információs rendszerét használja.
- A rendszer használatot figyelhetik, rögzíthetik és naplózhatják.
- A rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással járhat.

Az elektronikus információs rendszer a figyelmeztető üzenetet mindaddig megjeleníti, amíg a felhasználó közvetlen műveletet nem végez a rendszerbe való belépéshez.

Nyilvánosan elérhető rendszerek esetén:

- Kijelzi a rendszer használatának feltételeit, mielőtt további hozzáférést biztosít.
- Tájékoztatást nyújt arról, hogy felügyelet, adatrögzítés vagy naplózás történik, amely megfelel az adatvédelmi szabályoknak.

Vezeték nélküli hozzáférés esetén

- A szervezet belső szabályozásában felhasználási korlátozásokat és technikai útmutatókat ad ki vezeték nélküli technológiák kapcsán.
- Engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Mobil eszközök hozzáférésének ellenőrzése

- A szervezet szabályozza és engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel történő kapcsolódást.
- Felhasználási korlátozásokat és konfigurálási követelményeket határoz meg.

3.4.4.3. Biztonsági követelmények

Hozzáférési események naplózása

- Minden hozzáférési eseményt (pl. sikertelen belépések) naplózni kell.
- A naplókat legalább 1 évig meg kell őrizni.

Többtényezős hitelesítés privilegizált fiókokhoz

- Kötelező többtényezős hitelesítést alkalmazni minden privilegizált fiókhoz való hálózati hozzáférés esetén.

Távoli kapcsolatok időbeli korlátozása

- A távoli kapcsolatok időtartamát minimalizálni kell; a kapcsolatot munka végeztével bontani szükséges.

Adatvédelmi megfelelőség biztosítása

- Az adatvédelmi szabályoknak megfelelően minden nyilvánosan elérhető rendszernek biztosítania kell, hogy az engedélyezett felhasználók kizárólag az előírt módon férjenek hozzá az adatokhoz.

3.5. Viselkedési szabályok az interneten

A szervezet e-mail és internet használati jogokkal rendelkező felhasználói kizárólag a munkájukkal kapcsolatban használhatják a szervezet által biztosított internetszolgáltatást. Az internethasználat során az alábbi szabályokat kell betartani:

3.5.1. Általános szabályok

Internetkapcsolat létesítése

- A belső hálózaton internetkapcsolatot kizárólag tűzfalon keresztül lehet létesíteni.
- Nem megengedett a szervezet informatikai hálózatába kapcsolt hordozható és asztali munkaállomásokról modemes, mobiltelefonos vagy egyéb nem szervezeti kapcsolat létrehozása internet-szolgáltatókkal.

Magáncélú használat tilalma

- Az internet szolgáltatás magáncélú használata nem engedélyezett.

Tartalomszűrés

- Az internetforgalom automatikusan, szoftveres alapon szűrésre kerül, így bizonyos tartalmak nem látogathatók, és technológiai eszközökkel tiltásra kerülnek.

3.5.2. Felhasználói kötelezettségek

- Az interneten csak a szervezeti munkával kapcsolatos oldalakat lehet látogatni.
- Tilos pornográf, online játék, fogadási, csevegő, letöltő és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása, ezekről letölteni, publikálni vagy adatokat cserélni.

3.5.3. Szoftver/programok letöltése és használata

- Az internetről a felhasználók számra szoftver/programok letöltése, telepítése és futtatása tilos!
- Igény esetén az informatikus/rendszergazda előzetes bevizsgálás után telepíti a szoftver/programot.
- A bevizsgálás során ellenőrizni kell:
- A programvírusmentességét.
- A program kompatibilitását az adott környezettel.
- A szerzői jogok betartását.

3.5.4. Csevegő programok használata

Információbiztonsági megfontolásokból tilos a csevegő szoftver/programok (pl. WatsApp, Messenger, Signal, Viber, MSN, Gtalk) használata.

Kivételt képezhet a szervezet vezetőjének dokumentált engedélye (pl. szakmai támogatás vagy kommunikációs költségek csökkentése érdekében), de minden esetben szervezeti érdekből használható.

3.5.5. Bizalmas információk kezelése

Amennyiben az interneten keresztüli kommunikáció nem titkosított formában történik, tilos bizalmas vagy magasabb minősítésű információkat küldeni.

Az információk minősítését a 2009. évi CLV. törvény és a 243/2016. (VIII.17.) Korm. rendelet szabályozza.

3.5.6. Tiltott/külön engedélyhez kötött tevékenységek

Alapértelmezésként: a szervezettel kapcsolatos belső információk nyilvános oldalakon való közzététele tilos.

Nem magyarországi illetőségű levelező- és egyéb, felhőalapú szolgáltatások igénybevétele a szolgáltatással érintett adatok besorolása szerint engedélyeztethető, de nem ajánlott, állami, egyes kiemelt ágazati szereplők számára csak abban az esetben lehetséges, ha a felügyeleti jogot gyakorló szerv írásos hozzájárult a felület igénybevételéhez.

3.5.7. Hálózati forgalom figyelése

Információbiztonsági vizsgálat és hibakeresés céljából és a visszaellenőrizhetőség biztosítása érdekében a szervezet informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíteni-menteni kell.

Elektronikus levelek esetén a megfigyelés nem terjed ki a levelek tartalmára. A felhasználói szabályokban meghatározott szabályok, korlátozások eleve kizárják a magán jellegű levelek keletkezését. Ebből kifolyólag, technikai tulajdonságokat vizsgálnak az automatizált folyamatok a biztonság növelése érdekében (pl. kéretlen levelek, vírusokat tartalmazó üzenetek).

3.5.8. Internethasználati szabálysértések kezelése

Munka rovására történő használat:

Ha a felhasználó internethasználata a munka elvégzésének rovására megy (pl. nagy hálózati terhelést okozó tevékenységet folytat), az informatikus/rendszergazda jelzi ezt a felhasználó közvetlen vezetőjének.

Amennyiben az intézkedés eredménytelen marad, az érintett munkatárs vezetője utasítására az internethozzáférést részlegesen vagy teljesen letiltják.

Internethozzáférés korlátozása:

Az internetkapcsolatok üzemeltetéséért felelős vezető jogosult az internethozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozására. A korlátozásról a felhasználókat előzetesen tájékoztatni kell.

3.5.9. Az elektronikus levelezés (e-mail)

Az e-mail szolgáltatás a szervezet által a felhasználók részére a szervezeti elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levelek is a szervezet felügyelete alá tartoznak. A levelező rendszerben keletkező információ, adat vagy dokumentum a szervezet tulajdonát képezi, ezért szándékos törlésük fegyelmi vétség, a BTK hatálya alá tartozik.

3.5.9.1. Általános szabályok

A szervezet elektronikus levelezési rendszere semmilyen mértékben, és a szabályzatban rögzített feltételek szerint sem használható magán (személyes) levelezés céljára.

Az elektronikus levelező rendszer felhasználója a rendszer használatával automatikusan aláveti magát ezeknek a korlátozásoknak.

A szervezet e-mail rendszerén mindennemű jogszabályellenes tartalom továbbítása és tárolása tilos.

3.5.9.2. Használati szabályok

- A szervezet nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező (kliens) szoftver/program, illetve az informatikus/rendszergazda által engedélyezett levelezési (szolgáltatás használható.
- A beállítások (működési paraméterek) meghatározásáért és beállításáért az informatikus/rendszergazda a felelős.
- Az elektronikus levelező rendszerben tárolt és továbbított dokumentumok kezelésénél be kell tartani az érvényben lévő ügyviteli, iratkezelési és adatkezelési szabályokat.

3.5.9.3. E-mail felhasználói kötelezettségek

Minden elektronikus postaládával rendelkező felhasználó köteles postaládájának tartalmát figyelemmel kísérni:

- Legalább munkakezdéskor és munkavégzés előtt ellenőrizni kell, hogy érkezett-e új üzenet.
- Az érkezett üzeneteket kezelni kell (pl. megtekinteni, szükséges intézkedéseket megtenni).
- Amennyiben a szervezeti levelezésben – pontos címzés mellett – kézbesíthetetlenségre utaló hibajelzés érkezik, a felhasználónak fel kell tárnia ennek okát, szükség szerint az informatikus/rendszergazda segítségével.

Tiltott tevékenységek:

- Nagy mennyiségű és méretű személyes jellegű üzenetek küldése.
- Kéretlen reklámok és hirdetések közzététele.
- Lánclevelek terjesztése vagy továbbítása.
- A szervezeti e-mail cím nem hivatalos minőségben történő használata (pl. magánlevelezés, regisztráció letöltési vagy online játék oldalakon).
- Levelek fejlécének megváltoztatása, hamis levelek küldése.
- Törvénytelenségeket vagy arra való felhívást tartalmazó üzenetek küldése.
- Tévesen címzett, másnak szóló levelek felhasználása.
- A szervezeti e-mail címre érkező üzenetek átirányítása külső (nem szervezeti) e-mail címre.
- Idegen nyelvű reklámcélú üzenetek megnyitása vagy továbbítása szigorúan tilos

3.5.9.4. Csoportos levelezés

- Csoportos levelezőlisták használata esetén meg kell győződni arról, hogy valóban szükséges-e minden címzett számára elküldeni az üzenetet.
- Titkos másolat (BCC) alkalmazása ajánlott olyan esetekben, amikor a címzettek nem szerezhetnek tudomást egymásról.

- A központilag létrehozott csoportos levelezők karbantartását az informatikus/rendszergazda végzi el, figyelembe véve a munkaügyi változásokat.

3.5.9.5. Nagyméretű fájlok kezelése

- A küldhető csatolmányok típusáról és méretéről az informatikus/rendszergazda ad kérésre tájékoztatást.
- Nagyméretű fájlok küldése esetén az informatikus/rendszergazdasegítséget nyújt alternatív megoldásokkal (pl. biztonságos fájlmegosztó rendszerek használata).

3.5.9.6. Biztonsági követelmények

Korlátozások:

Az elektronikus levelek méretét és csatolt fájlok típusát az informatikus/rendszergazda korlátozhatja a rosszindulatú kódok terjedésének megakadályozása érdekében.

Ismeretlen feladók kezelése:

Gyanús csatolmányokat vagy linkeket tartalmazó üzeneteket nem szabad megnyitni; az ilyen leveleket törölni kell.

Adatbiztonság:

Bizalmas vagy magasabb minősítésű információkat csak titkosított formában szabad továbbítani.

3.5.9.7. Postaládák kezelése

A felhasználói postaládák mérete korlátozott, amelyet az informatikus/rendszergazda határoz meg technikai lehetőségek figyelembevételével. Nagyobb postaládára vonatkozó igényt a szervezeti egység vezetőjének jóváhagyásával lehet benyújtani.

4. Az informatikai rendszerek üzemeltetése

4.1. Általános rendelkezések

Az informatikai rendszerek üzemeltetésének célja és feladata a szervezet az Információbiztonsági szabályzatában (IBSZ) meghatározott elvek és követelmények teljesítése, valamint az informatikai rendszerek folyamatos és biztonságos működésének biztosítása.

Az informatikus/rendszergazda feladatai

Az informatikus/rendszergazda feladata a felhasználók informatikai támogatása, a szolgáltatások folyamatos, hivatali időben való rendelkezésre állásának biztosítása, a felmerülő biztonsági problémák, megbízható kezelése és a biztonságért felelős személy tájékoztatása a felmerült problémákról és észlelt jelenségekről. Az informatikus/rendszergazda:

- Felelős az informatikai rendszer és a hálózat működőképességéért.
- Felelős a hálózati szolgáltatások, csatlakozások üzembiztonságáért és koordinálásáért.
- Gondoskodik az informatikai eszközök tervszerű megelőző karbantartásáról.
- Felelős a folyamatos, munkaidőben való rendelkezésre állásért, valamint a jelentkező hibák mielőbbi szakszerű ellátásáért.

Felhasználói szabályok

Tiltott tevékenységek:

- A gépek megbontása, hardver konfigurációk megváltoztatása.
- A számítógépes hálózat megbontása vagy átstrukturálása.
- Gépek, eszközök engedély nélküli csatlakoztatása.

Hálózati csatlakozás:

- A szervezet hálózatára számítógépet csak akkor lehet rácsatlakoztatni, ha:
- A hálózati csatlakozás főbb paraméterei (fizikai és logikai címek, a hálózatin struktúrában elfoglalt hely stb.) rögzítésre kerültek.
- A csatlakozást a szervezet vezetője) írásban engedélyezte.
- Illetéktelen eszközcsatlakozás esetén az informatikus/rendszergazdaköteles az eszközt azonnal lekötni a hálózatról, jelenteni a felhasználó vezetőjének, vagy a szervezet vezetőjének.

Kábelek kezelése:

Tilos a hálózat kábeleinek szándékos kihúzása a fali csatlakozóból vagy a gépből.

Eszközök mozgatása:

Számítástechnikai eszközt és tartozékait felhasználásra kijelölt helyéről elvinni csak az informatikus/rendszergazda és az eszköznyilvántartással foglalkozó szervezeti egység tudtával és írásos engedélyével lehet.

Hozzáférés biztosítása

A számítógépes hálózathoz és az informatikai szolgáltatásokhoz való hozzáférés munkaidőben biztosított. Az ettől eltérő igényeket legkésőbb három munkanappal korábban kell jelezni az informatikus/rendszergazda részére.

Az informatikus/rendszergazda köteles biztosítani a hozzáférést, amennyiben az üzemeltető rendszergazda, vagy csoport rendelkezésre áll és technikailag megoldható.

Eszközök használata

Munkavégzés befejezése:

A munka végeztével a felhasználónak ki kell jelentkeznie a használt alkalmazásokból, és ki kell kapcsolnia az informatikai eszközöket.

Átmeneti munkaszünet:

Ha a munkavégzés 15 percnél hosszabb időre megszakad, akkor ki kell lépni a használt alkalmazásokból.

Karbantartás:

Az informatikus/rendszergazda által végzett karbantartási vagy szoftver/program frissítési munkák idejére az érintett alkalmazásokkal történő munkavégzést be kell fejezni.

Rendeltetésszerű használat:

- Az informatikai eszközöket rendeltetésszerűen kell használni:
- A számítógépen és perifériáin papírokat vagy egyéb tárgyakat tárolni nem lehet.
- A szellőző nyílásokat szabadon kell hagyni.
- A billentyűzetet védeni kell a szennyeződésektől.
- A számítógép közelében enni-inni vagy dohányozni tilos!

4.2. Konfigurációkezelés

4.2.1. Konfigurációkezelési eljárásrend

A szervezet:

Kidolgozza, dokumentálja és a szervezeten belül kihirdeti a ***„N06 Konfigurációkezelési szabályzat"***, amely:

- Összhangban van a hatályos jogszabályokkal.
- Elősegíti a konfigurációkezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását.
- Meghatározza a konfigurációkezelés célját, hatókörét, szerepköröket, felelősségeket és a szervezeten belüli együttműködés kereteit.

A fizikai védelmi eljárásrendben vagy más belső szabályozásban meghatározott gyakorisággal, de legalább évente egyszer felülvizsgálja és szükség esetén frissíti a konfigurációkezelési eljárásrendet.

Amennyiben hatáskörébe tartozik, beszerzi és megőrzi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely részletesen tartalmazza:

- A rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálásának, telepítésének és üzemeltetésének lépéseit és követelményeit.
- A biztonsági funkciók hatékony alkalmazásának és fenntartásának módszereit, beleértve a rendszeres biztonsági frissítések és javítások telepítésének eljárásait.
- A funkcióval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket, valamint ezek kezelésének ajánlott módszereit.

Beszerzi és megőrzi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely részletesen tartalmazza:

- A felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját, beleértve a jelszókezelés, hozzáférés-védelem és adatvédelmi beállítások használatát.
- A rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit, kitérve a social engineering támadások elleni védekezésre is.
- A felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának fenntartásához, beleértve az incidensjelentési kötelezettségeket és a biztonságtudatos viselkedés alapelveit.

Gondoskodik arról, hogy az információs rendszerre vonatkozó dokumentáció - különösen az adminisztrátori és fejlesztői dokumentáció - jogosulatlanok számára ne legyen megismerhető vagy módosítható:

- A dokumentációkat biztonságos, korlátozott hozzáférésű tárhelyen tárolja.
- A hozzáférést szerepkör alapú jogosultságkezeléssel és erős azonosítással szabályozza.
- A dokumentációk módosítását naplózza és rendszeresen ellenőrzi.

Biztosítja, hogy a dokumentációkat csak az arra jogosult, meghatározott szerepköröket betöltő személyek ismerhessék meg:

- Nyilvántartást vezet a dokumentációkhoz hozzáférő személyekről és szerepkörökről.
- Rendszeres időközönként felülvizsgálja a hozzáférési jogosultságokat.
- A dokumentációk megismerését oktatással és tudatossági programokkal támogatja.

A konfigurációkezelési eljárásrendet beépíti a szervezet átfogó információbiztonsági programjába, és gondoskodik annak rendszeres és felülvizsgálatáról az aktuális fenyegetettségek és technológiai változások tükrében.

4.2.2. Alapkonfiguráció

Az érintett adminisztrátorok és adatgazdák az IBF közreműködésével elektronikus információs rendszereikhez egy-egy alapfunkciót fejlesztenek ki, dokumentálják és karbantartják azt, leltárba foglalva annak lényeges elemeit ***(„N06.1 Konfigurációkezelési eljárásrend"*** *és* ***„N06.1.1 Konfigurációkezelés -alapkonfiguráció nyilvántartása").***

A szervezet:

- Az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, valamint meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftver/programok használatát (legszűkebb funkcionalitás elve).

Meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon – a „szükséges minimum" elv alapján – az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező funkció beállítást, és ezt ellenőrzési listaként dokumentálja ***(„N06.1.2 Alapkonfiguráció változásainak nyilvántartása").***

- Elvégzi a funkció beállításokat az elektronikus információs rendszer valamennyi elemében.
- A meghatározott elemek funkció beállításaiban azonosít, dokumentál és jóváhagy minden eltérést.
- Figyelemmel kíséri és ellenőrzi a funkció beállítások változtatásait, a szervezet belső szabályzataival és eljárásaival összhangban.

4.2.3. Konfigurációváltozások felügyelete (változáskezelés)

A szervezet:

- Meghatározza a változáskezelési felügyelet alá eső változástípusokat.
- Meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit.
- kockázatelemzés) alapján megvizsgálja, jóváhagyja vagy elutasítja a javasolt változtatásokat.
- Dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket.
- Megvalósítja a jóváhagyott és tesztelt változtatásokat az elektronikus információs rendszerben.
- Visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását.
- Auditálja és felülvizsgálja a funkcióváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.
- A funkció megváltoztatása előtt teszteli az új verziót, dönt annak megfelelőségéről, és dokumentálja a változtatásokat az éles rendszerben történő megvalósítás előtt.

4.3. Programok használatának korlátozásai

A szervezet:

- Kizárólag az informatikusnak/rendszergazdának van joga és lehetősége szoftver/programok telepítésére az informatikai rendszerben. A felhasználóknak nem lehet jogosultsága szoftver/program telepítésre, vagy bizonyos beállítások módosítására.
- Szigorúan tiltja illegális és/vagy nem jogtiszta szoftver/program telepítését a szervezet informatikai eszközeire.
- Kizárólag a szervezet által megvásárolt licencű kereskedelmi termékek és/vagy szabad szoftver/programok használatát engedélyezi a feladatok végrehajtására az informatikai infrastruktúrában.
- Előírja, hogy minden illegális vagy nem a munkavégzést szolgáló szoftver/programot és adatot törölni kell a rendszerből. Ezt a műveletet az informatikus/rendszergazda végzi el a felhasználó tudtával.
- Fenntartja a jogot, hogy illegális szoftver/program használata esetén fegyelmi, kártérítési, illetve egyéb eljárást indítson a felhasználóval szemben felelősségének megállapítása érdekében.
- Megköveteli, hogy a telepítést megelőzően a szervezetben üzemeltetett vírusvédelmi eszközzel vizsgálják meg az esetleges vírusfertőzöttségét.
- Előírja, hogy amennyiben technikailag/technológiailag lehetséges, az új szoftver/program csomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad végezni, az eredeti példányt biztonságos helyen kell tárolni.

Szigorúan megtiltja idegen szoftver/program vagy adat másolását a szervezet infrastruktúrájában található eszközökre.

4.3.1. Felhasználó által használható programok

A szervezet az informatikai eszközöket kizárólag munkavégzés céljára biztosítja a felhasználók számára.

A felhasználók jogosultságát a belső hálózaton az alábbiakra korlátozza:

A jóváhagyott, a telepíthető alkalmazások listáján ***(„N06.1.3 Telepíthető alkalmazások listája")***

- szereplő egységes irodai alkalmazások és szolgáltatások használata.
- A munkájukhoz kizárólag alkalmazói -felhasználói jog biztosított a felhasználó számára.
- A felhasználóknak sem joguk, sem lehetőségük nincs alkalmazások telepítésére, amennyiben ilyen igény felmerül, a felettes vezetőtől írásban igényelni szükséges.
- Szigorúan megtiltja a szervezet informatikai infrastruktúrájának magáncélú használatát.

4.3.1.1. Eszközkivonás

Kivételes esetben, kizárólag hordozható eszközökre (notebook, tablet, mobiltelefon, mobil adathordozók) vonatkozóan engedélyezheti az eltérést, az alábbi feltételekkel:

A szervezet vezetője és az Információbiztonsági Felelős (IBF) írásbeli engedélye szükséges

A felhasználónak nyilatkozatot kell tennie, amelyben vállalja, hogy:

- Nem használja a szervezet belső informatikai struktúráját (kivéve a tűzfallal leválasztott nyilvános részeket, pl. vendég wifi)
- Tudomásul veszi a kapcsolódó kockázatokat
- Lemond a szervezet nem nyilvános hálózatának bármilyen használati lehetőségéről
- Átvállalja a kivont eszköz hardver- és szoftver/program karbantartását (kivéve a garanciális javítások ügyintézését)

Az informatikai üzemeltetésért felelős szervezeti egység feladata marad a garanciális javítások ügyintézése. A felhasználót tájékoztatni és nyilatkoztatni kell a kivételes használattal járó feltételekről és kockázatokról.

4.4. Adathordozók védelme

4.4.1. Adathordozók védelmére vonatkozó eljárásrend

A szervezet:

A hordozható külső adattárolókat (pl. flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) egyedi azonosítóval látja el, kivéve az optikai adathordozókat (CD, DVD) és a hajlékonylemezeket, amelyeket csak számszerűen tart nyilván.

Az egyedi azonosítóval ellátott hordozható adathordozók pontos helyéről naprakész nyilvántartást vezet.

Az adathordozók használatára vonatkozóan az alábbi szabályokat alkalmazza:

- A használni kívánt adattárolót a tárolásra kijelölt helyről kell kivenni és használatot követően oda kell visszahelyezni.
- A munkaasztalokon és a számítógépekben csak a munkavégzéshez szükséges adathordozók lehetnek.

A fontos adatokat tartalmazó adathordozókról másolatot készít, melyeket:

- Egymástól elkülönítetten, lehetőleg külön szobában tárol.
- Jól zárható lemezszekrényben helyez el.

Az adathordozók védelmére vonatkozó további részletes szabályozást az ***„N11 Adathordozó védelmi szabályzat"*** dokumentumban és az ***"N11.1 Adathordozó védelmi eljárásrend"***-ben határozza meg.

4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz

A szervezet:

Nyilvántartást vezet az egyes adathordozó-típusokhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk tartalmáról, és ezt rendszeres időközönként felülvizsgálja, aktualizálja az ***„N11.1.1 Adathordozók nyilvántartása"*** dokumentumban.

Előírja, hogy minden munkatárs köteles az adattárolókat rendeltetésszerűen, csak a munkavégzéshez szükséges adatok és szoftver/programok tárolására használni.

A szervezet tulajdonában lévő hordozható külső adattárolók (flash diskek, pendrive-ok, memóriakártyák, hordozható HDD-k) szervezeten kívüli használatát csak kivételes esetben, írásbeli vezetői engedéllyel teszi lehetővé.

Megköveteli, hogy a felhasználók külső adathordozót az informatikai hálózatra csak a szervezet vezetője írásbeli engedélyével, vírusellenőrzés után csatlakoztassanak. A vírusellenőrző szoftver/programot lehetőség szerint úgy kell beállítani, hogy automatikusan elvégezze az ellenőrzést külső eszköz csatlakoztatásakor.

Előírja, hogy munkaállomás meghibásodása esetén a felhasználók kötelesek jelenteni azt az informatikus/rendszergazda felé.

A további felhasználásra alkalmatlan adathordozókat fizikai roncsolással használhatatlanná teszi.

Megköveteli, hogy külső szervizbe szállítás előtt a bizalmas adatokat tartalmazó adathordozókat el kell távolítani a munkaállomásból.

Meghibásodott eszköz cseréje esetén – garanciális esetben is – csak olyan adathordozó vihető ki a szervezet területéről, amelyről minden adat visszaállíthatatlan módon törlésre került. Minimum hétszer történő, teljes mélységű újraírást fogad el végleges visszaállíthatatlan törlésnek.

A rendszert üzemeltető rendszergazda, vagy csoport kötelessége a felülírások sikerességének ellenőrzése.

4.4.3. Adathordozók újra felhasználása, selejtezése, megsemmisítése

A szervezet:

Meghatározza és alkalmazza az adathordozók újrafelhasználásra, selejtezésére és megsemmisítésére vonatkozó eljárásokat.

Az adathordozók újrafelhasználása esetén biztosítja, hogy:

- Az új felhasználó(k) jogosulatlanul ne férhessenek hozzá a korábban az eszközön tárolt adatokhoz.
- Az eszközökön biztonságos törlést hajtanak végre, ahol a teljes adathordozón található valamennyi adat, partíció legalább hétszer kerül felülírásra. A biztonságos adattörlés esetén az ajánlott módszer a NIST SP 800-88 Rev. 1[5] ajánlás
- A törlést végző minden esetben ellenőrzi a törlés sikerességét.

A szervezet:

Megtiltja azon adathordozók újrafelhasználását, amelyeket nem lehet engedélyezett módon törölni. A sérült vagy elhasználódott adathordozókat, amelyek további használata lehetetlen vagy célszerűtlen, selejtezi és fizikailag megsemmisíti.

Az informatikai eszközök és adattárolók selejtezését, beleértve a megsemmisítési folyamatokat az Selejtezési és megsemmisítési jegyzőkönyvben dokumentáltan végzi el.

A selejtezési eljárás során olyan módszereket alkalmaz, amelyek megakadályozzák, hogy a későbbiekben az eszközökről adatokat lehessen visszanyerni.

Az alábbi adatmegsemmisítési módszereket alkalmazza:

- FDD, CD, DVD, pendrive, SSD merevlemez esetén erre alkalmas adatmegsemmisítő eszközzel fizikailag semmisíti meg, égetéssel vagy átfúrással, dokumentált formában.
- Alternatívaként szerződésben megbíz egy fizikai megsemmisítésre szakosodott céget.

Gondoskodik arról, hogy az adathordozók megsemmisítését csak arra jogosult személyek végezhessék.

A megsemmisítési folyamatról jegyzőkönyvet készít, amely tartalmazza legalább a megsemmisített eszközök típusát, azonosítóját, a megsemmisítés módját és időpontját, valamint a folyamatban résztvevő személyek nevét és aláírását.

4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra

A szervezet teljes informatikai rendszerére ***„N07 Üzletmenet-folytonossági szabályzat"-ot*** (BCP és DRP) készít, amely meghatározza, hogyan lehet a szervezet kritikus funkcióit üzemben tartani, vagy biztonságos üzemüket minél hamarabb visszaállítani különböző mértékű problémák bekövetkezése esetén. A terv célja, hogy megfeleljen a rendelet előírásainak.

A szervezet kötelezettségei:

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

- **Összehangolja** a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével, biztosítva az üzletmenet-folytonosságot és a kiberbiztonsági incidensek kezelését.
- **Felülvizsgálja** az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági terveket meghatározott gyakorisággal, de legalább évente egyszer.
- **Aktualizálja** az **üzletmenet-folytonossági tervet** az elektronikus információs rendszer vagy a működtetési környezet változásainak, valamint a végrehajtás és vagy tesztelés során felmerülő problémáknak megfelelően.
- **Tájékoztatja** az **üzletmenet-folytonossági terv** változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.
- **Biztosítja**, hogy az üzletmenet-folytonossági tervet jogosulatlan személyek számára ne legyen megismerhető vagy módosítható, megfelelő hozzáférés-kezelési intézkedésekkel (pl. RBAC modell).
- **Meghatározza**; az alapfeladatokat biztosítandó szolgáltatásokat és funkciókat, valamint ezekhez kapcsolódó vészhelyzeti követelményeket, figyelembe véve a NIS2 által előírt kritikus rendszerek osztályozását (alapjelentőségű/jelentős/magas).
- **Rendelkezik**; á helyreállítási feladatokról, prioritásokról és mértékekről (RTO ≤ 4 óra, RPO ≤ 1 óra magas besorolású rendszereknél).
- **Jelöli**, a vészhelyzeti szerepköröket, felelősségeket és kapcsolattartó személyeket, beleértve a kiberbiztonsági felelőst és – ha szükséges – a magyarországi képviselőt nemzetközi szervezetek esetén.
- **Fenntartja**; a szervezet által előzetesen definiált alap szolgáltatásokat még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája esetén is.
- **Kidolgozza**; a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

Az ***„N07.1.1 Üzletmenet-folytonossági terv rendszerelemekre"*** azaz a BCP/DRP tartalma:

- A kritikus fontosságú rendszerek és erőforrások azonosítását, azok alapfeladatait és funkcióit.
- A rendelkezésre állás biztosításának módját (pl. redundáns rendszerek, tartalékképzés.
- Az ehhez kapcsolódó vészhelyzeti követelménye a minimális szolgáltatási szintek fenntartása.
- A szervezeti adatvagyon mentési-, archiválási- és helyreállítási rendjét, beleértve titkosított mentések alkalmazását AES-256 szabvánnyal és törlésgátló mechanizmusokkal.
- A helyreállítási prioritások részletezését RTO/RPO célkitűzésekkel összhangban.

Megvalósítási kötelezettségek:

- A kidolgozott stratégiák (előkészületek, eljárások dokumentálása, oktatás megvalósításához felelősöket kell kijelölni a BCP/DRP-ben rögzített módon.
- A terv hatékonyságát évente legalább egyszer teljes körű teszteléssel kell ellenőrizni (pl. szimulációs gyakorlatok), amelynek eredményeit dokumentálni kell.
- Az incidensekről történő jelentéstételt a NIS2 szabályozás szerint 24/72 órán belül kell megtenni hatóság felügyeleti jogot gyakorló szerv részére.

Karbantartási kötelezettségek:

- A BCP-t és a DRP-t minden jelentős változás után frissíteni kell (pl. új rendszerek bevezetése vagy jogszabályváltozás esetén) és legalább évente felül kell vizsgálni.
- Az érintett kulcsszereplőket minden esetben tájékoztatni kell a változásokról.

4.6. Az elektronikus információs rendszer mentései

A szervezeti informatikai rendszerekben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell, összhangban szabályozás követelményeivel, a kapcsolódó rendelet előírásaival.

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve szoftver/programok biztonsági besorolásával, elvesztésük, sérülésük kockázatával és hatásával ***„N15.1.1 Kockázatelemzés -kockázatértékelés"***, valamint a szervezet ügyintézési ciklusával. A kritikus fontosságú rendszerek esetében napi mentés szükséges, míg alacsonyabb prioritású rendszerek esetén heti vagy havi mentések is elegendők lehetnek.

Az informatikai infrastruktúrában a biztonsági mentési eljárást ***(„N04.2 Mentési szabályzat")***, annak pontos leírását, valamint az ehhez tartozó feladatokat, szabályokat az ***„N04.2.1 Mentési rend")*** című dokumentum szabályozza részletesen a következő alapelvek betartásával. A dokumentum elkészítésért az informatikus/rendszergazda felelős.

Az informatikus/rendszergazda feladata a felhasználói rendszerekben leírtakon felüli rendszeres és időszakos biztonsági mentések elvégzése. A mentéseket úgy kell végezni, hogy az adatbázisok konzisztenciája biztosítva legyen, illetve a munkaállomások mentései a hálózat működését ne akadályozzák.

A mentési rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőből adódó hibák előfordulásának valószínűségét. Ennek koordinációjáért és a szükséges források tervezéséért az informatikus/rendszergazda a felelős.

A szoftver/programok változtatás előtt biztonsági mentést kell készíteni, amelynek felelőse az informatikus/rendszergazda. A mentést követően az adathordozót a szerver szobától eltérő helyiségben (lehetőség szerint a szerverszobával nem azonos épületben), erre a célra rendszeresített biztonsági szekrényben, elzárva kell tárolni. A NIS2 követelményeinek megfelelően, legalább két földrajzilag elkülönült helyszínen kell tárolni a kritikus rendszerek mentéseit (georedundancia), hogy csökkentsék egyetlen helyszín kiesésének kockázatát. Törekedni kell arra, hogy a mentések tárolása fizikailag biztonságos legyen, védeni kell őket az illetéktelen hozzáférésektől, illetve a különböző fizikai behatásoktól (tűz, víz, mágnesesség stb.).

A biztonsági mentéseket legalább AES-256 szabványú titkosítással kell védeni, hogy biztosítsák az adatok bizalmasságát és sértetlenségét még illetéktelen hozzáférés esetén is. A biztonsági mentéseket hibajelzésmentesen, visszatölthető módon kell elkészíteni. Ennek érdekében a mentések felhasználhatóságát, amennyiben technikailag lehetséges, szúrópróbaszerűen tesztelni kell, illetve a mentési eljárásba épített automatikus ellenőrzéseket kell végrehajtani. Ennek betartásáért a biztonsági mentés elvégzésével megbízott rendszergazda tartozik felelősséggel. Sikertelen mentés esetén a lehető legrövidebb időn belül meg kell ismételni a mentést.

A magas prioritású rendszereknél az RTO (helyreállítási időcél) legfeljebb 4 óra, míg az RPO (adatvesztési cél) legfeljebb 1 óra lehet. A mentési folyamatokat legalább kétévente független auditnak kell alávetni annak érdekében, hogy megfeleljenek mind a belső szabályozásoknak, mind pedig a NIS2 követelményeinek.

Mentési hibákból eredő adatvesztést vagy adatbiztonsági incidenst 24 /72 órán belül jelenteni kell a hatóság felügyeleti jogot gyakorló szerv részére.

4.6.1. A felhasználók adatainak mentése

A felhasználók munkaállomásokon lévő adatainak kezelését és mentését az alábbi követelményeknek megfelelő szabályok szerint kell végezni:

Központi tárolás és mentés

A felhasználók kötelesek a munkájukhoz tartozó fontos dokumentumokat a fájlszerverek erre kijelölt, megfelelően védett területein tárolni. Ezeket a központi tárhelyeket az informatikai osztály rendszeresen menti a szervezet általános Mentési rendje szerint.

Felelősségi körök

A belső szabályozásokban meghatározott adatállományok tekintetében a szerverre nem mentett, helyi adatok elvesztéséért vagy sérüléséért a felhasználó felelős. Az informatikai osztály nem vállal felelősséget a nem központi tárhelyen tárolt adatok helyreállításáért.

Mobil eszközök kezelése

A szervezet által kiadott notebook-ok adatainak mentését az informatikus/rendszergazda végzi el, előzetes egyeztetés alapján. A mentés gyakoriságát az adatok kritikussága és a felhasználó mobilitása alapján kell meghatározni, de legalább havonta egyszer el kell végezni.

Adathordozók használata

A felhasználók által kezelt adatok külső adathordozóra (pl. DVD) írását - ha az iroda nem rendelkezik saját eszközzel - kérésre az informatikus/rendszergazda végzi el.

- Az adathordozókon tárolt adatok jogtisztaságáért a felhasználó felelős.
- A munkaállomásokon lévő adat be- és kiviteli eszközök (FDD, CD, DVD, USB) használata korlátozott és ellenőrzött, kizárólag indokolt esetben, vezető írásos engedély kiadása után valósítható meg.
- A mobil adathordozók használatát minimalizálni kell a biztonsági kockázatok csökkentése érdekében.

Titkosítás és adatvédelem

Minden külső adathordozóra mentett kritikus vagy személyes adatot titkosítani kell, legalább AES-256 szabvány szerint. Az informatikai osztálynak biztosítania kell a megfelelő titkosítási eszközöket és **oktatást** a felhasználók számára.

Adathordozók kezelése és selejtezése

- A már nem használt, megrongálódott vagy selejtezendő adathordozókat a felhasználók kötelesek leadni az informatikai osztálynak.
- Az adathordozók biztonságos megsemmisítéséről az informatikai osztály gondoskodik, a vonatkozó adatvédelmi és környezetvédelmi előírásoknak megfelelően.

Oktatás és tudatosítás

Az informatikai osztály rendszeres képzéseket tart a felhasználóknak az adatmentés fontosságáról és a helyes gyakorlatokról. A felhasználókat oktatni, képezni kell a nem megfelelő adatkezelésből eredő kockázatokról és azok potenciális következményeiről.

Ellenőrzés és audit

Az informatikai osztály rendszeres ellenőrzéseket végez a felhasználói adatmentési gyakorlatok megfelelőségének biztosítására. Évente legalább egyszer vizsgálatot kell végezni az adatmentési folyamatok hatékonyságának és megfelelőségének értékelésére.

Incidenskezelés

Adatvesztés vagy adatszivárgás esetén a felhasználónak azonnal értesítenie kell az informatikai osztályt. Az informatikai osztály köteles az incidenst kivizsgálni és szükség esetén 24/72 órán belül jelenteni a hatóságfelügyeleti jogot gyakorló szerv részére, összhangban a NIS2 követelményeivel.

4.6.2. A szervereken tárolt adatok mentése

A központi szervereken tárolt elektronikus információvagyont a biztonsági káresemények ellen mentéssel védi az üzemeltető rendszergazda, vagy csoport. A mentési folyamatokat az alábbiak szerint kell végrehajtani:

Mentési rend

- A rendszer egészéről a mentési rend dokumentumban leírtaknak megfelelően teljes mentést kell készíteni.
- A Mentési rendet évente felül kell vizsgálni és szükség esetén aktualizálni kell a változó technológiai és szabályozási környezetnek megfelelően.

Mentések gyakorisága és típusa

- kritikus rendszerek esetében napi inkrementális és heti teljes mentést kell végezni.
- Kevésbé kritikus rendszerek esetében heti inkrementális és havi teljes mentés is elegendő lehet.

Mentések ellenőrzése

- A mentéseket minden mentési rendet érintő (fizikai, logikai, vagy adminisztratív) változáskor, de legalább negyedévente egyszer ellenőrizni kell aszerint, hogy visszatöltésük, helyreállításuk valóban működik-e.
- Az ellenőrzéseket dokumentálni kell a mentési rend dokumentumban.

Titkosítás és adatvédelem

- Minden mentést AES-256 vagy erősebb titkosítással kell védeni.
- A titkosítási kulcsokat biztonságosan, a mentésektől elkülönítve kell tárolni.

Georedundancia (Földrajzilag elosztott biztonsági másolatok)

- A kritikus rendszerek mentéseit legalább két, földrajzilag elkülönült helyszínen kell tárolni.

Helyreállítási terv

A mentések rendjét, valamint a helyreállítási tervet a rendszerszintű leírásoknak, illetve az ***„N04.2.1 Mentési eljárásrend"*** dokumentumnak kell tartalmaznia.

- A helyreállítási tervnek tartalmaznia kell a helyreállítási időcélt (RTO) és az adatvesztési célt (RPO), amelyek kritikus rendszerek esetében nem haladhatják meg a 4 órát (RTO), illetve 1 órát (RPO).

Audit és megfelelőség

- A mentési folyamatokat évente legalább egyszer független auditnak kell alávetni.
- Az audit eredményeit dokumentálni kell, és az esetleges hiányosságokat 30 napon belül meg kell szüntetni.

Incidenskezelés

Mentési hibák vagy adatvesztés esetén az incidenst 24 órán belül jelenteni kell a hatóságfelügyeleti jogot gyakorló szerv felé észlelési jelentésként, 72 órán belül részletesen, majd 30 napon belül zárójelentés formájában, a jogszabályi követelményeinek megfelelően.

Oktatás és tudatosítás

Az üzemeltető rendszergazda, vagy csoport tagjainak rendszeres képzést kell kapniuk a legújabb mentési technológiákról és biztonsági gyakorlatokról.

Dokumentáció és nyomon követhetőség

Minden mentési és visszaállítási műveletről részletes naplót kell vezetni, amely tartalmazza a művelet időpontját, típusát, terjedelmét és az elvégző személy azonosítóját.

4.7. Az elektronikus információs rendszer helyreállítása és újraindítása

A szervezet rendszereinek az informatikus/rendszergazda az ***„N07.1 Üzletmenet-folytonossági eljárásrend"*** BCP/DRP-ben leírtaknak megfelelően gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően. A helyreállítási és újraindítási folyamat a következő elemeket tartalmazza:

Helyreállítási prioritások

- A **kritikus rendszer**ek helyreállítását prioritásként kell kezelni, összhangban a szervezet által meghatározott RTO (Recovery Time Objective) és RPO (Recovery Point Objective) célokkal.
- **kritikus rendszer**ek esetében az RTO nem haladhatja meg a 4 órát, az RPO pedig az 1 órát.

Helyreállítási folyamat

- A helyreállítási folyamatot részletesen dokumentálni kell, beleértve a szükséges lépéseket, felelősségi köröket és időkereteket.
- A folyamatnak tartalmaznia kell a rendszer integritásának ellenőrzését a helyreállítás után.

Adatintegritás és konzisztencia

- A helyreállítás során biztosítani kell az adatok integritását és konzisztenciáját.
- Ellenőrizni kell, hogy a helyreállított rendszer nem tartalmaz-e malware-t vagy egyéb biztonsági fenyegetést.

Tesztelés és validálás

- A helyreállított rendszert alaposan tesztelni kell a normál üzembe helyezés előtt.
- A tesztelési folyamatnak ki kell terjednie a funkcionalitásra, teljesítményre és biztonsági szempontokra.

Kommunikáció

- A helyreállítási folyamat során rendszeres tájékoztatást kell nyújtani az érintett feleknek, beleértve a vezetőséget és a felhasználókat.
- Kritikus incidensek esetén bejelentés 24 órán belül kel megtenni, majd 72 órán belül részletes jelentést kell tenni a hatóságfelügyeleti jogot gyakorló szerv részére, a jogszabály követelményeinek megfelelően.

Dokumentáció és naplózás

- A helyreállítási folyamat minden lépését részletesen dokumentálni kell.
- A naplóknak tartalmazniuk kell az elvégzett műveleteket, időpontokat és felelős személyeket.

Utólagos elemzés

- A helyreállítás után részletes elemzést kell végezni az incidens okairól és a megelőzés lehetőségeiről.

- Az elemzés eredményeit fel kell használni a jövőbeli incidensek megelőzésére és a helyreállítási folyamat javítására.

Rendszeres gyakorlatok

- Évente legalább egyszer teljes körű helyreállítási gyakorlatot kell végezni (helyreállítási teszt) a kritikus rendszerre.
- A gyakorlatok eredményeit dokumentálni kell, és fel kell használni a folyamatok finomítására.

Biztonsági frissítések

- A helyreállítás során biztosítani kell, hogy a rendszer a legfrissebb biztonsági frissítésekkel rendelkezzen.

Audit és megfelelőség

- A helyreállítási folyamatokat rendszeres időközönként, de legalább kétévente független auditnak kell alávetni.
- Az auditnak ki kell terjednie a folyamatok hatékonyságára és a jogszabályi követelményeknek való megfelelésre.

4.8. Karbantartás

4.8.1. Rendszer karbantartási eljárásrend

A szervezet a követelményeknek megfelelően:

Kidolgozza, dokumentálja és kihirdeti a rendszer karbantartási szabályzatot ***„N10 Karbantartási szabályzat"*** a rendszerüzemeltető kidolgozza az ***„N10.1 Karbantartási eljárásrend"***-et, amely összhangban van a NIS2 irányelvekkel és a vonatkozó nemzeti jogszabályokkal.

- Rendszeresen, de legalább évente felülvizsgálja és frissíti a rendszer karbantartási eljárásrendet, figyelembe véve a változó fenyegetettségi környezetet és a technológiai fejlődést.
- Kialakít egy szigorú folyamatot a karbantartók munkavégzési engedélyének kezelésére, beleértve a háttérellenőrzést és a biztonsági oktatást.
- Részletes nyilvántartást vezet a karbantartó szervezetekről vagy személyekről, beleértve a szerződéses feltételeket és a titoktartási kötelezettségeket.
- Többfaktoros hitelesítést követel meg a karbantartást végzőktől az elektronikus információs rendszerhez való hozzáféréshez.
- Kijelöl megfelelő jogosultságokkal és szakértelemmel rendelkező belső személyzetet a külső karbantartók tevékenységének felügyeletére, különös tekintettel a kritikus rendszerre.

4.8.2. Rendszeres karbantartás

A szervezet a követelményeknek megfelelően:

A karbantartásokat és javításokat ütemezetten hajtja végre ***„N10.1.2 Elvégzett karbantartások nyilvántartása"*** dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket, összhangban a gyártói specifikációkkal, a szervezeti követelményekkel és a NIS2 előírásaival.

- Minden karbantartási tevékenységet jóváhagy és ellenőriz, beleértve a távoli karbantartást is, különös figyelmet fordítva a kritikus rendszerre.

Az elektronikus információs rendszer vagy rendszerelemek szervezeti létesítményből való kiszállítását szigorú jóváhagyási folyamathoz köti ***(„N11.1.2 Adathordozó eszköz kiviteli engedély")*** biztosítva a folyamatos nyomon követhetőséget.

- Az elszállítás előtt minden adatot és információt biztonságosan töröl a berendezésről, használva a NIS2 által ajánlott adattörlési módszereket.
- A karbantartás vagy javítás után alapos biztonsági ellenőrzést végez, beleértve a sérülékenység-vizsgálatot és a funkciós beállítások ellenőrzését.
- Részletes karbantartási naplót vezet, amely tartalmazza a végrehajtott műveleteket, az érintett rendszereket, a karbantartást végző személyeket és a biztonsági ellenőrzések eredményeit.

Rendszeres kockázatértékelést végez a karbantartási folyamatokra vonatkozóan, és szükség esetén frissíti az eljárásrendet. Biztosítja, hogy a karbantartási tevékenységek során használt szoftver/programok és firmware-ek megfeleljenek a legújabb biztonsági követelményeknek és frissítéseknek.

5. Rendszer- és információ sértetlenség

Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert a szervezet üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell az alábbiakat érvényesíteni, és azokat a szolgáltatónak kell biztosítania.

5.1. Rendszer- és információsértetlenségre vonatkozó eljárásrend

A szervezet az alap biztonsági osztály biztonsági osztály követelményeinek megfelelően:

Eljárásrend kidolgozása és dokumentálása

Megfogalmazza, dokumentálja és a szervezeten belül kihirdeti a rendszer- és információsértetlenségre vonatkozó szabályzatot ***(„N18 Rendszer- és információsértetlenségi szabályzat")*** és eljárásrendet ***(„N18.1 Rendszer- és információsértetlenségi eljárásrend").***

- Az eljárásrend a szervezet információbiztonsági szabályzatának szerves részét képezi.
- Az eljárásrend összhangban van a NIS2 irányelv követelményeivel és a vonatkozó nemzeti jogszabályokkal.

Eljárásrend tartalma

- Részletesen leírja a rendszer- és információsértetlenség biztosításának módszereit és eszközeit.
- Meghatározza a sértetlenség ellenőrzésének gyakoriságát és módját.
- Tartalmazza az incidenskezelési eljárásokat, beleértve a 24/72 órás jelentési kötelezettséget a hatóságfelügyeleti jogot gyakorló szerv részére, incidensek esetén.

Rendszeres felülvizsgálat és frissítés

- Az eljárásrendet legalább évente, vagy jelentős változások esetén azonnal felülvizsgálja és frissíti.
- A és felülvizsgálat során figyelembe veszi a legújabb fenyegetettségi trendeket és technológiai fejlesztéseket.

Felelősségi körök meghatározása

- Egyértelműen definiálja a rendszer- és információsértetlenséggel kapcsolatos felelősségi köröket és szerepeket a szervezeten belül.

- Kijelöl egy felelős személyt vagy csoportot az eljárásrend karbantartására és végrehajtásának felügyeletére.

Oktatás és tudatosítás

- Rendszeres képzéseket tart a munkatársak számára a rendszer- és információsértetlenség fontosságáról és az eljárásrend betartásáról.
- Az új belépők számára kötelező bevezető **oktatás**t biztosít.

Megfelelőség ellenőrzése

- Rendszeres belső auditokat végez az eljárásrend betartásának ellenőrzésére.
- Legalább kétévente független külső auditot végeztet a jogszabályi követelményeknek való megfelelés értékelésére.

Incidenskezelés és jelentés

- Részletes eljárásokat dolgoz ki a rendszer- és információsértetlenséget érintő incidensek kezelésére.
- Biztosítja a gyors reagálást és a 24/72 órán belüli jelentéstételt a hatóságfelügyeleti jogot gyakorló szerv részére, incidensek esetén.

Technológiai megoldások

- Meghatározza és dokumentálja a rendszer- és információsértetlenség biztosításához használt technológiai megoldásokat (pl. integritás-ellenőrző szoftver/programokat, naplózási rendszerek).
- Rendszeresen felülvizsgálja és frissíti ezeket a megoldásokat a változó fenyegetettségi környezetnek megfelelően.

Kockázatértékelés

- Rendszeres kockázatértékelést végez a rendszer- és információsértetlenséget érintő fenyegetésekre vonatkozóan.
- A kockázatértékelés eredményeit felhasználja az eljárásrend és a védelmi intézkedések fejlesztésére.

Külső partnerek kezelése

- Meghatározza a külső partnerekkel és szolgáltatókkal szemben támasztott követelményeket a rendszer- és információsértetlenség tekintetében.
- Rendszeres ellenőrzéseket végez a partnerek megfelelőségének biztosítására.

5.2. Felügyelet

A biztonsági események olyan események, melyek eltérnek a megszokott ügymenettől, zavarokat okozhatnak és fenyegethetik az információk, illetve az információfeldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

5.2.1. Definíciók és kategorizálás

- **Biztonsági események**: A megszokott ügymenettől eltérő események, amelyek potenciálisan veszélyeztethetik az információk és az információfeldolgozó eszközök biztonságát.
- **Információbiztonsági incidensek**: Az IBF vagy a szervezet vezetője által minősített olyan biztonsági események, melyek ténylegesen fenyegetik az információk, illetve az információfeldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

- **Minősített incidens**: A rendszerelemek (hardverek, szoftver/programok, adathordozók rendeltetésszerű használata közben fellépő, normál működéstől eltérő viselkedése.

A védelem gyenge pontjai: A rendszer, a folyamatok, illetve az abban részt vevő személyek olyan tulajdonságai, hiányosságai, melyek biztonsági incidensek kialakulásához vezethetnek.

5.2.2. Észlelés és jelentés

Biztonsági eseményt, illetve a védelem gyenge pontjait a szervezet minden munkatársa, a rendszereket használó szerződött partnere és a projektekbe bevont harmadik felek észlelhetik, illetve annak létét feltételezhetik. Biztonsági eseményre – incidensre - utaló jelek lehetnek többek között:

- Adatok, információk, fájlok eltűnése, módosulása;
- Információfeldolgozó eszközök, adattárolók eltűnése, rongálódása;
- Információfeldolgozó eszközök megszokottól eltérő működése;
- Adatátvitel szokásostól eltérő lelassulása;
- Bizalmas információk nem ellenőrzött, külső csatornából történő visszahallása.

A szervezetnek nem kell bejelentenie azt a kiberbiztonsági incidensközeli helyzetet és üzemeltetési kiberbiztonsági incidenst, amely (...) automatizmus által kezelésre, elhárításra került és nem járt a szolgáltatás degradációjával. Az ismétlődő kiberbiztonsági incidensközeli helyzetet és üzemeltetési kiberbiztonsági incidenst a szervezet ez esetben is bejelenti.

5.2.3. Azonnali teendők és jelentési kötelezettség

Elsődleges szabály, hogy az információbiztonsági incidensek gyanújának felmerülése esetén (incidens észlelésekor) azonnal értesíteni kell:

- az információbiztonsági felelőst (IBF),
- az adatvédelmi felelőst (DPO),
- az informatikust/rendszergazdát,
- ha a szervezet a 2024. évi LXXXIV. törvény[6] hatálya alá tartozik, akkor a kritikus szervezet ellenálló képességéért felelős vezetőt,
- valamint a 7/2024. (II. 5.) MK rendelet a rendelkezésre állással működő incidenskezelő csoportot (CSIRT)

A felhasználónak TILOS az incidens körülményeit önállóan vizsgálni, illetve megkísérelni elhárítani azt!

5.2.4. Kiegészítő intézkedések és folyamatok

Automatizált felügyeleti rendszerek:

- Bevezetésre kerülnek a gyors észlelés és reagálás érdekében.
- Folyamatos monitorozást és naplóelemzést végeznek.

Jelentési kötelezettség:

- Biztosítja a gyors reagálást és a 24/72 órán belüli jelentéstételt a hatóság felügyeleti jogot gyakorló szerv részére, incidensek esetén.
- Részletes incidensjelentési folyamat kerül kidolgozásra és dokumentálásra.

---

[6] 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről Forrás: https://net.jogtar.hu/jogszabaly?docid=a2400084.tv# - Wolters Kluwer - Minden jog fenntartva!

Rendszeres gyakorlatok:

- Évente legalább egy incidens-szimulációs gyakorlat végrehajtása kötelező.
- A tapasztalatok alapján az eljárásrend frissítésre kerül.

Külső partnerek bevonása:

- Szerződéses kötelezettségként szerepel a biztonsági események azonnali jelentése.
- Rendszeres képzés és tájékoztatás biztosított a partnerek számára.

Folyamatos kockázatértékelés:

- A felügyeleti rendszer hatékonyságának rendszeres felülvizsgálata történik.
- Új fenyegetések és sebezhetőségek proaktív azonosítása folyamatos.

Dokumentáció és nyomon követhetőség:

- Minden észlelt esemény és incidens részletes dokumentálásra kerül.
- Az incidenskezelés teljes folyamata naplózásra és archiválásra kerül.

Utólagos elemzés és tanulságok levonása:

- Minden jelentős incidens után részletes elemzés készül.
- Az eredmények felhasználásra kerülnek a védelmi intézkedések fejlesztésére.

5.2.5. Felügyeleti eszközök

A szervezet az információs rendszerei meghatározott alapvető attribútumainak gyűjtésére és elemzésére automata felügyeleti eszközöket alkalmaz, összhangban a követelményekkel.

Felügyeleti eszközök alkalmazása

Automatizált monitorozás:

- A rendszer alapvető attribútumainak (pl. merevlemez telítettség, CPU használat) folyamatos gyűjtése és elemzése.
- Valós idejű riasztások beállítása kritikus küszöbértékek átlépése esetén.

Gyűjtendő információk:

- Az érintett rendszer dokumentációja részletesen tartalmazza a gyűjtendő információk körét.
- A gyűjtött adatok köre kiterjed a biztonsági eseményekre és a teljesítménymutatókra is.

Aktív elemek megfigyelése:

- Az elektronikus információs rendszerben üzemelő aktív elemek üzemállapotának megfigyelése és forgalmának nyomon követése csak az informatikai vezető engedélyével lehetséges.
- A megfigyelést az érvényes törvények és irányelvek betartása mellett kell végezni.
- Csak az szervezet vezetője által engedélyezett hardver- és szoftver/program eszközök használhatók erre a célra.

Felhatalmazás és jogosultságok:

- Diagnosztikai megfigyelő tevékenységet kizárólag az szervezet vezetője által felhatalmazott személyek végezhetnek.
- A jogosultságok rendszeres felülvizsgálata és dokumentálása kötelező.

Tiltott tevékenységek:

- Minden egyéb állapot-, illetve forgalomfigyelő tevékenység gyakorlása szigorúan tilos.
- A tiltott tevékenységek kísérletét is naplózni és jelenteni kell.

Elemzés és jelentéskészítés

Rendszeres elemzés:

- Az elektronikus információs rendszer felügyeleti információit az IBF éves rendszerességgel elemzi.
- Az elemzés kiterjed a trendek azonosítására és a potenciális kockázatok előrejelzésére.

Jelentéskészítés:

- Igény esetén az IBF részletes jelentést készít a felügyeleti információkról rendszerfelügyeleti jelentés.
- A jelentések tartalmazzák az észlelt anomáliákat és a javasolt intézkedéseket.

Fokozott kockázatkezelés:

- Fokozott kockázatra utaló jelek észlelése esetén az IBF azonnal javaslatokat tesz a szükséges intézkedésekre.
- A javaslatokat dokumentálni kell, és nyomon kell követni azok végrehajtását.

Incidenskezelés integrációja:

- A felügyeleti eszközök által észlelt kritikus eseményeket azonnal továbbítani kell az incidenskezelő csoportnak (CSIRT).
- Az incidenskezelési folyamatot a felügyeleti adatok alapján folyamatosan finomítani kell.

Adatmegőrzés és archiválás:

- A felügyeleti adatokat a jogszabályi előírásoknak és a jogszabályi követelményeknek megfelelő ideig meg kell őrizni.
- Az archivált adatokat biztonságos, csak arra jogosultak által hozzáférhető módon kell tárolni.

Rendszeres felülvizsgálat:

- A felügyeleti eszközök hatékonyságát és relevanciáját évente legalább egyszer felül kell vizsgálni.
- A felülvizsgálat eredményei alapján szükség esetén frissíteni kell a felügyeleti stratégiát és eszközöket.

Az elektronikus információs rendszer felügyeleti információt az IBF havi vagy negyedéves rendszerességgel elemzi, igény esetén jelentést készít azokról. Fokozott kockázatra utaló jelek észlelése esetén javaslatokkal él rendszerfelügyeleti információs jelentés.

5.2.6. Biztonsági riasztások és tájékoztatások

A szervezet a következő módon kezeli a biztonsági riasztásokat és tájékoztatásokat, összhangban a követelményekkel:

Külső források figyelése:

- Folyamatosan figyeli az NBSZ-NKI által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket.
- Folyamatosan figyelemmel kíséri az NBSZ-NKI-tól érkező értesítéseket.
- Automatizált rendszert alkalmaz a közlemények azonnali feldolgozására.
- Figyelemmel kíséri a nemzetközi CERT-ek és biztonsági szervezetek közleményeit.

- Részt vesz releváns információbiztonsági fórumokon és szakmai közösségekben.

Belső riasztási rendszer:

- Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki.
- A belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez.
- Többcsatornás kommunikációt alkalmaz (e-mail, SMS, belső chat rendszer) a gyors információterjesztés érdekében.
- A riasztásokat az érintett rendszerek és felhasználók specifikus igényeihez igazítja.

Eseménybejelentési rendszer:

- Kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét.
- Kapcsolatot tart az érintett, jogszabályban meghatározott szervekkel.

Biztosítja a gyors reagálást és a 24/72 órán belüli jelentéstételt a hatóság felügyeleti jogot gyakorló szerv részére, incidensek esetén az ***„N09.1.3 Biztonsági esemény bejelentési űrlap"*** dokumentum megküldésével.

Részletes szabályozást ***„N09 Biztonsági eseménykezelési szabályzat"*** és „N***09.1 Biztonsági eseménykezelési eljárásrend"***-et dolgoz ki a jelentésköteles események azonosítására és a jelentések elkészítésére.

Ellenintézkedések és válaszlépések:

- Megfelelő ellenintézkedéseket és válaszlépéseket tesz a beérkezett riasztások alapján.
- Előre kidolgozott válaszforgatókönyveket alkalmaz a gyakori fenyegetéstípusokra.
- A riasztásokat és fenyegetéseket kockázati szint alapján priorizálja és kezeli.
- Rendszeresen értékeli az ellenintézkedések hatékonyságát.

Folyamatos fejlesztés:

- Minden jelentős incidens vagy riasztás után elemzést végez.
- Az elemzés eredményeit felhasználja a védelmi intézkedések és folyamatok fejlesztésére.
- Rendszeres gyakorlatokat tart a riasztási és válaszlépési folyamatok tesztelésére.
- A gyakorlatok tapasztalatait beépíti a biztonsági eljárásrendbe.

5.3. Incidensek kezelése

Az incidensek kezelése során a szervezet vezetője és az IBF döntenek a szükséges lépésekről, figyelembe véve az alábbi főbb irányelveket és követelményeket:

Döntéshozatal és végrehajtás:

- A döntésekről írásban értesítik az informatikust/rendszergazdát, aki felelősséggel tartozik azok haladéktalan végrehajtásáért.
- A döntéshozatali folyamatba bevonják az incidenskezelő csoportot (CSIRT) is.

Lokalizálás és terjedés megakadályozása:

- A biztonsági incidensek érintett rendszerelemeit minősítést követően lokalizálni kell.
- Meg kell akadályozni az esetleges tovább terjedést (pl. hálózatról leválasztás, internet kapcsolat megszüntetése, hardverelem kiemelése).

Adatgyűjtés és bizonyítékok rögzítése:

- Be kell gyűjteni az összes releváns adatot és bizonyítékot a biztonsági incidensről (naplóbejegyzések, okozott jelenségek stb.).
- Dokumentálni kell az okozott fennakadásokat és károkat.
- A bizonyítékok gyűjtése során figyelembe kell venni a későbbi esetleges jogi eljárások követelményeit.

Kárcsökkentés és helyreállítás:

- Gondoskodni kell a károk enyhítéséről.
- Biztosítani kell a szervezeti funkcionalitás minimálisan elvárt szintű visszaállítását az érintett vezetők által meghatározott módon.
- A helyreállítást úgy kell végezni, hogy az kizárja vagy elfogadható kockázatúra csökkentse a biztonsági incidens megismétlődését.
- Az incidensekről és az incidensek következményeiből le kell vonnia a megfelelő tanulságokat és minden esetben szükséges a kockázatértékelésben figyelembe venni és a kockázatkezelésben beépíteni. Az incidenseket minden esetben dokumentálni kell függetlenül attól, hogy a szervezet működésén belül milyen kimenetellel járt.

Teljes körű helyreállítás:

- Biztosítani kell a szervezeti funkcionalitás teljes körű visszaállítását.
- A helyreállítás során figyelembe kell venni a jogszabály által előírt RTO (Recovery Time Objective) és RPO (Recovery Point Objective) célokat.

Jelentéstétel:

Biztosítja a gyors reagálást és a 24/72 órán belüli jelentéstételt a hatóság felügyeleti jogot gyakorló szerv részére, incidensek esetén az ***(" N09.1.3 Biztonsági esemény bejelentési űrlap „)*** c. dokumentum kitöltésével és eljuttatásával.

5.3.1. Tanulás az incidensekből

Az IBF az Incidens nyilvántartást ***(„N09.1.2 Biztonsági események naplója")*** minden évben kiértékeli még a vezetőségi átvizsgálás előtt. Ezen felülvizsgálat során különös figyelmet fordít:

Ismétlődő incidensek azonosítása:

- Az ismétlődő incidensek mintázatainak felismerése és elemzése.
- Trendek azonosítása az incidensek típusaiban és gyakoriságában.

Incidenskezelés hatékonyságának vizsgálata:

- Az incidensek megfelelő kezelésének vizsgálata.
- Az incidenskezelési folyamatok hatékonyságának értékelése.

Fejlesztési lehetőségek azonosítása:

- Az incidensek előfordulási valószínűségét csökkentő, átfogó, az elektronikus információs rendszert érintő fejlesztési lehetőségek azonosítása.
- Proaktív biztonsági intézkedések javaslata.

Jelentéskészítés és intézkedések kezdeményezése:

- A felülvizsgálatokról jelentést készít a szervezet vezetésének.

- A jelentésben értékeli az incidenseket és szükség esetén megelőző, helyesbítő intézkedéseket kezdeményez.

Tudásmegosztás és képzés:

- Az incidensekből levont tanulságokat beépíti a szervezet biztonsági képzési programjába.
- Rendszeres tájékoztatást nyújt a munkatársaknak az aktuális fenyegetésekről és védekezési módszerekről.

Folyamatos fejlesztés:

- Az incidenskezelési folyamatokat és eljárásrendeket rendszeresen felülvizsgálja és frissíti az új tapasztalatok alapján.
- A jogszabályi követelményeinek való megfelelést folyamatosan ellenőrzi és szükség esetén korrigálja.

5.4. Naplózás

A szervezet informatikai rendszereinek tervezésekor és üzemeltetésekor az alábbi naplózási szabályokat kell alkalmazni, figyelembe véve a követelményeket:

5.4.1. Általános alapelvek

1. A szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg, legalább 1 évig, a jogszabály követelményeinek megfelelően. Külön jogszabályi előírás esetén a megőrzési idő jelentősen eltérhet.
2. Az egyedi elszámoltathatóság érdekében a naplózási funkciókat úgy kell beállítani, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetők legyenek.
3. A napló tartalmazza a problémák megoldásához szükséges adatokat az események és problémák azonosítása érdekében, támogatva a 24/72 órán belüli incidensjelentési kötelezettséget az hatóság felügyeleti jogot gyakorló szerv részére.
4. A jogosult felhasználói tevékenységek és jogosulatlan tevékenységekre irányuló kísérletek naplózásra kerülnek a visszaélések felderítése érdekében.
5. A naplóállományokat minden rendszerben megbízható módon védeni kell a jogosulatlan felfedés, módosítás és törlés ellen, különös tekintettel a központi naplógyűjtő rendszerre. A naplóadatok integritását és hitelességét digitális aláírással vagy más kriptográfiai módszerrel kell biztosítani.
6. A naplóállományok ellenőrzését szükséges rendszeres időközönként elvégezni. Automata ellenőrző szoftver/program alkalmazása javasolt a gyors anomália-detektálás érdekében.
7. A naplóállományok adattartalmába az informatikuson/rendszergazdán túl betekinthetnek: az IBF és vagy az IBF által írásban felhatalmazott munkatárs, a szervezet vezetőjének írásban kiadott engedélyével.

5.4.2. Technikai követelmények

Az elektronikus információs rendszer:

- Naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek.
- Elvégzi a meghatározott végrehajtandó tevékenységeket (pl. rendszer leállítása, legrégebbi naplóbejegyzések felülírása, naplózási folyamat leállítása).
- Belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához.

- Időbélyegeket rögzít a naplóbejegyzésekben UTC vagy GMT szerint, megfelelve a szervezet által meghatározott időmérési pontosságnak.

5.4.3. Naplózható események

A szervezet:

- Meghatározza az a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét.
- Egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel.
- Megvizsgálja, hogy a naplózható események megfelelőek-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

5.4.4. Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédje a naplóinformációkat és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

5.4.5. Napló tárkapacitás

A szervezet a naplózásra elegendő méretű tárkapacitást biztosít, figyelembe véve a biztonsági osztályba sorolásból következő naplózási funkciókat és a 1 év megőrzési időt kell biztosítani.

5.4.6. Naplózási hiba kezelése

Az elektronikus információs rendszer:

- Naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek.
- Elvégzi a meghatározott végrehajtandó tevékenységeket (pl. rendszer leállítása, legrégebbi naplóbejegyzések felülírása, naplózási folyamat leállítása).

5.4.7. Naplóvizsgálat és jelentéskészítés

A szervezet:

- Rendszeresen felülvizsgálja és elemzi az előre meghatározott naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából, automatizált eszközök alkalmazásával.

Az elemzés eredményeiről jelentést készít ***„N04.1.2 Naplóelemzés jelentés"***.

- Jelenti a feltárt problémákat a meghatározott személyeknek vagy szerepköröknek.
- Legalább éves rendszerességgel független audit keretében ellenőrzi a naplózási rendszer megfelelőségét és hatékonyságát.

5.5. Kártékony kódok elleni védelem

A szervezet az alábbi intézkedéseket alkalmazza a kártékony kódok elleni védelem érdekében, figyelembe véve a követelményeket:

5.5.1. Általános védelmi intézkedések

- A szervezet számítógépes hálózatát, szervereit és munkaállomásait folyamatosan, illetve felhasználói jelzés alapján vírusvédelmi szempontból figyelni kell. A vírusfertőzés ellenőrzéséről és annak eredményéről nyilvántartást kell vezetni.

- A preventív vírusvédelmet, a tartalom- és spamszűrést és a hálózat határvédelmet hardvereszközök és szoftver/program megoldások biztosítják. Ezek kiszűrik a vírusos üzeneteket, a kéretlen leveleket, valamint letiltják meghatározott weblapok megnyitását.
- A honlapok megnyitásának korlátozását elsősorban a Nemzeti Kibervédelmi Intézet (GovCERT-Hungary) által közzétett tiltólistákból, másodsorban helyi tiltólistákból kell előállítani.
- A **hálózat** határvédelemi eszközeinek működését folyamatosan ellenőrizni kell, a rendszer elemeinek frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell, hiba esetén automatizált riasztási mechanizmusokat alkalmazni.

A szervezetben a hálózat határvédelmi, illetve vírusvédelmi funkciókat az ***„N13 Biztonságtervezési szabályzat"-ban*** felsorolt szoftver/programok valósítják meg.

5.5.2. Felhasználói kötelezettségek

- Valamennyi felhasználónak kötelessége minden tőle telhetőt megtenni annak érdekében, hogy rosszindulatú kódot vagy tartalmat tartalmazó fájl ne kerüljön fel a munkaállomásokra, hordozható számítógépekre vagy a hálózati adattárolókra.
- A felhasználóknak tilos a vírusvédelmi alkalmazások működését leállítani.
- A felhasználónak tilos vírusirtót, személyes tűzfalat vagy egyéb biztonsági szoftver/programot önállóan telepíteni.
- Külső helyekről származó adattárolókat csak szervezeti okból szabad használni és a használat előtt vírusellenőrzésnek kell alávetni.
- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesíteni kell az informatikus/rendszergazdat.

5.5.3. Technikai védelmi intézkedések

- A határvédelmi szoftvereknek/programoknak folyamatosan kell működniük, vizsgálva a bejövő és kimenőhálózatforgalmat.
- A vírusvédelemnek a klienseken rezidens módon kell futnia, rendszeres időközönként automatikus vírusellenőrzést végrehajtva.
- A vírusvédelemnek ki kell terjednie a fájlokra, rendszeradatokra, hálózati elemekre, web- és email forgalomra.
- A határvédelmi rendszer elemeinek frissítéséről automatizált módszerrel kell gondoskodni, a frissítések sikerességét ellenőrizni kell.
- Fejlett végpontvédelmi megoldásokat (EDR - Endpoint Detection and Response) kell alkalmazni a kifinomult támadások észlelésére és elhárítására.

5.5.4. Incidenskezelés

- Vírusfertőzés gyanúja esetén az informatikus/rendszergazda és vagy az IBF a fertőzött gépet izolálja, annak használatát a hiba elhárításáig felfüggeszti.
- Az incidenskezelési folyamatnak ki kell terjednie a kártékony kódok által okozott incidensek gyors 24 órán belül jelentésére az hatóságfelügyeleti jogot gyakorló szerv részére, a jogszabály követelményeinek megfelelően.

5.5.5. Rendszeres felülvizsgálat és fejlesztés

- A kártékony kódok elleni védelmi rendszert legalább évente felül kell vizsgálni és szükség esetén fejleszteni kell.
- A felülvizsgálatnak ki kell terjednie az új típusú fenyegetések elleni védekezési képességek értékelésére és fejlesztésére.
- Rendszeres (legalább éves) penetrációs teszteket kell végezni a védelmi rendszer hatékonyságának ellenőrzésére.

5.6. Hibajavítás, biztonsági frissítések

A szervezet által használt szoftver/programok hibáinak napvilágra kerülése esetén számítani lehet arra, hogy az ártó szándékú támadók ezeket a biztonsági réseket kihasználva próbálnak az információs rendszerbe behatolni, ezért elengedhetetlen, hogy a szoftver/programgyártója által készített javítások (frissítések) a lehető leghamarabb telepítésre kerüljenek. A szervezet informatikus/rendszergazda a fentiek megvalósulása érdekében az alábbi intézkedéseket teszi, figyelembe véve a követelményeket:

5.6.1. Hibák azonosítása és jelentése

- Azonosítja az elektronikus információs rendszer hibáit belső eljárásrendje alapján.
- A feltárt hibákat haladéktalanul jelenti a megfelelő belső fórumoknak és szükség esetén a hatóságfelügyeleti jogot gyakorló szerv részére, összhangban a jogszabály által meghatározott 24/72 órás jelentési kötelezettségével.
- Rendszeres sebezhetőségi vizsgálatokat végez a potenciális biztonsági rések proaktív feltárása érdekében.

5.6.2. Hibajavítás és frissítések kezelése

- Kijavítja vagy kijavíttatja az azonosított hibákat, prioritást adva a kritikus rendszernek.
- Telepítés előtt teszteli a hibajavítással kapcsolatos szoftver/program frissítéseket az érintett szervezeti egység feladatellátásának hatékonysága és a szóba jöhető negatív hatású következmények szempontjából.
- A teszteléshez elkülönített tesztkörnyezet)et kell használni, amely reprezentatív a valós működési környezetre.

5.6.3. Kritikus frissítések kezelése

A biztonságkritikus szoftver/programokat a frissítésük kiadását követően a lehető legrövidebb időn belül, de legkésőbb 14 napon belül telepíti vagy telepítteti.

Sürgős esetekben (pl. aktívan kihasznált sebezhetőségek) gyorsított eljárást alkalmaz a frissítések azonnali telepítésére.

5.6.4. Konfigurációkezelés

- Beépíti a hibajavítást a funkciók kezelési folyamatba, biztosítva a változások nyomon követhetőségét.
- Dokumentálja az összes végrehajtott frissítést és hibajavítást, beleértve a telepítés időpontját és a felelős személyt.

5.6.5. Automatizálás és monitoring

- Ahol lehetséges, automatizált frissítési mechanizmusokat alkalmaz a gyors és konzisztens hibajavítás érdekében.
- Folyamatosan monitorozza a frissítések sikerességét és hatékonyságát.

5.6.6. Rendszeres felülvizsgálat

- Legalább negyedévente felülvizsgálja a hibajavítási és frissítési folyamatokat, biztosítva azok hatékonyságát és a jogszabályi követelményeknek való megfelelést.
- Az felülvizsgálat eredményeit dokumentálja és szükség esetén fejleszti a folyamatokat.

5.6.7. Képzés és tudatosítás

- Rendszeres képzéseket tart az informatikai személyzet számára a legújabb hibajavítási és frissítési gyakorlatokról.
- Tudatosító oktatásokat szervez a felhasználók számára a frissítések fontosságáról.

6. Rendszer- és kommunikációvédelem

6.1. Rendszer- és kommunikációvédelmi eljárásrend

A szervezet a következő intézkedéseket teszi a rendszer- és kommunikációvédelem érdekében, figyelembe véve az kritikus biztonsági követelményeit:

Eljárásrend kidolgozása és dokumentálása

- Megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja a rendszer- és kommunikációvédelmi eljárásrendet.

Az eljárásrend tartalmazza a rendszer- és kommunikációvédelmi szabályzatot ***(„N17 Rendszer- és kommunikációvédelmi szabályzat")*** és az ahhoz kapcsolódó ellenőrzések megvalósítását segítő elemeket.

A részletes szabályozást az ***„N17.1 Rendszer- és kommunikációvédelmi eljárásrend"*** c. eljárásrend tartalmazza.

Kihirdetés és hozzáférhetőség

- Az eljárásrendet kihirdeti a szervezeten belüli szabályozásában meghatározott személyek vagy szerepkörök számára.
- Biztosítja, hogy az eljárásrend könnyen hozzáférhető legyen az érintett munkatársak számára, például belső hálózati tárhelyen vagy dokumentumkezelő rendszerben.

Rendszeres felülvizsgálat és frissítés

- A rendszer- és kommunikációvédelmi eljárásrendet vagy más belső szabályozásában meghatározott gyakorisággal, de legalább évente felülvizsgálja és frissíti.
- A felülvizsgálat során figyelembe veszi a technológiai változásokat, új fenyegetéseket és a jogszabályi előírások esetleges módosulásait.

Felelősségi körök meghatározása

- Egyértelműen definiálja a rendszer- és kommunikációvédelemmel kapcsolatos felelősségi köröket és szerepeket a szervezeten belül.

- Kijelöl egy felelős személyt vagy csoportot az eljárásrend karbantartására és végrehajtásának felügyeletére.

Oktatás és tudatosítás

- Rendszeres képzéseket tart a munkatársak számára a rendszer- és kommunikációvédelem fontosságáról és az eljárásrend betartásáról.
- Tudatosító programokat indít a felhasználók számára a biztonságos kommunikációs gyakorlatokról.

Megfelelőség ellenőrzése

- Rendszeres belső auditokat végez az eljárásrend betartásának ellenőrzésére.
- Legalább kétévente független külső auditot végeztet a jogszabály követelményeknek való megfelelés értékelésére.

Incidenskezelés és jelentés

- Részletes eljárásokat dolgoz ki a rendszer- és kommunikációvédelmet érintő incidensek kezelésére.
- Biztosítja a gyors reagálást és a 24/72 órán belüli jelentéstételt a hatóságfelügyeleti jogot gyakorló szerv részére, incidensek esetén.

Technológiai megoldások

- Meghatározza és dokumentálja a rendszer- és kommunikációvédelem biztosításához használt technológiai megoldásokat (pl. tűzfalak, titkosítási eszközök, VPN-ek).
- Rendszeresen felülvizsgálja és frissíti ezeket a megoldásokat a változó fenyegetettségi környezetnek megfelelően.

Együttműködés és információmegosztás

- Kialakítja az együttműködés és információmegosztás csatornáit más szervezetekkel és hatóságokkal felügyeleti jogot gyakorló szerv a rendszer- és kommunikációvédelem területén.
- Részt vesz releváns szakmai fórumokon és információmegosztó platformokon.

Kockázatértékelés és -kezelés

- Az eljárásrendbe beépíti a rendszeres kockázatértékelés és -kezelés folyamatát, különös tekintettel a rendszer- és kommunikációvédelmi aspektusokra.
- A kockázatértékelés eredményeit felhasználja az eljárásrend és a védelmi intézkedések fejlesztésére.

6.2. Határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A zónák közötti kommunikáció csak szabályozott formában, határvédelmi rendszer beiktatásával biztosítható. Jelen fejezetben rögzített szabályok betartása alapvető követelmény, megszegése súlyos biztonsági eseménynek tekintendő.

6.2.1. Vezeték nélküli technológiák szabályozása

A szervezet belső szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán, valamint engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

6.2.2. Alapvető szabályok és védelmi intézkedések

- A különböző zónák (pl. intranet -> internet) közötti kommunikáció tűzfal által kontrollált. Emellett fejlett behatolás-észlelő és -megelőző rendszereket (IDS/IPS) kell implementálni a határvédelem megerősítésére.
- Ha egy kommunikációs csatorna nincs külön engedélyezve, az tiltott.
- Az egyes hálózati zónák közötti kapcsolat létrehozásakor az alábbiakat kell figyelembe venni:
- A kapcsolat legyen megfelelő erősségű titkosítással biztosítva;
- A kapcsolat legyen megfelelő erősségű azonosítási algoritmussal ellátva.
- A kapcsolat megvalósításához ajánlott technológiák (ebben a sorrendben):
- VPN kapcsolat kiépítése
- SSL/TLS kapcsolat kiépítése
- Egyedi, titkosított és azonosított kapcsolat kiépítése
- Automatizált fenyegetés-intelligencia megoldásokat kell bevezetni a határvédelmi rendszerek naprakész védelmének biztosítására.

6.2.3. Tűzfal konfiguráció és karbantartás

- Az alkalmazott tűzfal beállításainak meghatározása a rendszergazda hatáskörébe tartozik, melyet az IBF véleményezhet.
- A tűzfal-funkció módosításának igényét, valamint annak jóváhagyását és végrehajtását dokumentálni kell.
- A módosítás végrehajtása a kijelölt rendszergazda feladata.
- A határvédelmi rendszerek funkcióját, módosításait és incidenseit részletesen dokumentálni kell, és rendszeres auditnak kell alávetni.

6.2.4. Nyilvános rendszerelemek elkülönítése

A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső szervezeti hálózattól.

6.2.5. Folyamatos ellenőrzés, frissítés és kockázatértékelés

- A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni!
- Legalább évente egyszer átfogó kockázatértékelést kell végezni a határvédelmi rendszerekre vonatkozóan, figyelembe véve az új fenyegetéseket és sebezhetőségeket.
- Évente legalább egyszer külső szakértők bevonásával penetrációs teszteket kell végezni a határvédelmi rendszerek hatékonyságának ellenőrzésére.

6.2.6. Incidenskezelés és jelentés

A határvédelmi rendszereket érintő kritikus incidenseket 24 órán belül jelenteni kell az hatóság felügyeleti jogot gyakorló szerv részére, összhangban a jogszabály követelményekkel.

6.2.7. Képzés és tudatosítás

Rendszeres képzéseket kell tartani a határvédelemért felelős személyzet számára a legújabb fenyegetésekről és védelmi technikákról.

6.2.8. Kriptográfiai kulcsok előállítása és kezelése

Az elektronikus információs rendszer szabványos, a jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg. A követelményeiknek megfelelően a szervezet az alábbi intézkedéseket alkalmazza:

6.2.9. Kriptográfiai műveletek

- Csak olyan kriptográfiai algoritmusokat és protokollokat használ, amelyek megfelelnek a hatályos magyar és európai uniós jogszabályoknak és szabványoknak.
- Rendszeresen felülvizsgálja és szükség esetén frissíti a használt kriptográfiai megoldásokat, figyelembe véve a legújabb biztonsági ajánlásokat és fenyegetéseket.
- A kriptográfiai kulcsok generálásához megfelelő entrópiaforrást használ, biztosítva a kulcsok véletlenszerűségét és erősségét.

6.2.10. Kulcskezelés

- Kidolgoz és alkalmaz egy átfogó kulcskezelési eljárásrendet, amely kiterjed a kulcsok generálására, tárolására, elosztására, visszavonására és megsemmisítésére.
- A kriptográfiai kulcsokat biztonságos, hardveres kulcstárolókban (HSM - Hardware Security Module) tárolja, különösen a kritikus rendszerek esetében.
- Rendszeres időközönként (legalább évente) elvégzi a kulcsok rotációját, csökkentve a kompromittálódás kockázatát.
- Többfaktoros hitelesítést alkalmaz a kulcsokhoz való hozzáférés során.

6.2.11. Távoli eszközök kezelése

Az elektronikus információs rendszer meggátolja az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a szervezet engedélyezte azt, és közvetlen jelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél. Ennek érdekében:

- Technikai megoldásokat implementál az eszközök nem engedélyezett távoli aktiválásának megakadályozására.
- Vizuális vagy hangjelzést alkalmaz az eszközök aktiválásakor, biztosítva a felhasználók azonnali tájékoztatását.
- Rendszeres auditot végez a távoli eszközök használatáról és az aktiválási eseményekről.

6.2.12. Folyamatok elkülönítése

Az elektronikus információs rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára. Ennek megvalósítása érdekében:

- Virtualizációs vagy konténertechnológiákat alkalmaz a folyamatok izolálására.
- Rendszeres biztonsági ellenőrzéseket végez a folyamatok elkülönítésének hatékonyságára vonatkozóan.
- Monitorozza és naplózza a folyamatok közötti esetleges nem engedélyezett interakciókat.

6.2.13. Képzés és tudatosítás

Rendszeres képzéseket tart a kriptográfiai megoldásokért felelős személyzet számára a legújabb technológiákról és biztonsági gyakorlatokról. Tudatosító oktatásokat szervez a felhasználók számára a biztonságos kriptográfiai gyakorlatok alkalmazásáról.

6.2.14. Incidenskezelés és jelentés

Kriptográfiai incidensek (pl. kulcs kompromittálódás) esetén azonnali intézkedési tervet alkalmaz. A kritikus kriptográfiai incidenseket 24 órán belül jelenti az hatóság felügyeleti jogot gyakorló szerv részére, összhangban a jogszabály követelményekkel.

6.2.15. Dokumentáció és audit

Részletes dokumentációt vezet a kriptográfiai megoldásokról, kulcskezelési eljárásokról és funkciókról. Rendszeres (legalább éves) független auditot végeztet a kriptográfiai rendszerek és gyakorlatok megfelelőségének ellenőrzésére.

6.3. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer a hitelesítés szolgáltatók tanúsítványainak elfogadása során a következő intézkedéseket alkalmazza:

6.3.1. Elfogadott tanúsítványok

Az elektronikus információs rendszer kizárólag a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el a szervezeten kívüli felhasználók hitelesítéséhez.

A rendszer rendszeresen (legalább havonta) ellenőrzi és frissíti az elfogadott hitelesítés szolgáltatók listáját az NMHH nyilvántartása alapján.

6.3.2. Kriptográfiai modulok hitelesítése

Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

A kriptográfiai modulok hitelesítési mechanizmusait rendszeresen (legalább évente) felülvizsgálja és szükség esetén frissíti a szervezet.

6.3.3. Tanúsítványok kezelése

A rendszer automatikusan ellenőrzi a beérkező tanúsítványok érvényességét, beleértve a lejárati dátumot és a visszavonási státuszt. Implementál egy tanúsítvány-visszavonási lista (CRL) vagy online tanúsítvány-állapot protokoll (OCSP) alapú ellenőrzési mechanizmust.

6.3.4. Naplózás és monitorozás

A rendszer naplózza a tanúsítványokkal kapcsolatos összes műveletet, beleértve az elfogadást, elutasítást és letiltott belépési - hitelesítési kísérleteket. Rendszeres (legalább heti) ellenőrzést végez a naplófájlokban a gyanús tevékenységek azonosítása érdekében.

6.3.5. Incidenskezelés

A szervezet kidolgoz és alkalmaz egy eljárásrendet a tanúsítványokkal kapcsolatos biztonsági incidensek kezelésére. A kritikus incidenseket 24 órán belül jelenti a hatóságfelügyeleti jogot gyakorló szerv részére.

6.3.6. Oktatás és tudatosítás

Rendszeres képzést biztosít a rendszer adminisztrátorok és biztonsági személyzet számára a tanúsítványkezelés és a kapcsolódó biztonsági kérdések feladatkörében.

Tudatosító oktatásokat szervez a felhasználók számára a biztonságos tanúsítvány használatról.

6.3.7. Dokumentáció és felülvizsgálat

Részletes dokumentációt vezet a tanúsítványkezelési folyamatokról és funkciókról.

Évente felülvizsgálja és szükség esetén frissíti a tanúsítványkezelési eljárásokat és szabályzatokat.

6.3.8. Biztonságos név/cím feloldó szolgáltatások

Az elektronikus információs rendszer a név/cím feloldási szolgáltatások terén a következő intézkedéseket alkalmazza:

6.3.9. Kiegészítő adatok biztosítása

A név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít. Amennyiben a rendszer egy elosztott, hierarchikus névtár részeként működik, jelzi az utódtartományok biztonsági állapotát. Támogatja és hitelesíti az utód- és elődtartományok közötti bizalmi láncot, amennyiben azok támogatják a biztonságos feloldási szolgáltatásokat.

6.3.10. Biztonságos feloldási szolgáltatás

Az elektronikus információs rendszer eredet hitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra. Implementál rekurzív vagy gyorsítótárat használó feloldást a biztonságos név/cím feloldó szolgáltatás érdekében. Rendszeresen (legalább havonta) ellenőrzi és frissíti a gyorsítótárban tárolt adatokat a pontosság és aktualitás biztosítása érdekében.

6.3.11. Architektúra és tartalékok

Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást a szervezet számára, hibatűrő kialakítással rendelkeznek. A szervezet megvalósítja a belső és külső szerepkörök szétválasztását a név/cím feloldási szolgáltatások terén.

Redundáns név/cím feloldó szervereket alkalmaz a szolgáltatás folyamatos elérhetőségének biztosítása érdekében.

6.3.12. Biztonsági intézkedések

Implementál DNSSEC (Domain Name System Security Extensions) protokollt a DNS-lekérdezések és -válaszok integritásának és eredetiségének biztosítására. A szervezet alkalmaz DNS-over-HTTPS (DoH) vagy DNS-over-TLS (DoT) protokollt a DNS-lekérdezések titkosítására.

Rendszeresen vizsgálni kell (legalább negyedévente) és frissíteni kell a DNS-protokollokat szoftver/programokat és funkciókat a legújabb biztonsági javítások alkalmazása érdekében.

6.3.13. Monitorozás és naplózás

Folyamatosan monitorozza a név/cím feloldó szolgáltatások működését és teljesítményét.

A szervezet naplózza a DNS-lekérdezéseket és -válaszokat, különös tekintettel a gyanús vagy anomális tevékenységekre. Rendszeresen (legalább hetente) elemzi a naplófájlokat a potenciális biztonsági fenyegetések azonosítása érdekében.

6.3.14. Incidenskezelés

A szervezet kidolgoz és alkalmaz egy eljárásrendet a név/cím feloldó szolgáltatásokkal kapcsolatos biztonsági incidensek kezelésére.

Biztosítja a gyors reagálást és a 24 órán belüli jelentéstételt a hatóság felügyeleti jogot gyakorló szerv részére, incidensek esetén.

6.3.15. Oktatás és tudatosítás

Rendszeres képzést biztosít a rendszeradminisztrátorok számára a biztonságos név/cím feloldó (szolgáltatások konfigurálásáról és karbantartásáról. Tudatosító oktatásokat szervez a felhasználók számára a biztonságos DNS-használat fontosságáról.

6.3.16. Dokumentáció és felülvizsgálat

A szervezet részletes dokumentációt vezet a név/cím feloldó szolgáltatások funkciójáról és működéséről. Évente felülvizsgálja és szükség esetén frissíti a név/cím feloldó szolgáltatásokkal kapcsolatos eljárásokat és szabályzatokat.

6.4. Túlterheléses (szolgáltatás megtagadás alapú) támadás elleni védelem

Az elektronikus információs rendszer a következő intézkedéseket alkalmazza a túlterheléses szolgáltatás megtagadás jellegű támadásokkal szembeni védelem érdekében, figyelembe véve a jogszabályban meghatározott követelményeit:

6.4.1. Védelmi intézkedések

Túlterheléses támadások azonosítása:

- A rendszer folyamatosan monitorozza a forgalmat, észlelve a gyanús aktivitásokat, amelyek túlterheléses támadásra utalhatnak.
- Implementálja a forgalom-elemző eszközöket, amelyek képesek azonosítani a normálistól eltérő mintákat.

Biztonsági intézkedések bevezetése:

- Bevezetésre kerülnek tűzfalak és behatolás-észlelő rendszerek (IDS/IPS), amelyek képesek blokkolni a gyanús forgalmat.
- A rendszer terheléselosztókat alkalmaz a forgalom elosztására, csökkentve ezzel a célzott erőforrások terhelését.

Korlátozások alkalmazása:

- A szolgáltatás megtagadásos támadások hatásainak korlátozása érdekében előre meghatározott biztonsági intézkedéseket kell bevezetni, például:
- Korlátozott számú kérések fogadása egy adott időszak alatt (rate limiting).
- IP-címek ideiglenes blokkolása, ha azok gyanús aktivitást mutatnak.

6.4.2. Incidenskezelési eljárás

Incidens jelentése:

- Túlterheléses támadás gyanúja esetén azonnal értesíteni kell az informatikai vezetőt és az incidenskezelő csoportot (CSIRT).
- A támadás részleteit és a válaszlépéseket dokumentálni kell.

Gyors reagálás:

- Az incidenskezelő csoport azonnali intézkedéseket hoz a támadás elhárítására, beleértve a forgalom blokkolását vagy átirányítását.
- A támadás során szerzett tapasztalatokat értékelni kell a jövőbeli védekezési stratégiák fejlesztése érdekében.

6.4.3. Rendszeres felülvizsgálat

Védelmi intézkedések hatékonyságának ellenőrzése:

- Rendszeresen (legalább negyedévente) felül kell vizsgálni a túlterheléses támadások elleni védelmi intézkedések hatékonyságát.
- Az auditok során azonosított hiányosságokat észlelve szükség esetén javító intézkedéseket kell hozni.

Frissítések és fejlesztések:

- A védelmi rendszerek szoftver/programokat és funkcióit rendszeresen frissíteni kell, hogy az adott rendszer védett legyen a legújabb fenyegetésekkel szemben.
- Rendszeresen értékelni kell a legújabb technológiákat és megoldásokat, amelyek javíthatják a védekezési képességeket.

6.4.4. Képzés és tudatosítás

Felhasználói tudatosság növelése:

- Rendszeres oktatásokat kell tartani a felhasználók számára a túlterheléses támadásokkal kapcsolatos ismeretekről és megelőzési technikákról.
- Tudatosító oktatásokat biztosít a felhasználók számára arról, hogyan ismerhetik fel gyanús tevékenységeket, amelyeket jelenteniük kell.

6.4.5. Dokumentáció

Naplózás és jelentéskészítés:

- Minden túlterheléses támadással kapcsolatos eseményt naplózni kell, beleértve a válaszlépéseket is.
- Évente jelentést készít az incidensek kezeléséről és az alkalmazott védelmi intézkedések hatékonyságáról.

7. Biztonsági besorolás

Adatbiztonság szempontjából a szervezet kezelésében lévő EIR-eket, elektronikus formában tárolt információkat, eszközöket, erőforrásokat és szolgáltatásokat a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából a jogszabályban előírt módon – a kockázat növekedésével arányosan növekvő - biztonsági osztályokba kell sorolni.

Biztonsági osztályba sorolás és felülvizsgálat

A szervezet EIR-einek biztonsági osztályba sorolását az 1. számú melléklet tartalmazza.

A besorolást évente felül kell vizsgálni, figyelembe véve az új fenyegetéseket és sebezhetőségeket, valamint az elektronikus információs rendszereket érintő változásokat.

A kockázatértékelés eredményeit dokumentálni kell és fel kell használni a biztonsági intézkedések fejlesztésére.

A biztonsági osztályba sorolás során külön figyelmet kell fordítani a jogszabály által meghatározott kritikus rendszerek azonosítására, amelyekre speciális védelmi intézkedéseket kell alkalmazni.

A szervezet jellemzői és adatkezelése

A szervezet vagy szervezeti egység szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt.

A szervezet közérdekből nyilvános adatokat kezel, valamint közérdekből nem nyilvános adatokat is kezel; minősített adatokat kezel és szervezetei érdekből bizalmas adatokat kezel.

Incidenskezelés és jelentési kötelezettség

A magasabb biztonsági osztályba sorolt rendszereket érintő incidenseket 24 órán belül jelenteni kell az hatóság felügyeleti jogot gyakorló szerv részére.

Dokumentáció és audit

Évente független auditot kell végezni a biztonsági osztályba sorolás megfelelőségének ellenőrzésére.

A biztonsági osztályba sorolás folyamatát és eredményeit részletesen dokumentálni kell.

Képzés és tudatosítás

A munkatársakat rendszeresen képezni kell a megállapított biztonsági osztály a felhasználókra vonatkozó előírásiról, azok be nem tartása esetén alkalmazható jogkövetkezményekről.

Tudatosító oktatásokat kell szervezni a biztonsági osztályoknak megfelelő adatkezelési gyakorlatokról.

Biztonsági osztályba sorolás

A szervezet valamennyi EIR-je a Kibertv. alapján meghatározott kritériumok szerint az alap biztonsági osztályba került besorolásra.

Vácduka, 2025. június 19.

Hegyi Ágnes
Jegyző
Jóváhagyó

Várfi András IBF

N01 Információ Biztonsági Szabályzat 1. sz melléklete **EIR-ek biztonsági osztályba sorolása**

	Szolgáltatások		Biztonsági osztály	RTO tolerálható kiesési idő	Bizalmasság	Sértetlenség	Rendelkezésre állás
	Elektronikus Információs Rendszerek (EIR)	**Tartalom – feladatellátás -funkció**					
1	Irodai és ügyviteli rendszerek	**Tartalom:** dokumentumkezelés, táblázatkezelés, szövegszerkesztés, nyilvántartások, adat-előkészítés **Funkció:** az adat-előállítás és -feldolgozás a szervezet munkaeszközein	Alap	8 óra	3	3	3
2	Testület feladatellátást támogató rendszerek	**Funkció:** a zárt és nyilvános testületi ülések szavazási, nyilatkozati, és vagy közzétételi, közmegjelenítési rendszerei	Alap	8 óra	3	3	3
3	Működéstámogató rendszerek	**Tartalom:** hálózati eszközök, informatikai rendszer működésének biztosítása **Funkció:** a háttérrendszerek és infrastruktúra technikai működését felügyelő vagy automatikusan kommunikáló EIR-ek	Alap	4 óra	3	3	3