NYÍRŐ GYULA ORSZÁGOS PSZICHIÁTRIAI ÉS ADDIKTOLÓGIAI INTÉZET
mb. főigazgató: Dr. Ézsi Robin
1135 Budapest, Lehel utca 59.
Telefon:(1) 451 2600
https://nyiro.euintezmeny.hu

Iktatószám: O/1241-1/2024

SZ-02

Informatikai Biztonsági Szabályzat

06. kiadás

2024.10.17.

Készítette:

Medgyessy Zsolt
információbiztonsági felelős

Kiadás előtt ellenőrizte:

Nyiri Katalin
minőségügyi vezető

Jóváhagyta és a kiadást elrendelte:

Dr. Ézsi Robin
mb. főigazgató

Tartalomjegyzék

1. Általános rendelkezések

1.1. A szabályozás célja

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja a **Nyírő Gyula Országos Pszichiátriai és Addiktológia Intézet** (továbbiakban: Intézet) által használt elektronikus információs rendszer, alkalmazások és szolgáltatások, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szabványos, szabályozott és egységes biztosítása, illetve a kapcsolódó jogszabályoknak való megfelelés, kiemelten a 2024. december 14.-i (EU) 2022/2555 irányelv (NIS2) valamint a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló a 2023. évi XXIII. törvény a hozzá kapcsolódó hazai szabályozásnak. Az egységesítés érdekében jelen szabályzat keretjelleggel meghatározza mindazokat a normákat és magatartásformákat, amelyek megvalósítják a kockázatokkal arányos, folyamatos és komplex információvédelmet az információs rendszer (a továbbiakban: rendszer) fizikai, adminisztratív és logikai védelmi területén (ahol ez értelmezhető, az informatikai rendszerre szűkítve). Az IBSZ általános célja, hogy az Intézet által használt és működtetett rendszer biztonságát garantáló eljárásokat és előírásokat átlátható és nyomon követhető formában egységes keretbe foglalva rögzítse az informatikai biztonság magasabb fokú kialakításának további szabályozása érdekében. Az IBSZ kiadásának célja továbbá:

- a NIS2 irányelvet átültető a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló a 2023. évi XXIII. törvényhezirányelvhez kapcsolódó magas szintű kiberbiztonságot biztosító intézkedések bevezetése,
- az Intézet által használt rendszer alkalmazásának és felhasználásának biztonsági szempontból történő szabályozása,
- a rendszerekben kezelt személyes adatok védelme,
- a megfelelő adatbiztonság kialakítása,
- a hozzáférési jogok meghatározása, az adatállományok épségének megőrzése,
- az alkalmazott rendszerek nyilvántartásának meghatározása.

1.2. A szabályzat hatálya

1.2.1. A szabályzat személyi hatálya

Az IBSZ hatálya kiterjed az Intézet által alkalmazott valamennyi rendszert működtető, azon adatkezelést, adatfeldolgozást végző, a rendszert felhasználó valamennyi személyre és szervezetre, így különösen az Intézet valamennyi munkavállalójára, illetve munkavégzés céljából egyéb jogviszonyban álló természetes és jogi személyre, szervezetre.

1.2.2. A szabályzat tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

- az Intézet üzemeltetésében lévő vagy érdekkörében üzemeltetett teljes informatikai infrastruktúrára, így a rendszer teljes konfigurációjára, az ahhoz tartozó rendszer- és felhasználói szoftverekre, valamint ezek dokumentációira;
- az informatikai működést biztosító informatikai és telekommunikációs hálózatra;
- a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után számítógépes adathordozókon tárolt, a feldolgozás eredményeként létrejött adatra;
- a számítástechnikai eszközök alkalmazásának teljes folyamatára, tevékenységeire;

– a számítástechnikai infrastruktúra elhelyezésére szolgáló helyiségekre.

Az IBSZ rendelkezéseit alkalmazni kell a külső helyszínen történő munkavégzéshez használt eszközökre is, amennyiben azok az IBSZ tárgyi hatálya alá tartoznak.

1.3. A szabályzattal kapcsolatos feladatok

A szabályzattal kapcsolatos feladatokat és felelősségeket az alábbi táblázat szemlélteti:

Feladat	*Felelős*	*Konzultensek*	*Tájékoztatandók*
Szabályzat elkészítése, felülvizsgálata és módosítása	Információbiztonsági Felelős (IBF)	szakmai igazgatók, Informatikai Osztályvezető (IOV)	Főigazgató
Szabályzat elfogadása és kihirdetése	Főigazgató (FOIG)		
Szabályzat betartásának ellenőrzése	Információbiztonsági Felelős (IBF)	igazgatók, Informatikai Osztályvezető (IOV)	

I. táblázat — Szabályzattal kapcsolatos feladatok és felelősségek

1.4. Vonatkozó jogszabályok

A védelmet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet, valamint az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 246/2015. (IX. 8.) Korm. rendelet előírásai szerint valósítja meg.

A szabályzat megteremti az Ibtv., a BM rendelet, illetve a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény és a biztonsági osztályba sorolás valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet közötti összhangot, a jogszabályi követelmények közötti átjárhatóságot, ezzel biztosítva a NIS2 irányelv átültetését szólgáló a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló a 2023. évi XXIII. törvény szerinti működés bevezetésével összefüggő kötelezettségek megvalósítását.

Jelen szabályzatban a bekezdések fejezet címe után „()" között a védelmi intézkedések 41/2015. (VII. 15.) BM rendelet szerinti azonosítója; a „[]" zárójelek között a 41/2015. (VII. 15.) BM rendelet {} zárójelben pedig a 7/2024 MK rendelet biztonsági osztály minimális szintje került megadásra. A szabályzatban az egyes információs biztonsági szerepek megnevezésére rövidítések kerülnek alkalmazásra, amelyek definíciója az informatikai biztonsági szervezetet leíró fejezetben található, az

intézet szervezeti és működési szabályzatában meghatározott szervezeti egységekhez és beosztásokhoz való hozzárendeléseiket pedig a jelen szabályzat végén található szerepbeosztási mátrix tartalmazza.

1.5. A szabályzat elkészítése, felülvizsgálata és módosítása

A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az **Információbiztonsági Felelős** (IBF) feladata és felelőssége, együttműködve a főigazgatóval és az informatikai osztály vezetőjével (Informatikai Osztályvezető, IOV). A felülvizsgálatot évente október 31-ig, illetve a szabályzat tekintetében lényeges körülmény változása esetén szükség szerint, de legfeljebb 30 napon belül kell elvégezni (rendkívüli felülvizsgálat). A szabályzat elkészítésében, felülvizsgálatában és módosításában közreműködnek az elektronikus információbiztonsági feladatok ellátásában közreműködő személyek és szervezeti egységek.

1.5.1. Időszaki felülvizsgálat (3.1.1.1.1.2. [1]), {1.1.2}

Az IBSZ-t minden év október 31. napjáig felül kell vizsgálni és szükség esetén módosítani kell. A vizsgálat alapja az ellenőrzések, rendkívüli események naplói, valamint a kockázatelemzés és -kezelés megállapításai.

1.5.2. Rendkívüli felülvizsgálat

Az IBSZ-t az időszakos felülvizsgálaton túl haladéktalanul megkezdett és legfeljebb 30 napon belül elvégzett felülvizsgálatnak kell alávetni és szükség esetén módosítani:

- az IBSZ szerinti feladatok megvalósításában részt vevő szervezeti egységek és személyi felelősök működését, illetve feladatkörét érintő változások esetén;
- súlyos információbiztonsági esemény bekövetkezése esetén; _ az IBSZ-t érintő jogszabályváltozások esetén;
- Az IBSZ hatálya alá tartozó rendszer nagy mértékű változása esetén.

A felülvizsgálatot írásban dokumentálni kell és annak eredményéről az Információbiztonsági Felelős (IBF) tájékoztatja a főigazgatót.

Jelen IBSZ-t 2025. január 31-ig rendkívüli felülvizsgálat keretében a jogszabályi megfelelés biztosítása érdekében felül kell vizsgálni.

1.6. A szabályzat elfogadása és kihirdetése (3.1.1.1.1.1 [1]), {1.1.1}

A szabályzat elfogadása és kihirdetése a főigazgató feladata és felelőssége.

1.7. A szabályzat betartásának ellenőrzése

A szabályzat betartásának ellenőrzése az Információbiztonsági Felelős (IBF) feladata, melyben közreműködnek az információbiztonsági feladatok ellátásában közreműködő személyek, egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős egységek vezetői.

1.8. Kivételkezeléssel kapcsolatos feladatok

Kivétel alatt kell érteni minden olyan technológiai kontroll nem teljesülését, mely a jelen szabályozásban rögzített követelményeket nem tudja teljesíteni.

A Szabályzattól való kivételeket minden esetben az adott rendszer rendszerbiztonsági tervében kell dokumentálni. A kivételek engedélyezésére — az Információbiztonsági Felelős (IBF) álláspontjának ismeretében — a főigazgató jogosult.

A kivételkezelés irányelvei:

- A kivételek meghatározása, a megszüntetésre irányuló terv kidolgozása, annak végrehajtása (megfelelés kialakítása, kiváltás, stb.) az IBF koordinálása mellett az adott rendszer üzemeltetésére kijelölt személy feladata.
- A kivételek megszüntetésére vonatkozóan tervben kell rögzíteni a hiányosságot (szabályzattól való eltérést) és annak tervezett kezelését (akcióterv).
- A kivétel megszüntetése érdekében javító intézkedéseket kell alkalmazni, melyek megfelelőségét és szükségességét a kockázatelemzés során meg kell vizsgálni. Ennek koordinálása az Információbiztonsági Felelős feladata.
- Meg kell szervezni az információs rendszer jogszabálynak való megfelelését, a költséghatékonyság figyelembevételével, szükség esetén a rendszer kiváltásáról gondoskodni kell.
- Új, fejlesztés vagy bevezetés alatt álló (elektronikus) információs rendszer esetén a szabályzati követelmények teljesülésére vonatkozó kivétel nem alkalmazható.

2. Fogalmak meghatározása

Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

Adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi.

Adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik.

Adathordozó: a mágneses, az optikai és egyéb típusú, vagy papír alapú, adatok tárolására alkalmas eszköz.

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adatkezelő: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adatvagyon: minden adat, mely az intézményi eszköznyilvántartásban szereplő hardver eszközökön, illetve mentési vagy mobil adathordozókon van, és az Intézet működéséhez kapcsolódó adatkörhöz tartozik. Az adatvagyon részét képezi:

- operációs rendszerek információi, és beállításai,
- a hardvereken található szoftverek és alkalmazások információi és beállításai,
- maguknak a szoftvereknek a felhasználási joga,
- a szoftverek és applikációk által előállított kimeneti adatok (képernyő, nyomtatás, fájl, email),
- a szoftverek és applikációk által előállított és (bármely formában és bárhol) tárolt fájlok.

Alapvető szolgáltatásokat nyújtó szolgáltató: a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 2/A. alapján kijelölt szolgáltató. Az Intézet alapvető szolgáltatásokat nyújtó szolgáltatónak minősül.

Azonosítás: az a folyamat, melynek során a felhasználó a rendszerben szereplő identitását nyilvánítja ki a felhasználói azonosító segítségével; (legjobb gyakorlat alapján).
Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

Biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

Biztonsági szint: a szervezet felkészültsége az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére; biztonsági szintbe sorolás: a szervezet felkészültségének meghatározása az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

BYOD eszközök: a felhasználó saját tulajdonában álló, a munkakörébe tartozó feladatainak elvégzése érdekében az Intézet erőforrásaihoz helyi (nem távoli) módon kapcsolódó eszközök.

Elektronikus információs rendszer: egy elektronikus információs rendszernek kell tekinteni az adott adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttesét; Elektronikus információs rendszer:

a) az elektronikus hírközlésről szóló 2003. évi C. törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre.

Felhasználói fiók: a felhasználói fiók segítségével a felhasználó autentikálhatja (hitelesítheti) magát a rendszer szolgáltatásai felé, és autorizációt (engedélyt) nyerhet az azokhoz való hozzáférésre.

Autentikáció (hitelesítés): a hitelesítés folyamat, arra szolgál, hogy egy egyed (felhasználó, program, számítógép) bizonyítsa az önmaga identitását; (legjobb gyakorlat alapján).

Autorizáció (engedélyezés): a jogosultságellenőrzés során az dől el, hogy az adott felhasználónak az adott erőforráshoz milyen típusú hozzáférése van; (legjobb gyakorlat alapján).

Hordozható informatikai eszköz: olyan informatikai eszköz, amely egyik helyről könnyen elvihető másik helyre, ott azonnal üzembe helyezhető, illetve mobil (azaz mozgás közben is használható; (legjobb gyakorlat alapján) informatikai eszköz: minden olyan eszköz és ennek funkcionális tartozéka, amely adatok összegyűjtésére, feldolgozására (rendezésére, csoportosítására, kiszámítására), előállítására, tárolására és megjelenítésére, illetve az e tevékenységekkel kapcsolatos adat-átalakításra és adattovábbításra alkalmas; (legjobb gyakorlat alapján).

Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

Információvédelem: az azonosítás, hitelesítés, jogosultság kiosztás, ellenőrzés; valamint a hitelesség és sértetlenség garantálása és a bizonyítékok rendszerének és folyamatának kialakítása terén az informatikai rendszerben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme; (legjobb gyakorlat alapján).

Informatikai biztonság: az informatikai biztonság a védelmi rendszer olyan, az Intézet számára kielégítő mértékű állapota, amikor az informatikai erőforrások bizalmassága, sértetlensége, és rendelkezésre állása sérülésének veszélye minimális; (Muha, Lajos (2008) Az informatikai biztonság egy lehetséges rendszertana. BOLYAI SZEMLE, 17 (4). pp. 137-156. ISSN 14161443).

Alkalmazási rendszerek: a manuális és programozott eljárások összessége; (legjobb gyakorlat alapján).

Jogosultság, hozzáférési jogosultság: az informatikai rendszer védelmi mechanizmusainak azon eleme, amely meghatározza, hogy a kezelésre jogosult egyed (személy, program, folyamat) milyen erőforrást (adatot, adathordozót, szolgáltatást, eszközt) milyen módon kezelhet (olvashat, írhat, módosíthat, törölhet, használhat, illetve ezek kombinációja); (legjobb gyakorlat alapján).

Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

Kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedések kidolgozása.

Kockázatok értékelése: annak megállapítása, hogy a beazonosított kockázatok milyen mértékben befolyásolják az Intézet célkitűzéseit. Az értékelés során meg kell határozni a feltárt kockázati tényezők bekövetkezésének valószínűségét, illetve az Intézetre gyakorolt hatását. Az értékelés eredményét (táblázat, vagy mátrix, vagy leíró formában) mutatja be; (legjobb gyakorlat alapján).

Személyes adat: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Különleges adat: (az Általános Adatvédelmi Rendelet 9. cikk (1) bekezdése, illetve az információs önrendelkezési jogról és az információszabadságról szóló 2011- évi CXII. törvény (Infotv.) 3. 3. pontja szerint) a személyes adatok különleges kategóriáiba tartozó minden adat, különösen a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Genetikai adat: (az Általános Adatvédelmi Rendelet 4. cikk 13. pontja és az Infotv. 3. 3a. pontja szerint) egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered.

Biometrikus adat: (az Általános Adatvédelmi Rendelet 4. cikk 14. pontja és az Infotv. 3. 3b. pontja szerint) egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például a daktiloszkópiai adat.

Egészségügyi adat: (az Általános Adatvédelmi Rendelet 4. cikk 15. pont és az Infotv. 3. 3c. pontja szerint) egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

Bűnügyi személyes adat: (Infotv. 3. 4. pontja szerint) a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetésvégrehajtás intézményénél

keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Kritikus adat: a személyes adat vagy valamely jogszabállyal védett adat.

Létfontosságú információs rendszerelem: az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer elem rendeltetésének megfelelően használható.

Teljes mentés: a rendszer minden adata válogatás nélkül mentésre kerül. A mentési folyamat ezért egyszerű, ellenben sok ideig tart és sok tárterület szükséges hozzá. Amennyiben adataink olyanok, hogy nem változnak túl sűrűn, a gyakori teljes mentés sok fölösleges adat tárolását okozza. Előnye azonban, hogy a visszaállítás viszonylag gyors.

Inkrementális mentés: alkalmazása esetén nem kerül elmentésre minden adat, hanem csak azok, amelyek egy korábbi mentés óta megváltoztak (ekkor a visszaállításhoz több biztonsági mentésre is szükség lehet). Az inkrementális mentésnek két alapvető fajtája van: a kumulatív és a differenciális mentés.

Kumulatív mentés: ezen mentés során mindig az utolsó teljes mentés óta megváltozott adategységek kerülnek elmentésre. A kumulatív mentésekből álló mentési stratégiánál, ha egy adategység valamikor megváltozott, akkor az minden kumulatív mentés alkalmával ismételten mentésre kerül egészen a következő teljes mentésig. A kumulatív mentés gyorsabb a teljes mentésnél és kevesebb helyet is kíván.

Differenciális mentés: a differenciális mentés során csak az utolsó inkrementális mentés óta megváltozott adategységek kerülnek elmentésre. Ha két teljes mentés között több differenciális mentést végzünk, akkor pl. a második differenciális mentés csak az első óta történt változásokat fogja rögzíteni. Ennek köszönhetően maga a mentés folyamata gyorsabbá válik, és esetenként kevesebb helyet foglal el. Hátránya azonban, hogy a visszaállításhoz a legutolsó teljes mentésre, és az azt követő összes differenciális mentésre szükség van. A differenciális mentésnél lassabb és a tárigénye is nagyobb, mint a kumulatív mentés.

Napló: a számítógépen végzett műveletek (felhasználói tevékenység), a gép által küldött hibaüzenetek és/vagy a hálózaton bejövő és kimenő adatok rögzítésére, nyomon követésére szolgáló adatállomány; (legjobb gyakorlat alapján).

Reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele; (Infotv. 3. 12. pontja szerint).

PKI: Public Key Infrastructure - nyilvános kulcsú infrastruktúra. A nyilvános kulcsú infrastruktúra az a rendszer, melynek feladata a digitális aláíráshoz szükséges nyilvános kulcsok létrehozása, kibocsátása, publikálása, menedzselése és visszavonása. A nyilvános kulcsú technológiák segítségével biztosítjuk a rendszerben a következő tulajdonságok meglétét: hozzáférés, hitelesítés, letagadhatatlanság, integritás és bizalmasság.

Vírus: olyan programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, „megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát, károkat és teljes működésképtelenséget okozhat.

Archiválás: a megőrzendő adatok áthelyezése a feldolgozó rendszer tárolójáról egy másik, elkülönített tárolóra, (legjobb gyakorlat alapján).

Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók legyenek.

Visszaállítás: meghibásodás vagy sérülés miatt leállt informatikai szolgáltatás helyreállítása, amely magában foglalja a rendszerek és adatbázisok mentéseinek visszatöltését is. Katasztrófaelhárítás esetén leginkább a gyors, ideiglenes szolgáltatás visszaállítást jelenti, megkülönböztetve a végleges helyreállítástól. (legjobb gyakorlat alapján).

3. Az informatikái biztonság szervezete

A fejezetben csak a Szabályzat hatókörébe tartozó, informatikai biztonsággal összefüggő feladatok, hatáskörök és felelősségek kerülnek meghatározásra.

3.1. Informatikai biztonsági szerepek és felelősségek

Az egyes információs biztonsági szerepek és felelősségek szervezeti szerepekhez rendelése a Szabályzat „Az informatikai biztonsági szerepek megfeleltetése" fejezetében található.

3.1.1. Főigazgató (FOIG)

3.1.1.1. Hatásköre

A szabályzatok és eljárásrendek elfogadása és intézményi szintű kihirdetése és az Információbiztonsági Felelős (IBF) kinevezése, valamint a Cselekvési terv és az ahhoz kapcsolódó költségvetési terv elfogadása.

3.1.1.2. Felelőssége

Az informatikai biztonság személyi és tárgyi feltételeinek, valamint a jogszabályoknak megfelelő működéshez szükséges feltételek biztosítása.

3.1.1.3. Feladatai

A főigazgató, köteles gondoskodni a jogszabályi megfelelésnek a következők szerint:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja az Intézetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
- meghatározza az Intézet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve gondoskodik az IBSZ rendszeres felülvizsgálatáról,
- jóváhagyja a hiányosságok megszüntetésének céljából készített Cselekvési tervet, valamint biztosítja az ezekben foglaltak végrehajtásához szükséges személyi és tárgyi feltételeket,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és az Intézet munkatársai elektronikus információbiztonsági ismereteinek szinten tartásáról,
- rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén biztosítja, hogy az Intézet elektronikus információs rendszereinek biztonsága megfeleljen a jogszabályoknak és alkalmas legyen az azonosított kockázatok elhárítására vagy elfogadható kockázati szintre csökkentésére.
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt (harmadik fél) vesz igénybe, gondoskodik a szerződéses kötelmek teljesüléséről,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért.

3.1.2. Főigazgatói Hivatal vezető

3.1.2.1. Hatásköre

Az információbiztonsággal összefüggő feladatok vonatkozásában irányítási, utasítási, beszámoltatási és ellenőrzési jogkörrel rendelkezik.

3.1.2.2. Feladatai

Az információbiztonsággal kapcsolatos stratégiai tervezési feladatok végrehajtása, az intézeti feladatvégrehajtás felügyelete, ellenőrzési nyomvonalak megfelelőségének biztosítása. A szabályzatban a hatáskörébe sorolt döntési, jóváhagyási, ellenőrzési feladatok elvégzése. Az Informatikai Osztályvezető információbiztonsággal összefüggő tevékenységének beszámoltatása.

3.1.3. Információbiztonsági Felelős (IBF)

Az Ibtv. értelmében az Intézet főigazgatójának az (elektronikus) információs rendszer biztonságáért felelős Információbiztonsági Felelőst kell kineveznie vagy megbíznia. Olyan munkaköri leírást,

többletfeladat megállapodást vagy megbízólevelet szükséges kiadni az IBF részére, mely kifejezetten kitér az Ibtv. 13 (1) — (7) bekezdése szerinti feladatok ellátását érintő személyes felelősségre.

3.1.3.1. Hatásköre

Jogosult bármely elektronikus információs rendszer tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködőtől a biztonsági követelményekről tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához jogosult bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. Jogosult ezen bekért információk és dokumentumok véleményezésére, továbbá véleményezési joga van valamennyi elektronikus információbiztonságot érintő szabályzat tekintetében, továbbá minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az elektronikus információbiztonságra. Feladatai ellátása során az Intézet főigazgatójának (FOIG)és a főigazgatói hivatalvezetőnek közvetlenül adhat tájékoztatást, jelentést.

3.1.3.2. Felelőssége

Az Intézet elektronikus információbiztonságának fenntartása és folyamatos fejlesztése, az informatikai biztonsági irányítási rendszer eseti és rendszeres karbantartása, valamint a jogszabályban előírt adatszolgáltatási és jelentési kötelezettség teljesítése, illetve a folyamatos szakmai kapcsolat fenntartása az érdekeltekkel. A jelentési kötelezettség keretében felelőssége és feladata az Intézet irányító vagy középirányító szerve által működtetett informatikai biztonsággal kapcsolatos elektronikus jelentési/adatgyűjtési rendszerbe való adatbevitel, illetve az ott nyilvántartott intézeti adatok karbantartása, a változások jóváhagyása.

3.1.3.3. Feladatai

Az IBF elsősorban, de nem kizárólagosan az alábbi feladatokat látja el:

- gondoskodik az Intézet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- elvégzi vagy irányítja az előző pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
- előkészíti és gondoskodik az Intézet elektronikus információs rendszereire vonatkozó Informatikai Biztonsági szabályzatának rendszeres felülvizsgálatáról,
- előkészíti az Intézet elektronikus információs rendszereinek biztonsági osztályba sorolását és az Intézet biztonsági szintbe történő besorolását,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából az Intézete tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart az illetékes hatósággal és az eseménykezelő központtal.

Továbbá biztosítja az Ibtv. 13. (5) bekezdésében meghatározott követelmények teljesülését

- az Intézet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők tevékenysége során,

- ha az Intézet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

Az IBF jogosult:

- az IBSZ, valamint a kapcsolódó szabályzatok és jogszabályok megsértésének észlelése esetén az érintettel szemben a szükséges büntetőjogi, szabálysértési, polgári jogi eljárás megindítását vagy munkajogi felelősségre vonását kezdeményezni,
- a rendszer használatával kapcsolatos kirívó, az Intézet működését veszélyeztető szabálysértés észlelése esetén az érintett felhasználói jogosultságát a további intézkedések megtételéig, illetve az eset kivizsgálásához szükséges időtartamban felfüggeszteni.

3.1.4. Informatikai Biztonsági Megbízott (IBM)

Az Informatikai Biztonsági Megbízott az informatikai biztonsági eljárások operatív végrehajtását végzi. Az Informatikai Biztonsági Megbízottat az IBF jelöli ki az Informatikai Osztályvezető javaslatára.

3.1.4.1. Hatásköre

Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, közreműködik az elektronikus információbiztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és javaslatokat tesz a hibák kijavítására. Ezen tevékenysége során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

3.1.4.2. Felelőssége

Gondoskodik az elektronikus információbiztonsági ellenőrzések módszereinek és rendszerének kialakításáról és működtetéséről, valamint részt vesz a katasztrófa-elhárítási terv összeállításában és a működésfolytonosság biztosításában.

3.1.4.3. Feladatai

Mint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy, az alábbiakban segíti és támogatja az IBF munkáját:

- felügyeli a beruházásokat, a fejlesztéseket és az ügyvitelt elektronikus információbiztonsági szempontból,
- munkája során felügyeli és ellenőrzi az elektronikus információbiztonsági követelmények megvalósulását, a szabályzatokban és eljárásrendekben foglaltak szabályszerű végrehajtását,
- a Szervezeti és Működési Szabályzat (a továbbiakban: SZMSZ) rendelkezései és a munkaköri leírások alapján az informatikai rendszer felhasználóinak jogosultságai ellenőrzésében közreműködik,
- az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz az IBF-nek a további intézkedésekre, a felelősségre vonás megállapítására irányuló eljárás megindítására,
- összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében,
- végrehajtja és/vagy támogatja a külső és belső auditok eredményes elvégzését.

3.1.5. Szervezeti egység vezetők / Adatgazdák (SZEV / AG)

3.1.5.1. Hatáskörük

A szervezeti egységükhöz tartozó elektronikus információs rendszerekhez és adatokhoz a hozzáférési — igénylés, módosítás, visszavonás —jogosultságok elbírálása.

3.1.5.2. Felelősségük és feladataik

A közvetlen irányításuk alá tartozók körében, illetve hatáskörükbe tartozó elektronikus információs rendszerekben kezelt adatok információ biztonsági követelményeinek betartása és betartatása és az elektronikus információbiztonsági kontrollok működtetése a szervezeti egységre vonatkozó hozzáférési jogosultságok engedélyezése, illetve rendszeres felülvizsgálata.

3.1.6. Az egyes szervezeti egységek informatikai és adatvédelmi felelősei (IAF)

Az egyes szervezeti egységek informatikai és adatvédelmi felelőseit az érintett szervezeti egység vezetője jelöli ki, kijelölés hiányában az ezzel kapcsolatos feladatokat a szervezeti egység vezetője látja el. A kijelölt felelősök nyilvántartását az IBF vezeti.
Az informatikai és adatvédelmi felelős:

- köteles részt venni a belső képzéseken, oktatásokon,
- köteles figyelemmel kísérni a szervezeti egység tekintetében az informatikai biztonsági követelmények teljesülését, az ezzel kapcsolatos hiányosságokat a szervezeti egység vezetője részére jelezni,
- kirívóan súlyos hiányosság vagy informatikai biztonsági incidens észlelése esetén köteles a szervezeti egység vezetőjét és az IBSZ-t értesíteni,
- az informatikai biztonsággal kapcsolatos ismereteit köteles a szervezeti egység keretében tevékenységet végzők számára átadni.

3.1.7. Jogi és Humángazdálkodási Főosztály vezetője (HSZV)

3.1.7.1. Felelőssége

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet, valamint a biztonsági osztályba sorolás valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet és más vonatkozó jogszabályok alapján a munkakörök elektronikus információbiztonsági besorolása, a nemzetbiztonsági ellenőrzés alá eső munkakörök felmérése és ellenőrzése, részvétel az informatikai biztonsági oktatások lebonyolításának szervezésében, a belépők és kilépők tájékoztatása a jogokról és kötelezettségekről.

3.1.7.2. Feladatai

A felelősségi körébe tartozó tevékenységek elvégzése, annak során együttműködés az Informatikai Osztályvezetővel (IOV).

3.1.8. Informatikai Osztályvezető (IOV)

3.1.8.1. Hatásköre

Utasítási joggal rendelkezik az informatikai feladatokat ellátó szervezeti egység munkatársai felé, valamint véleményezési, tájékoztatási joga van az informatikai üzemeltetést és fejlesztést érintő stratégiai és koncepcionális kérdésekben. Jogosult továbbá az elektronikus információbiztonság megszervezésére és ellenőrzésére.
Javaslatot tesz az Informatikai Biztonsági Megbízott (IBM) személyére. Kijelöli az IT infrastruktúra üzemeltetésért felelős személyt (IÜFSZ), az Alkalmazás fejlesztésért felelős személyt (AFFSZ), és az Alkalmazás támogatásáért és üzemeltetéséért felelős személy(eke)t (ATFSZ), továbbá irányítja és ellenőrzi azok tevékenységét.

3.1.8.2. Felelőssége

Irányítási jogkörének megfelelően az informatikai feladatokat ellátó szervezeti egység és az elektronikus információs rendszerek szabályzatoknak és előírásoknak megfelelő működtetése.
Felelőssége kiterjed az informatikai biztonsággal kapcsolatos minden olyan tevékenységre, amelyet a jelen szabályzat vagy más további intézeti szabályzatok nem rendelnek más személyhez.

3.1.8.3. Feladatai

Az információbiztonsági követelmények megfogalmazása a beszerzési, fejlesztési, üzembe állítási folyamatok során, az információbiztonsági követelmények megvalósításának ellenőrzése, belső auditálása, a vonatkozó dokumentációk elkészítése / begyűjtése.
Az IÜFSZ, AFFSZ és ATFSZ tevékenységének irányítása és ellenőrzése. Feladatai kiterjednek az informatikai biztonsággal kapcsolatos minden olyan feladatra, amelyet a jelen szabályzat vagy más intézeti szabályzatok nem rendelnek más személyhez.
Minden, az informatikai rendszerekkel összefüggésbe hozható, az információs biztonságot jelentősen veszélyeztető eseményt vagy annak gyanúját haladéktalanul jelenteni az Információbiztonsági Felelősnek (IBF).

- Privilegizált fiókok engedélyezése.
- Kockázatkezelési terv kidolgozása.
- Biztonsági osztályba és szintbe sorolás.
- Informatikai biztonsági képzési terv kidolgozása.
- A helyiségek megfelelő informatikai biztonsági kategóriába sorolása.
- Az elektronikus információs rendszerek összekapcsolását célzó külső és belső rendszerkapcsolatok kialakítása, az integráció során alkalmazott műszaki paraméterek (funkciók, protokollok, portok és egyéb szolgáltatások).
- Az információbiztonsági követelmények kidolgozása.
- Biztonságtervezési szabályzat, illetve a fejlesztésekre vonatkozó biztonsági dokumentumok kidolgozása.
- A fejlesztések során kidolgozandó rendszerbiztonsági terv(ek) elkészítése.
- A külső helyszíneken használt eszközök belső használatba vonása, annak konfigurációi.

- Az üzletmenet-folytonosság tekintetében kiemelt jelentőségű rendszerek és komponensek informatikai biztonsági szempontból lényeges konfigurációs módosításai.
- Távoli felhasználói hozzáférési kapcsolat kiépítése.
- Távoli karbantartási kapcsolat kiépítése.
- BYOD eszközök engedélyezési elveinek kialakítása.
- Intézeten kívüli felhasználók azonosítóinak kiadása, jogkörök meghatározása.
- Hitelesítés szolgáltatók tanúsítványának elfogadása, tanúsítványok beszerzése, cseréje, használatba vonása.
- Az intézeti rendszerekhez elérést biztosító és a nyilvános internet elérést biztosító vezeték nélküli hozzáférések rendszerének kidolgozása.
- Külső elektronikus információs rendszer bármely intézeti információs rendszerrel való összekapcsolásának kialakítása.
- A hálózatra történő csatlakozás korlátozási szabályainak kialakítása és módosítása.
- A digitális aláírásokra és az alkalmazott kriptográfiai eszközökre és eljárásokra vonatkozó szabályok és működési mód kialakítása.
- Üzletmenet-folytonossági vagy adatintegritási kockázattal járó, tervezett rendszerleállások elrendelése.
- Az interneten elérhető erőforrások és az internethasználattal kapcsolatos korlátozások részletes meghatározása.

3.1.9. IT infrastruktúra üzemeltetésért felelős személy (IÜFSZ)

Az IT infrastruktúra üzemeltetésért felelős személyt az Informatikai Osztályvezető jelöli ki.

3.1.9.1. Hatásköre

Intézeti informatikai infrastruktúra kialakításával, üzemeltetésével és fejlesztésével kapcsolatban javaslattételi hatásköre van, illetve a kapcsolódó feladatok ellátása tekintetében döntési jogköre van, mely döntési jogköre az IOV által előzetesen jóváhagyott kereteken belül érvényes.

3.1.9.2. Felelőssége

Felelős az intézeten belüli, illetve azon kívüli vállalt infrastruktúra szolgáltatási szintek, illetve az üzemmenet-folytonosság elvárt szinten való fenntartásáért.

3.1.9.3. Feladatai

Az intézeti informatikai infrastruktúra kialakításával, üzemeltetésével és fejlesztésével kapcsolatos feladatok tervezése, végrehajtása, javaslattétel a fejlesztésekre, erőforrástervezés az üzemeltetési, fejlesztési, illetve javítási feladatok tekintetében.
Az informatikai infrastruktúra biztonsági követelményeinek való folyamatos megfelelés biztosítása.
Az informatikai erőforrások teljesítményét és kapacitását folyamatosan figyelemmel kíséri, a kapcsolódó problémák kezelésére javaslatot ad. Az automatizált felügyeleti környezet működtetése és felügyelete, ennek alapján a felmerülő biztonsági intézkedések kezdeményezése. Az infrastruktúra elemek és kapcsolódó rendszer beszerzés és fejlesztés esetén a szükséges erőforrások felmérése, és igénylése a vonatkozó belső szabályzatok rendelkezéseinek figyelembevétele mellett.

A fenti feladatokkal összefüggő hibajelentések megfelelő kezelésének (megelőző intézkedések, naplózás, ellenőrzés, korai riasztás, stb.) biztosítása.
Üzemmenet folytonossági feladatok szabályozása, tervezése, megvalósítása és működtetése az informatikai rendszerek (infrastruktúra) tekintetében.
Elkészíti a hatáskörébe tartozó elemek (infrastruktúra) kockázatelemzését és kockázatkezelési tervére javaslatot ad.
Részt vesz az informatikai auditokon.

3.1.10. Alkalmazás fejlesztésért felelős személy (AFFSZ)

Az alkalmazás fejlesztésért felelős személyt az Informatikai Osztályvezető jelöli ki.

3.1.10.1. Hatásköre

Az Intézetben használt alkalmazások fejlesztésével, beszerzésével és üzemeltetésével kapcsolatban javaslattételi hatásköre van, illetve a feladatok ellátása tekintetében döntési jogköre van, mely döntési jogköre az IOV által előzetesen jóváhagyott kereteken belül érvényes.

3.1.10.2. Felelőssége

Felelős az Intézeten belüli, illetve azon kívüli, vállalt alkalmazási szolgáltatási szintek, az üzletmenet folytonosság fenntartásáért.

3.1.10.3. Feladatai

Az Intézet által használt alkalmazások üzemeltetésével és fejlesztésével kapcsolatos feladatok tervezése, végrehajtása, javaslattétel a fejlesztésekre, erőforrástervezés az üzemeltetési, fejlesztési, illetve javítási feladatok tekintetében.
Rendszer beszerzés és fejlesztés esetén a szükséges erőforrások felmérése, és igénylése, ideértve az alkalmazások implementálásának és üzemeltetéshez szükséges erőforrások becslését is. A rendszerfejlesztésekkel összefüggő hibajelentések megfelelő kezelésének (megelőző intézkedések, naplózás, ellenőrzés, korai riasztás, stb.) biztosítása.
Üzletmenet-folytonossági feladatok szabályozása és tervezése az informatikai rendszerek tekintetében.
Részt vesz az „Információbiztonsági kockázatkezelési koncepció és eljárásrend"-nek megfelelő kockázatmenedzsment folyamatokban, elkészíti a hatáskörébe tartozó elemek (alkalmazások) kockázatelemzését és kockázatkezelési tervére javaslatot ad. Részt vesz az informatikai auditokon.

3.1.11. Alkalmazás támogatásáért és üzemeltetéséért felelős személy (ATFSZ)

Az alkalmazás támogatásáért és üzemeltetéséért felelős személyt az Informatikai Osztályvezető jelöli ki. A kijelölés történhet alkalmazásonként, vagy alkalmazáscsoportonként különböző személyek irányában is.

3.1.11.1. Hatásköre

Utasítási joggal rendelkezik az alkalmazás támogató feladatokat ellátó egység munkatársai felé az IOV által előzetesen jóváhagyott kereteken belül, valamint véleményezési, tájékoztatási joga van az alkalmazás támogatást érintő stratégiai és koncepcionális kérdésekben.

3.1.11.2. Felelőssége

Minden információs eszköz vagy eszközcsoport, elektronikus információs rendszer, informatikai szolgáltatás működtetésére informatikai alkalmazásgazdát (adminisztrátort) kell kijelölni, aki felelős a szabályzatokban és eljárásrendekben megfogalmazott követelmények szerinti üzembe helyezésért, időszakos konfigurálásért és a folyamatos üzemeltetésért.

3.1.11.3. Feladatai

Az intézeti előírásoknak és a gyártói ajánlásoknak megfelelően a folyamatos működéshez szükséges beállítások elvégzése, munkafolyamatok és ellenőrzések végrehajtása, a dokumentációk naprakészen tartása, a rendszerek felhasználóinak támogatása, valamint ezen tevékenységeik előírásszerű adminisztrálása.

3.1.12. Fizikai védelemért felelős személy (FVFSZ)

3.1.12.1. Hatásköre

Az Intézet informatikai üzemeltetési területén általános fizikai biztonsági és vagyonvédelmi vonatkozásában ellenőrzési, véleményezési, javaslattételi, kezdeményezési, betekintési és hozzáférési jog illeti meg.

3.1.12.2. Felelőssége

A vonatkozó jogszabályok és belső eljárásrendek alapján a fizikai védelmi szabályzatok, dokumentumok kialakítása, frissítése. Az informatikai üzemeltetési területeknél fellépő fizikai biztonsággal és vagyonvédelemmel kapcsolatos tervek, utasítások, szabályzatok elkészítése, a kapcsolódó intézeti dokumentumok véleményezése.

3.1.12.3. Feladatai

Az informatikai biztonsági irányítási rendszer szabályozó dokumentumokban rögzítettek szerint.

3.1.13. Tűzvédelmi felelős (TVF)

Az Intézet tűzvédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában közreműködik az információbiztonsággal összefüggő IT rendszerek tűzvédelmének biztosításában, az Intézet tűzvédelemre vonatkozó szabályzatában rögzítettek szerint.

3.1.14. Munkavédelmi felelős (MVF)

Az Intézet munkavédelemre vonatkozó szabályzása alapján előírt feladatok végrehajtásában közreműködik az informatikai rendszerek üzemeltetéséhez kapcsolódó munkavédelmi feladatok ellátásában, az Intézet munkavédelemre vonatkozó szabályzatában rögzítettek szerint.

3.1.15. Intézeten belüli vagy kívüli felhasználók (FELH)

3.1.15.1. Hatáskörük

Jogosultak a munkavégzésükhöz szükséges és elégséges mértékű hozzáférést kapni az információs rendszerekhez, eszközökhöz, szolgáltatásokhoz.

3.1.15.2. Felelősségük

Valamennyi felhasználó felelős az átvett informatikai eszközök előírásszerű használatáért, megőrzéséért, valamint a rájuk vonatkozó előírások és biztonsági követelmények betartásáért azon

adatok és elektronikus információs rendszerek tekintetében, amelyeket használnak, vagy amelyekkel bármilyen módon kapcsolatba kerülnek.

3.1.15.3. Feladataik

A Felhasználók kötelesek:

- az informatikai biztonsági képzéseken, oktatásokon részt venni, az ezzel kapcsolatos ismereteket megfelelő szinten elsajátítani,
- gondoskodni a személyükhöz rendelt felhasználói hozzáférések, a belépést biztosító fizikai eszközök (felhasználói fiókok, jelszavak, kártyák, tokenek) bizalmasságáról,
- a személyükhöz rendelt hozzáféréseket érintő incidensek bekövetkezése esetén haladéktalanul értesíteni közvetlen felettesüket és az IBF-et.

A Felhasználót a rendszer használatával összefüggésben szabálysértési, büntetőjogi, polgári jogi és munkajogi felelősség terheli.
Így a rendszerekben bekövetkező valamennyi kárért, amely az IBSZ-ben meghatározott felhasználói feladatok és kötelezettségek megsértésének vagy elmulasztásának következtében, a felhasználónak felróható okból következnek be, a felhasználó felelősséggel tartozik az irányadó jogszabályi előírások keretei között. A károkozás körülményeit jegyzőkönyvben rögzíteni kell.

3.2. Kapcsolattartás a hatóságokkal

A jogszabályokban meghatározott hatóságokat az IBF tájékoztatja az elektronikus információs rendszerek biztonsági eseményeiről és incidenseiről, valamint teljesíti az Intézet jogszabályi előírásként megfogalmazott elektronikus információbiztonsággal összefüggő adatszolgáltatási kötelezettségeit is, továbbá a kapcsolatot tart fenn a kormányzati és más eseménykezelő központokkal, a Nemzeti Kibervédelmi Intézettel és egyéb hatóságokkal.

Feladat	Felelős	Konzulens(ek)	Tájékoztatandó(k)
Kapcsolat a hatóságokkal	Információbiztonsági Felelős (IBF)	Informatikai Osztályvezető (IOV) Főigazgatói Hivatal vezetője	Főigazgató (FOIG)

2. táblázat —NKI kapcsolattartók

A fenti tevékenységeiről az IBF Főigazgatói Hivatal vezető, Informatikai Osztályvezető (IOV) és a Főigazgató (FOIG) felé tartozik tájékoztatással, továbbá megosztja a tudomására jutott naprakész informatikai biztonsági — fenyegetésekre és sebezhetőségekre vonatkozó — információkat, eljárásokat és technikákat az érintett szervezeti egységekkel.
A Nemzeti Kibervédelmi Intézet és a kormányzati eseménykezelő központ részére az IBF-nek az Ibtv. alapján előírt adatait be kell jelentenie.
Az IBF-nek folyamatosan figyelemmel kell kísérnie a jogszabályban kijelölt szervezetek által kiadott riasztásokat és gondoskodnia kell az egyes elektronikus információs rendszerekre vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

4. Az Intézmény biztonsági szintje

A szervezet a megvalósított előzetes vizsgálat alapján az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15) BM rendelet szerint 3-as biztonsági szintbe sorolja magát, amely megfelel a biztonsági osztályba sorolás valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI.24.) MK rendelet „alap" biztonsági osztályának.
Indoklás: A 41/2015. (VII. 15) BM rendelet 2. számú, a 7/2024. MK rendelet 1. 2.2 pontjában mellékletében foglaltak szerint

4.1. Biztonsági szintbe és osztályba sorolás, informatikai biztonsági kockázatelemzés

A biztonsági szintbe és osztályba sorolást, valamint az informatikai biztonsági kockázatelemzést az IBF végzi el:

- Szervezeti egység vezetők / Adatgazdák,
- Informatikai biztonsági megbízott,
- Főigazgatói Hivatal vezető,
- Informatikai Osztályvezető,
- IT infrastruktúra fejlesztésért és üzemeltetéséért felelős vezető,
- Alkalmazás fejlesztésért és üzemeltetéséért felelős vezető,
- IT üzemeltetésért felelős vezető,

(illetve az általuk kijelölt munkatársak) bevonásával.

4.1.1. Biztonsági szintbe és osztályba sorolás

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében az elektronikus információs rendszereket — ideértve a rendszer által kezelt adatokat — biztonsági osztályba kell sorolni, a bizalmasságuk, a sértetlenségük, valamint a rendelkezésre állásuk szempontjából. Az elektronikus információs rendszerek biztonsági osztályba sorolását az alábbi alapkövetelmények figyelembevételével kell végrehajtani:

- a biztonsági osztályokhoz tartozó védelmi követelményeket jogszabály rögzíti,
- a nemzeti adatvagyont kezelő rendszerek esetében a jogszabályi előírásoknak megfelelően,
- a biztonsági osztályokat a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából erősödő védelmi követelményeket meghatározó, 1-5 fokozatú skála szerint kell megállapítani.

Az Intézetet az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

A biztonsági szintbe és osztályba sorolást az Intézet vagy az elektronikus információs rendszer — illetve az abban kezelt adatok — jelentős megváltozása esetén, de legalább 3 évente felül kell vizsgálni.

4.1.2. Cselekvési terv készítése

Amennyiben a vizsgálat vagy felülvizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre jogszabályban meghatározott biztonsági szint, vagy ha az szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot

állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére vagy hiányosságok megszüntetésére.
A cselekvési terv elkészítése és folyamatos nyomon követése az Információbiztonsági Felelős (IBF) feladata, együttműködve az elektronikus információbiztonsági feladatok ellátásában közreműködő személyekkel, szervezeti egységekkel és munkacsoportokkal. A cselekvési terv elfogadása — a Főigazgatói Hivatal vezetőjének jóváhagyását követően — a Főigazgató (FOIG) feladata.

4.2. Informatikai biztonsági kockázatelemzés

Az informatikai biztonsági kockázatelemzés célja azoknak az informatikai, fizikai és humán tényezőknek a feltárása, amelyek kockázatot hordoznak magukban, ezáltal veszélyeztetve az Intézet megfelelő működését, illetve, hogy számszerűsíthető módszerekkel megbecsülje a fenyegető tényezők bekövetkezési gyakoriságát és hatását, majd a kockázatok összehasonlítása érdekében számszerűsítse a releváns kockázatokat.
A felmerült kockázatok kezelésére intézkedési terveket kell készítenie, melyek a feltárt kockázatok függvényében az alábbiakat kell, hogy tartalmazzák:

- a kockázatok csökkentésére tett javaslatokat a technikai eszközök megváltoztatására, vagy fejlesztésére (pl.: új védelmi eszközök alkalmazása, vagy a jelenlegi átkonfigurálása),
- a kockázatok csökkentésére tett javaslatokat az érvényben lévő szabályozás megváltoztatására,
- a kockázatok csökkentésére tett javaslatokat a személyi állományra vonatkozóan (pl.: motiváció, a fegyelmi eljárások szigorítása, oktatás stb.),
- a kockázatok tudatos felvállalására irányuló javaslatot, ha a védelmi intézkedés anyagi vonzata nagyobb, vagy közel azonos, mint a fenyegetettség által elszenvedhető anyagi kár.

4.3. Informatikai biztonsági ellenőrzés

Az informatikai biztonsági ellenőrzések alapvető célja, hogy a kockázatok csökkentése és a rendkívüli események elkerülése érdekében objektív információkat szolgáltasson a felelős vezetők számára az informatikai biztonság helyzetéről.
Az informatikai biztonsági ellenőrzés célja, hogy rendszeresen vizsgálja:

- az informatikai rendszerek biztonsági megfelelését az Intézet által elfogadott biztonsági követelményeknek;
- az intézeti és rendszerszintű biztonsági szabályozásokban (jogszabályokban, fenntartói és belső utasításokban, körlevelekben, stb.) foglaltak érvényesülését;
- az alkalmazott módszerek jogszabályi előírásoknak való megfelelését;
- az informatikai rendszerek és az általuk nyújtott szolgáltatások biztonságát;
- a biztonsági alapelveket sértő események bekövetkezési valószínűségét, illetve a már korábban bekövetkezett események körülményeit, és az azok miatt esetlegesen szükségessé vált korrekciós intézkedések hatékony megvalósulását.

Az ellenőrzések során feltárt hiányosságok képezik azon védelmi intézkedések alapját, melyek biztosítják, hogy minimális legyen a védelmi képességek kívánt és valós szintje közötti távolság. A megállapításokat mindig írásos jelentésbe kell foglalni, a védelmi intézkedések megsértésével

kapcsolatban adott esetben szankciókat is kell alkalmazni. Az ellenőrzések során tapasztalt hiányosságok megszüntetésére intézkedési tervet kell kidolgozni.

5. Adminisztratív védelmi intézkedések

5.1. Az elektronikus információs rendszerekkel kapcsolatos engedélyezés (3.3.6.2.2. [4]), {1.11}

Az Intézet az általa kezelt adatok, adatkezelő információs rendszerek információbiztonsági céljait az információbiztonsággal kapcsolatos engedélyezési eljárásrenddel biztosítja.

5.1.1. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás (3.1.1.5. [1]) {1.11.1}

Bármely, az Intézet informatikai eszközeinek (hardverek, szoftverek, alkalmazások) használatával összefüggő engedélyezési eljárást az érintett szervezeti egység vezetőinek kell kezdeményezniük.

A kérelemben fel kell tüntetni:

- az engedély jogosultjának, nevét, beosztását;
- az engedélyezés időtartamát (kezdő és záró időpontot);
- a kért hozzáférések, elvégezhető műveletek leírását;
- a munkahelyi feladatokat, amelyekhez a kért jogosultság szükséges;
- az esetleges korlátozásokat.

Nem privilegizált fiókok esetében a jogosultság megadásának kérelmét jóváhagyás céljából el kell küldeni az illetékes rendszergazdának.

A rendszergazda a kérelem jóváhagyása során a következők alapján mérlegel:

- hatályos jogszabályok;
- hatályos utasítások;
- a kérelem indokoltsága;
- a rendelkezésre álló erőforrások.

A jóváhagyást követően a rendszergazda beállítja a kért jogosultságot, elutasítás vagy kérdéses esetben a kérelmet döntésre továbbítja az Informatikai Osztályvezető (IOV) felé.

Privilegizált fiókok esetében a jogosultság beállításának kérelmét el kell juttatni az Informatikai Osztályvezetőnek (IOV).

Az Informatikai Osztályvezető (IOV) a kérelem jóváhagyása során a következő szempontok mérlegelése alapján dönt:

- hatályos jogszabályok;
- hatályos utasítások;
- a kérelem indokoltsága;
- a rendelkezésre álló erőforrások.

Az Informatikai Osztályvezető (IOV) által engedélyezett jogosultságot el kell juttatni az illetékes rendszergazdához, aki az engedély birtokában további mérlegelés nélkül beállítja az engedélyezett jogosultságot a privilegizált fiókhoz.

5.1.2. Engedélyek visszavonása/felfüggesztése (3.1.1.5. [1]), {1.11}

Bármely, az Intézet informatikai eszközeinek (hardverek, szoftverek, alkalmazások) használatával összefüggő jogosultság visszavonása vagy felfüggesztése

- az alkalmazott jogviszonyának megszűnése;
- a szerződő partner számára biztosított jogosultság okafogyottá válása;
- feladatkör megváltozása, megszűnése

esetén a Szervezeti egység vezetőjének (SZEV) kell kezdeményeznie a jogosultság beállításának elvégzésében illetékes rendszergazdánál.

A jogosultságok megadásának és visszavonásának e-mail levelezését e-mail/ticketing rendszer naplóit utólagos ellenőrzés céljából 5 évig meg kell őrizni.

5.2. Az elektronikus információs rendszerek nyilvántartása (3.1.1.4. [1]), {1.5}

Az Intézet az elektronikus információs rendszereiről nyilvántartást vezet. A nyilvántartást az Informatikai Osztályvezető (IOV) elektronikus formában vezeti, és gondoskodik azok naprakészségéről.

A nyilvántartásnak minden rendszerre nézve tartalmaznia kell:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (amennyiben azok az Intézet kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
- a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezeteknél a rendszer tekintetében illetékes kapcsolattartó személyek személyazonosító és elérhetőségi adatait.

5.3. Kockázatkezelés, kockázatelemzés (3.1.2. [1]) {15}

5.3.1. A kockázat azonosítása

A kockázati tényezők azonosításának célja annak megállapítása, hogy melyek az Intézet informatikai biztonságának célkitűzéseit veszélyeztető fő kockázatok. A kockázatok azonosítását az Információbiztonsági Felelős (IBF) végzi el.

Az Információbiztonsági Felelős (IBF) kötelessége minden olyan kockázat azonosítása, amelyek potenciális hatással lehetnek az Intézet informatikai biztonságának céljaira vagy működésére, függetlenül attól, hogy azok igazgatási, szabályozási, jogi, technológiai, szállítói, emberi erőforrás-jellegűek, vagy működési szempontot érintenek.

A kockázati csoportok az alábbiak szerint állapíthatók meg:

- Informatikai: az alkalmazott IT rendszerek, az informatikai infrastruktúra hibái (rendszerhiba, rendszerleállás, korlátozott rendelkezésre állás).
- Ügyviteli: az üzleti folyamatok hiányosságai, nem megfelelő szervezettség, szabályozatlanság.
- Külső hatások: gazdasági, jogszabályi, környezeti, természeti csapások vagy a harmadik fél által okozott veszteség, árvíz, földrengés, villámcsapás, rablás, betörés vandalizmus, terrortámadás.
- Humán: a munkavállalók, vezetők által — akár szándékosan, akár gondatlanságból - elkövetett károkozás, információ és pénz jogosulatlan eltulajdonítása, üzleti és személyiségi jogokhoz kapcsolódó titok megszerzése, megvesztegetés, tévedés vagy szakmai hozzáértés hiánya miatti hibák.
- Egyéb: az előzőkbe nem sorolható kockázati tényező.

A kockázattal kapcsolatos érdemi információk megadása, összegyűjtése érdekében rögzíteni kell a Kockázati Naplóban (továbbiakban: KN) az adott kockázat jellemző adatait, amelyek a következők:

- kockázat azonosítója;
- kockázat típusa;
- kockázat rövid leírása (Mi történhet, ami rossz, mikor következhet be);
- kockázat azonosításának dátuma;
- kockázat azonosítójának neve;
- kockázat azonosítójának szervezeti egysége.

Az Információbiztonsági Felelős (IBF) elemzi a KN-ben újonnan rögzített kockázatot és a Kockázatkezelési dokumentumban (KD):

- megállapítást tesz a bekövetkezési valószínűség és a lehetséges kár értékére;
- kijelöli a kockázat gazdát;
- meghatározza az adott kockázathoz tartozóan a
  - kockázati jellemzőket,
  - bekövetkezhető kár osztályát (1-5),
  - bekövetkezés valószínűségi osztályát (1-5),
  - kockázati faktort,
  - kockázati osztály (kritikus, magas, közepes, alacsony, nagyon alacsony),
  - kockázat gazda nevét,
  - kockázat kezelésnek határidejét.

5.3.2. A kockázatok értékelése

5.3.2.1. A kockázat bekövetkezéséből adódó lehetséges kár értékelése

Az egyes lehetséges kockázati események bekövetkezéséből adódó lehetséges károk nagyságait 1 - től 5-ig terjedő skálán, kár osztályokba kell sorolni a következő szempontok alapján:

Kár osztály	Bekövetkezhető kár
1	Jelentéktelen káresemény következhet be, mivel: – személyes adatok nem sérülhetnek; – nincs bizalomvesztés, a probléma kisebb, az Intézeten belül marad, és azon belül meg is oldható; – a közvetlen és közvetett anyagi kár az Intézet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest jelentéktelen.

Kár osztály	Bekövetkezhető kár
2	Csekély káresemény következhet be, mivel: – személyes adat sérülhet; – az ügymenet szempontjából csekély értékű, és/vagy csak belső szabályozóval védett adat vagy elektronikus információs rendszer sérülhet; – a lehetséges társadalmi-politikai hatás az Intézeten belül kezelhető; – a közvetlen és közvetett anyagi kár az Intézet költségvetéséhez, szellemi és anyagi erőforrásaihoz képest csekély.
3	Közepes káresemény következhet be, mivel: – különleges személyes adatok, vagy nagy mennyiségű személyes adat sérülhet; – az ügymenet szempontjából közepes értékű, vagy az Intézet szempontjából érzékeny folyamatokat kezelő elektronikus információs rendszer, információt képező adat, vagy egyéb, jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett adat sérülhet; – lehetséges társadalmi-politikai hatás, bizalomvesztés állhat elő az Intézeten belül, vagy szabályokban foglalt kötelezettségek sérülhetnek; – a közvetlen és közvetett anyagi kár a költségvetéshez, szellemi és anyagi erőforrásokhoz képest közepes.
4	Nagy káresemény következhet be, mivel: – nagy mennyiségű különleges személyes adat sérülhet; – személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket); – az ügymenet szempontjából nagy értékű, üzleti titok, vagy az Intézet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet; – a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés az Intézeten belül, az Intézet felsővezetésében, vezetésében személyi konzekvenciákat kell alkalmazni; – a közvetlen és közvetett anyagi kár az Intézet költségvetéséhez, szellemi és an a i erőforrásaihoz képest jelentős.

Kár osztály	Bekövetkezhető kár
5 (4+)	Kiemelkedően nagy káresemény következhet be, mivel: – kiemelten nagy mennyiségű különleges, személyes adat sérül; – emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be; – a nemzeti adatvagyon helyreállíthatatlanul megsérülhet; – az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított; – a lehetséges társadalmi-politikai hatás súlyos bizalomvesztés az Intézettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek; – a közvetlen és közvetett anyagi kár az Intézet költségvetését, szellemi és anyagi erőforrásait meghaladó, különösen nagy értékű üzleti titok, az Intézetszempontjából kiemelten érzéken információt képező adat sérül.

3. táblázat - Kár osztályok és a bekövetkezhető kár

5.3.2.2. A kockázati események bekövetkezésének valószínűsége

Az Intézet az egyes lehetséges kockázati eseményeket azok bekövetkezési valószínűségei szerint valószínűségi osztályokba sorolja.

Valószínűségi osztály (lehetséges értékek)	A bekövetkezés valószínűsége
1	Jelentéktelen
2	Csekély
3	Közepes
4	Nagy
5	Kiemelkedő
5+	Katasztrofális

4. táblázat - Kockázati események valószínűségi osztályai

5.3.2.3. A kockázatok besorolása kockázati faktor szerint

A kockázati faktort a kockázat bekövetkezési valószínűségének (kár osztály) és a bekövetkezés valószínűsége (valószínűségi osztály) szorzataként kell megállapítani.

Kockázati faktor	Kockázati osztály
1-2	1 (Nagyon alacsony)

Kockázati faktor	Kockázati osztály
3-5	2 (Alacsony)
6-7	3 (Közepes)
8-14	4 (Magas)
15-20	5 (Kritikus)
20-	5+ (Katasztrofális)

4. táblázat - Kockázatok besorolása kockázatifaktor szerint

5.3.3. Az intézkedési terv és mérföldkövei (3.1.1.3. [2]), {1.4}

A kockázati naplóban rögzített kockázatok kezelésével kapcsolatban intézkedési tervet kell készíteni. Az intézkedési tervet az Információbiztonsági Felelős (IBF) és az általa kijelölt kockázatgazda (a kockázat megszüntetésének vagy csökkentésének felelőse) közösen készíti el.

5.3.3.1. Az intézkedési terv tartalma

Az intézkedési tervnek tartalmaznia kell az alábbi információkat:

- az adott kockázat megnevezése, azonosítója a Kockázati Naplóban;
- a kockázat kezelésének célja;
- a kockázat kezelésének javasolt módja;
- a kockázat kezeléséhez szükséges feladatok, felelősök és határidők;
- a kockázat kezeléséhez szükséges eszköz/ szoftver beszerzések;
- a kockázat kezelése után megmaradó kockázatok;
- a kockázat kezelését koordináló felelős.

A kockázatkezelési intézkedések lehetséges céljai a következők lehetnek:

- **Elkerülés:** a kockázat bekövetkezési valószínűségének vagy a kockázat bekövetkezés az Intézetre való hatásának kiküszöbölése. (Jellemzően magas kockázati faktorú kockázatok esetén szokták kitűzni ezt a célt).
- **Áthárítás:** az Elkerülés egy speciális esete, amikor a kockázat hatásait egy másik félre hárítjuk, pl. szerződéses kötbér, biztosítás stb. segítségével.
- **Valószínűségcsökkentés:** a kockázat bekövetkezési valószínűségének tolerálható szintre történő csökkentése.
- **Vészforgatókönyv:** a kockázat bekövetkezése esetén a negatív hatások csökkentésére irányuló terv.
- **Tolerálás:** A túlzottan jelentős ráfordítási igény miatt kockázattal történő együttélés.

5.3.3.2. Az intézkedési terv elkészítésének határidői

Kockázati osztály	Intézkedési terv kidolgozása és elfogadása	Az intézkedési terv végrehajtásának végső határideje	Az intézkedési terv végrehajtásának ellenőrzése
Katasztrofális	A kockázat értékelését követő 3. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	naponta
Kritikus	A kockázat értékelését követő 8. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	hetenként
Magas	A kockázat értékelését követő 20. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	2 hetenként
Közepes	A kockázat értékelését követő 30. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	havonként
Alacsony	A kockázat értékelését követő 30. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	havonként
Nagyon alacsony	A kockázat értékelését követő 60. munkanap	Az intézkedési tervben meghatározott ütemterv szerint	2 havonként

5. táblázat - Az intézkedési terv elkészítésének határidői

5.3.3.3. Kockázatkezelő intézkedések végrehajtása

A kockázatgazda által beterjesztett/kidolgozott intézkedést a kockázatgazda vagy az Informatikai Osztályvezető (IOV) terjeszti a Főigazgató (FOIG) elé jóváhagyásra. A Főigazgató (FOIG) által jóváhagyott intézkedési tervet a kockázatgazda végrehajtja/végrehajttatja.
Abban az esetben, ha a kockázat kezelésre az azzal történő együttélés javasolt, a kockázat kezelését annak kiemelt figyelésével kell megvalósítani.
A kockázatkezelési intézkedés végrehajtása után a kockázati naplóban frissíteni kell a kockázat valószínűségének és hatásainak értékét.

5.3.4. A végrehajtás ellenőrzése, felülvizsgálat

5.3.4.1. A kockázatkezelési feladatok nyomon követése

Az intézkedési terv végrehajtásának nyomon követése az Információbiztonsági felelős (IBF) feladata.
A kockázatkezelés végrehajtásának ellenőrzése során a kockázatkezelési dokumentumban:

- nyomon kell követni és dokumentálni kell az egyes kockázatkezeléssel kapcsolatban megfogalmazott feladatok végrehajtását;
- rendszeresen jelentést kell készíteni a vezetés számára az egyes kockázatkezelési feladatok végrehajtásának státuszáról.

5.3.4.2. Eszkaláció

A kockázatgazda eszkalálni köteles, ha:

- a kockázati faktor megnövekszik;
- a kockázatkezelés kitűzött céljának elérése olyan akadályba ütközik, hogy az csak vezetői szinten kezelhető.

5.3.5. A kockázatkezelés lezárása

A kockázatkezelés lezárását a kockázatgazda kezdeményezésére az Információbiztonsági felelős (IBF) hagyja jóvá és adminisztrálja a kockázati naplóban.

5.3. Biztonsági osztályba sorolás (3.1.2.2. [1]) {15.2}

A 2013. évi L. törvény 7. S-ának (1) bekezdése alapján az Intézet elektronikus információs rendszereit a kockázatarányos, költséghatékony védelem megvalósítása érdekében biztonsági osztályokba kell sorolni.
Az osztályba sorolást az elektronikus információs rendszereket 1-5-ig terjedő skálán az elektronikus információs rendszerben kezelt adatok bizalmassága, a sértetlensége és a rendelkezésre állása, illetve az elektronikus információs rendszer sértetlensége és rendelkezésre állása elvesztéséből fakadó jogi, társadalmi-politikai, közvetlen, illetve közvetett anyagi kár vagy hatás szempontjából külön-külön kell elvégezni.
A biztonsági osztályba sorolást minden új rendszer implementációja esetén el kell végezni, illetve minden olyan esetben, amikor változás áll be az elektronikus információs rendszerben vagy annak működési környezetében, továbbá olyan körülmények esetén, amelyek befolyásolják az elektronikus információs rendszer biztonsági követelményeit vagy állapotát.
A biztonsági osztályok megállapítása során a következő feladatokat kell elvégezni:

- adatbesorolás;
- a rendszerrel kapcsolatos kockázatelemzés;
- a rendszer elvárt biztonsági osztályának meghatározása;
- a rendszer tényleges biztonsági osztályának meghatározása;
- a biztonsági osztálybesorolás eredményének rögzítése az Intézet rendszereinek nyilvántartásában;
- kapcsolódás biztosítása a 41/2015. (VII. 15.) BM rendelet szerinti 3.1.1.3 pontban foglalt intézkedési terv mérföldköveihez;
- a NKI értesítése az osztályba sorolásról.

5.4.1. Adatbesorolás

Az Intézet által használt egyes adatokat, adatköröket adatbiztonsági szempontok alapján osztályozni kell. Az adatok besorolását bizalmasság, sértetlenség és rendelkezésre állás szerint kell elvégezni.

5.4.1.1. Az adatok osztályozása bizalmassá szerint

Biztonsági osztályok	Jogszabállyal, belső szabályzóval szabályozott, vagy védett adat
1. (Nyilvános)	– Az Infotv. szerint közérdekű vagy közérdekből nyilvános adatok. – Egyéb, az Intézet által nyilvánosnak besorolt adat.

Biztonsági osztályok	Jogszabállyal, belső szabályzóval szabályozott, vagy védett adat
2. (Belső)	– Napi operatív munkavégzéshez szükséges, vagy annak során keletkezett belső használatú adatok.
3. (Fokozott biztonságú)	– Egyéb belső szabályozásban hozzáférés korlátozás alá eső adatok (pl. egyes feladatok végrehajtása érdekében keletkezett bizalmas adatok). – Az Általános Adatvédelmi Rendelet, valamint az Infotv. szerinti személyes adatok. – Egyéb, jogszabállyal védett titok (kivétel üzleti titok, minősített adat).
4 (Kiemelt bizalmasságú)	– Az Általános Adatvédelmi Rendelet, valamint az Infotv. és az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény szerinti különleges adatok, köztük az egészségügyi adatok. – Üzleti titkok, tömeges személyes adat.
5. (Minősített adat)	A minősített adat védelméről szóló 2009. évi CLV. törvény hatálya alá tartozó: – „Korlátozott terjesztésű!", – „Bizalmas!", – „Titkos!" – „Szigorúan titkos!" Nemzeti/EU/NATO minősítésű adatok.

6. táblázat - Az adatok osztályozása bizalmasság szerint

5.4.1.2. Az adatok osztályozása sértetlenség és rendelkezésre állás szerint

Az adatok osztályozása sértetlenség és rendelkezésre állás szerint megegyezik az adatintegritás vagy rendelkezésre állás sérülés kockázati osztályba sorolásával (ld. A kockázatok értékelése).

5.4.2. A rendszerrel kapcsolatos biztonsági kockázatelemzés

Elemezni kell az egyes informatikai rendszerek kockázatait:

- bizalmasság;
- sértetlenség;
- rendelkezésre állás
- szerint külön-külön.

5.4.3. A rendszer elvárt biztonsági osztályának meghatározása

Az Intézet az elektronikus információs rendszerek biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti;

- a nemzeti adatvagyont kezelő rendszerek esetében a sértetlenség követelményét emeli ki;
- a létfontosságú információs rendszerelemek esetében a rendelkezésre állást követeli meg elsődlegesen;

- a különleges személyes adatokkal kapcsolatban alapvető igényként fogalmazza meg a bizalmasság fenntartását.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet a Főigazgató (FOIG) hagy jóvá, kockázatelemzés alapján kell elvégezni.

5.4.4. A rendszer tényleges biztonsági osztályának meghatározása

A rendszer tényleges biztonsági osztályának meghatározását az NKI által kiadott táblázat alapján kell elvégezni. A táblázat letölthető az NKI oldaláról.

5.4.5. A biztonsági osztálybesorolás eredményének rögzítése a rendszer nyilvántartásban

Minden egyes osztályba sorolást követően a változást át kell vezetni az informatikai rendszerek nyilvántartásán.

5.4.6. Kapcsolódás biztosítása más intézkedési tervek mérföldköveihez

Abban az esetben, ha egy informatikai rendszer nem felel meg az elvárt biztonsági osztályának megfelelő biztonsági előírásoknak, az előírások teljesülésének érdekében intézkedési tervet kell készíteni, amelynek illeszkednie kell az Intézet kockázatkezelésekkel kapcsolatos intézkedési terveihez.

5.4.7. Az NKI értesítése az osztályba sorolásról

Az egyes rendszerek biztonsági osztályba sorolásának eredményéről 10 munkanapon belül az IBF-nek értesítést kell küldenie az NKI számára. A rendszerek biztonsági osztályba sorolásának és állapotfelmérésének eredményét rendszerenként az NKI által közzétett segédletnek megfelelően kitöltött formában kell feltölteni.

5.4.8. A biztonsági osztályba sorolás felülvizsgálata

A rendszerek kockázatelemzését és biztonsági osztályba sorolását az Információbiztonsági Felelősnek (IBF) dokumentált módon legalább évente, de a következő esetekben soron kívül felül kell vizsgálni:

- amennyiben változik az elektronikus információs rendszer biztonságát érintő jogszabály;
- új elektronikus információs rendszer bevezetése esetén;
- ha bármely audit során szükségessé válik kockázatelemzés elvégzése;
- az Intézet státuszában változás áll be;
- az Intézet által kezelt vagy feldolgozott adatok kategóriái vonatkozásában változás következik be.

5.5. Az informatikai rendszerek biztonsági követelményei

Az informatikai rendszerek integrált biztonságának kialakítása a biztonságpolitika által meghatározott szempontok szerint kell, hogy történjen. A biztonság alapvető feltétele az alkalmazást vagy szolgáltatást támogató szervezeti munkafolyamat megtervezése és megvalósítása. Az informatikai rendszerek kifejlesztése előtt szükség van a biztonsági követelmények meghatározására és egyeztetésére.

Informatikai projekt követelményeinek megfogalmazása során meg kell határozni az összes biztonsági követelményt. A követelményeket és szükséges megoldásokat az informatikai rendszer fejlesztésének részeként kell megindokolni, egyeztetni és dokumentálni.

5.5.1. A biztonsági követelmények elemzése és meghatározása

Az informatikai beruházások előkészítési, tervezési fázisában figyelemmel kell kísérni a következő biztonsági szempontok érvényesítését:

- az informatikai rendszer által kezelendő adatoknak az információvédelem és a megbízható működés szempontjából történő elemzése és a védelmi célkitűzések meghatározása;
- az informatikai rendszer várható informatikai biztonsági osztályba sorolása az információvédelem és a megbízható működés területén;
- a jogszabályokból és a belső szabályozásból eredő kötelezettségek bemutatása;
- a fizikai és a logikai védelem rendszerszintű bemutatása;
- a megvalósításhoz szükséges feltételrendszer meghatározása;
- a biztonsági rendszer teljes költségének becslése, ennek összehasonlítása a lehetséges kockázatokkal, károkkal;
- az informatikai biztonsági fejezetnek a tervezési dokumentumokba történő beállításáért a projektvezető, annak kijelöléséig, vagy hiánya esetén az illetékes vezető (előterjesztő) a felelős;
- az Intézet minden informatikai projekt előterjesztésének tartalmaznia kell a létrehozandó (fejlesztendő, átalakítandó) informatikai rendszer fizikai, logikai és adminisztratív védelmi rendszerének — a projekt keretében történő — tervezési és megvalósítási lépéseit, költségeit, felelőseit;
- az informatikai projekt jóváhagyott költségvetésében szerepelnie kell a biztonsági rendszer tervezési és megvalósítási költségeinek;
- az alkalmazott operációs rendszer meg kell feleljen minimum az ISO/IEC 15408 (CommonCriteria) EAL4-as szintjének;
- az előző pontokban megfogalmazott feltételek hiánya az informatikai projektek esetében jelentősen megnöveli az információbiztonsági kockázatokat, valamint a későbbi kiadásokat, mivel a tervezési szakaszban bevezetett intézkedések lényegesen olcsóbban foganatosíthatók, mint azok, amelyeket a bevezetés alatt vagy után valósítanak meg. Amennyiben szükséges (pl. a költségek vagy a projekt nagysága miatt) az Intézet megkövetelheti a független kiértékelt és tanúsított termékek használatát;
- az Intézet úgy tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységekre gyakorolt hatását.

5.5.2. Biztonság az alkalmazási rendszerekben

A felhasználói rendszerek integrált biztonsága kiterjed a rendszerekben tárolt felhasználói adatok illetéktelen hozzáférésének, módosításának, törlésének, nem megfelelő felhasználásának stb. megelőzésére. A rendszertervek összeállítása során mérlegelni kell a rendszerbe beépítendő automatikus ellenőrző eszközök, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.
A felhasználói rendszerek biztonságát a következő intézkedések szavatolják:

- A felhasználói rendszerekben meg kell tervezni a megfelelő ellenőrző eszközöket és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatok, a belső adatfeldolgozás és a kimenő adatok ellenőrzését.
- Az érzékeny, egyéb védendő vagy kritikus adatok feldolgozását végző, vagy ilyen adatokat befolyásoló rendszereknél további ellenőrző eszközökre lehet szükség. Ezeket az ellenőrző eszközöket a biztonsági követelmények és a kockázatelemzés alapján kell kiválasztani.
- Az előző két pontban meghatározott biztonsági intézkedéseket pontosan, minden részletre kiterjedően dokumentálni kell.

5.5.3. A bemeneti adatok ellenőrzése

Az adatfeldolgozó rendszerekbe bevitt adatokat a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a feldolgozás jellegének figyelembevételével ellenőrizni kell. A bemenő adatok ellenőrzésének eszközei a következők lehetnek:

- az ismételt adatbevitel és az ebből származó adat-karbantartási anomáliák elkerülésére írt eljárások; időszakos adatmező és -állomány vizsgálat, valamint a felvitt adatok hitelességének, integritásának ellenőrzése és igazolása;
- az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése, illetve ezek engedély nélküli módosításának megakadályozása, valamint az engedélyezés kikényszerítésére írt eljárások;
- adat ellenőrzési hibák kiküszöbölését elősegítő eljárások;
- adatbevitel során, a mezőtípus kompatibilitást biztosító, illetve adattartalom helyességét ellenőrző és kikényszerítő eljárások, függvények;
- az alkalmazáshoz történő hozzáférés naplózása;
- a feldolgozásban résztvevő alkalmazottak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

5.5.4. Az adatfeldolgozás ellenőrzése

A felvitt adatok pontosságát, hiánytalanságát, és integritását a feldolgozás ideje alatt a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével a következő intézkedésekkel kell elősegíteni:

- Az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni, különös tekintettel az adatmódosító-, törlő funkciók helyére.
- Adatfeldolgozási hibák esetén hibadetektáló, és a további rendszerfutást leállító eljárások beépítése a rendszerbe.
- Korrekciós programok alkalmazása a feldolgozás során felmerülő hibák korrigálására.

A folyamatba épített ellenőrzés ellátásáért az Informatikai Osztályvezető (IOV) által kijelölt informatikus a felelős.

5.5.4.1. A sértetlenség biztosítása

A helyesen rögzített adatok adatminősége akár a feldolgozás hibáitól, akár szándékos tevékenységektől is megváltozhat. A rendszerekben az ilyen meghibásodások felismerése érdekében a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével érvényesítő ellenőrzéseket kell beépíteni. Az alkalmazások tervezésével

lehetőség szerint gondoskodni kell arról, hogy a korlátozások megvalósítása valóban minimalizálja a sértetlenség elvesztésére vezető feldolgozási hibák kockázatát. Biztonsági szempontok alapján a lehetséges kockázatok mértékének, a rendelkezésre álló lehetőségek és a szoftver jellegének figyelembevételével meg kell tervezni:

- az adatváltoztatást megvalósító hozzáadó és leválasztó funkciók helyét és használatát a végrehajtó programokban;
- azokat az eljárásokat, amelyek megakadályozzák, hogy a programok rossz sorrendben, vagy korábbi feldolgozásban előállt meghibásodás után lefussanak;
- a helyes programok használatát a meghibásodás utáni visszatérésre annak érdekében, hogy az adatokat helyesen/pontosan dolgozzuk fel.

5.5.4.2. Vezérlő és ellenőrző eljárások

A szükséges intézkedések attól függenek, hogy milyen az alkalmazás természete, és hogy az Intézet tevékenységére a hibás adat milyen hatással lehet. Esettől függően a következő ellenőrzések felvételét kell mérlegelni:

- eseményenkénti ellenőrzéseket;
- az állományfrissítések ellenőrző összegeit;
- program(futás)onkénti ellenőrzéseket;
- a rendszer által keltett adatok érvényesítését;
- a központi és a távoli számítógépek között a feltöltött vagy letöltött adatok vagy szoftverek ellenőrzéseit;
- az ellenőrzéseket, amelyek szavatolják, hogy az alkalmazási programokat időben lefuttatták;
- az ellenőrzéseket, amelyek szavatolják, hogy az alkalmazási programokat a helyes sorrendben futtatták le, és hogy a programokat meghibásodáskor félbeszakították, amíg a felmerült nehézséget meg nem oldották.

5.5.5. Az üzenetek hitelesítése

Az üzenethitelesítés alkalmazása esetén észlelhető a továbbított elektronikus üzenet integritásának megváltozása.
Alkalmas módként kriptográfiai módszereket alkalmazhatóak az üzenethitelesítés megvalósítására. Elvárások az üzenethitelesítés, valamint az elektronikus aláírás kialakítása kapcsán:

- az azonosítás és hitelesítés keretében a hozzáférést ellenőrizni kell;
- a hitelesítést a felhasználó és a rendszer között egy, a felhasználó által megnyitott, védett csatornán keresztül kell biztosítani.

5.5.6. A kimenő adatok ellenőrzése

Az adatfeldolgozás rendszerében ellenőrizni kell a kimenő adatokat. A kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:

- integritás ellenőrzés;
- adattartalom meglétének, értékének ellenőrzése;
- a megfelelő minősítés meglétének ellenőrzése;
- a kimenő adatok értékelésében és ellenőrzésében résztvevők feladatainak és felelősségének meghatározása.

A kimenő adatok esetén az adat kiküldését végző személy felelőssége a kiküldés tényének, időpontjának, címzettjének és tartalmának rögzítése és nyilvántartása, amit megvalósíthat a kiküldést biztosító informatikai rendszer révén is.

5.6. Rendszer és szolgáltatás beszerzés eljárásrendje (3.1.3.1. [3]), {16.1}

A beszerzések során követendő szabályokat az Intézetnek a gazdálkodásával összefüggésben hozott szabályzatai alapján kell megvalósítani. Ezen túlmenően hozott, az informatikai rendszerek és szolgáltatások beszerzésére vonatkozó eljárásrend célja, hogy az Intézet ezt az eljárásrendet alkalmazza minden olyan esetben, amelyben informatikai szolgáltatást vagy eszközöket szerez be vagy rendszerfejlesztési tevékenységet végez vagy végeztet.
Az eljárásrendben kerülnek rögzítésre mindazok a követelmények, amelyeket be kell betartani a beszerzés során, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.), és *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet alapján, figyelemmel a Digitális Kormányzati Ügynökség Zrt. és a kormányzati informatikai beszerzések központosított közbeszerzési rendszeréről szóló a 301/2018. (XII. 27.) Korm. rendeletben, valamint a kormányzati informatikai beszerzéssel érintett alkalmazások, informatikai eszközök és szoftverek köréről szóló* 2/2019. (VII. 12.) MK rendeletben, továbbá az Intézet irányító vagy középirányító szerve vonatkozó utasításában foglaltakra.

5.6.1. Erőforrás igény felmérés (3.1.3.2. [3]), {16.2}

Az Intézetnek az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a beruházás, vagy költségvetési tervezés részeként a rendszerek teljes életciklusában meg kell határoznia, dokumentálnia és biztosítania kell az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat. Ennek érdekében az Intézet folyamatosan figyelemmel kíséri az elektronikus információs rendszerek biztonsági elemeinek megbízhatóságát és teljesítményét. A rendszerek biztonságát érintő igények felmerülése esetén az Intézet beszerzési eljárásain belül, de külön dokumentumokban kezdeményezi a szükséges eszközök vagy szolgáltatások beszerzését. Az informatikai erőforrások teljesítményét és kapacitását folyamatosan figyelemmel kell kísérnie az IT infrastruktúra üzemeltetésért felelős személynek (IÜFSZ). Kapacitás határértékek esetén, amennyiben a rendszer mindezt engedélyezi, automatikus riasztásokkal kell figyelmeztetni az adott rendszerért felelős Alkalmazás támogatásáért és üzemeltetéséért felelős személyeket (ATFSZ).
Amennyiben igény merül fel — akár bővítés, akár szolgáltatás kimaradás miatt — adatokat kell gyűjteni az adott elektronikus információs rendszerekből. A következő adatokat kell megnézni:

- az adott elektronikus információs rendszerek aktuális teljesítményei;
- a nyújtott szolgáltatások rendelkezésre állását;
- erőforrásigény növekedésének várható mértékéről (pl.: tárhelykapacitás, felhasználók száma).

A fejlesztések során úgy kell tervezni a hardver erőforrásokat, hogy az igénylő üzleti terület elvárásainak megfeleljen, és az elvárt időszakon belül (pl. egy év) ne igényeljenek további bővítést, arányosak legyenek a rendszerterhelés növekedési ütemével.
Az erőforrás igény felmérése az Informatikai Osztályvezető (IOV) és az IT infrastruktúra üzemeltetésért felelős személy (IÜFSZ) feladata, konzultálva az Alkalmazás támogatásáért és üzemeltetéséért felelős személyekkel (ATFSZ).

5.6.2. Szerződéses követelmények meghatározása a beszerzés során (3.1.3.3.2 [4]), {16.7}

Az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben követelményként meg kell határozni legalább a következőket:

- funkcionális biztonsági követelményeket;
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- a biztonsággal kapcsolatos dokumentációs követelményeket;
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat;
- az átadás — átvétel folyamatának leírását, a tesztelési követelményeket;
- a dokumentáltsági követelményeket.

A fenti követelményeket szerződési sablonokban kell rögzíteni, amelyek alkalmazását kötelezővé kell tenni. Ezek kialakításáért az Informatikai Osztályvezető (IOV), míg az alkalmazásáért a szerződés szakmai anyagának előkészítője felel.

5.6.3. Elfogadási kritériumok

Az új informatikai rendszerekre, a bővítésekre és az új változatokra vonatkozó elfogadási, átvételi kritériumokat rögzíteni kell a következők szerint:

- a rendszer leírását, annak funkcióinak összekapcsolását a folyamatokkal;
- paramétereit, ki- és bemenő adatait, minden olyan további igényt, melyet az Intézet támaszt az új rendszerrel kapcsolatban specifikációba kell foglalni és azt mind a megrendelő, mind a szállító oldalán el kell fogadni a fejlesztés megkezdése előtt;
- a specifikáció szerint kell lefolytatni a tesztelést az érintett felhasználók, alkalmazás rendszergazdák és az adatgazdák bevonásával;
- amennyiben a tesztelések pozitív eredménnyel zárulnak, a szoftver átvehető;
- a szoftvernek maradéktalanul meg kell felelnie a specifikációnak és az Intézet elektronikus információs rendszeréhez illeszkednie kell, mind funkcionális, mind biztonsági szempontból;
- az átadás-átvételi eljárást az Intézet belső szabályait és a jogszabályi előírásokat betartva kell lefolytatni, az eljárás részeként jóváhagyó tesztelést kell végezni, arról és magáról az átadásról is jegyzőkönyvet kell készíteni;
- oktatások megtartása, rendszer és egyéb dokumentációk (felhasználói leírások, üzemeltetési utasítások stb.) átvétele, eljuttatása az összes érintetthez kötelező.

5.6.4. A rendszerre vonatkozó dokumentáció

Az alkalmazásfejlesztés során a fejlesztőtől — függetlenül attól, hogy külső, vagy belső fejlesztő — a következő dokumentumokat kell minimálisan megkövetelni:

- rendszerbiztonsági terv;
- felhasználói kézikönyv;
- üzemeltetési kézikönyv;
- üzletmenet-folytonossági terv (BCP);
- katasztrófa-elhárítási terv (DRP);
- fizikai és logikai rendszerterv;
- topológiai és rendszerarchitektúra ábra;
- mentési utasítás;
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció, amely tartalmazza:
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
  - a fejlesztői módosítások átvezetésének módját,
  - az alkalmazást működtető rendszerelemek (operációs rendszer) frissítésének módját,
  - a biztonsági funkciók hatékony alkalmazását és fenntartását;
  - a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;
- fejlesztői dokumentáció, forrásprogram (amennyiben azt a szerződés lehetővé teszi).

Meg kell követelni az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó üzemeltetési dokumentációt, amelynek tartalmaznia kell:

- az üzemeltető által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
- az üzemeltető kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;
- katasztrófahelyzet kezelési tervet (DRP - akár közös dokumentumban a BCP-vel).

Meg kell követelni az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amelynek tartalmaznia kell:

- felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját;
- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit;
- a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához.

Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

- fizikai és logikai rendszerterv;
- rendszerbiztonsági terv;
- üzemeltetési utasítás;
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

- a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
- a biztonsági funkciók hatékony alkalmazását és fenntartását,
- a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

5.6.4.1. A védelmi intézkedések terv-, és megvalósítási dokumentációi (3.1.3.3.3. [4]) {16.15}

Szerződéses követelményként meg kell határozni, hogy a fejlesztő, szállító hozza létre és adja át az alkalmazandó védelmi intézkedések terv- és megvalósítási dokumentációit, köztük a biztonsággal kapcsolatos külső rendszer interfészek leírását, a magas, és alacsony szintű biztonsági tervet, - amennyiben azzal a szállító rendelkezik - a forráskódot, fejlesztési kézikönyvet és futtatókörnyezetet.

5.6.4.2. Funkciók - protokollok — szolgáltatások (3.1.3.3.4. [4]), {16.13}

A szerződésekben kötelezni kell a szállítókat arra, hogy már a fejlesztési életciklus korai szakaszában meghatározzák a használatra tervezett funkciókat, protokollokat és szolgáltatásokat.

5.6.4.3. Biztonságtervezési elvek (3.1.3.5. [4]), {16.16}

Az informatikai beszerzés teljes életciklusára ki kell terjednie a biztonsági megfelelősségnek, azaz a beszerzési tervek, és az igények engedélyeztetési folyamatába is be kell építeni azokat a követelményeket, amelyek majd a megfelelő biztonságot jelentik. A beszerzési folyamat lépéseibe: ajánlati kiírás, ajánlatok elbírálása, szállító kiválasztása, szerződéskötés, a szerződés tárgyának átvételi procedúrája és a beüzemelés lépései sem zárják le teljesen a beszerzés biztonsági folyamatának követését, ugyanis a beszerzés folyamata során gondolni kell a majdani üzemeltetés során jelentkező olyan folyamatos beszerzésekre, amelyek az informatikai rendszer használatát biztosítják. (pl. alkatrész utánpótlás vagy szoftver rendszerek követése). Az eljárásrend az adminisztratív védelem feltételeit teremti meg a biztonság érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések felsorolásával.

Az IBF-nek véleményezési joga van minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az informatikai biztonságra.

5.6.4.4. Külső elektronikus információs rendszerek szolgáltatásai (3.1.3.6. [2]), {16.49}

A szolgáltatási szerződésekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett külső elektronikus információs rendszerek szolgáltatásai megfeleljenek az Intézet elektronikus információbiztonsági követelményeinek.

Az Intézetnek külső és belső ellenőrzési eszközökkel ellenőriznie kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket (beszállítói minősítés). Az ellenőrzést az IBF végzi szúrópróba-szerűen.

5.6.5. Független értékelők (3.1.3.7. [4])

A független értékelők és felmérő csoportok olyan egyének vagy csoportok, akik pártatlan értékelést adnak az Intézet információs rendszereiről. A pártatlanság azt jelenti, hogy mentesek minden vélt vagy valós érdekütközéstől az információs rendszerek értékelésekor, illetve ez igaz a megállapításaikra is. Ahhoz, hogy a pártatlan legyen egy értékelő:

- nem jöhet létre közös vagy ellentétes érdek az Intézettel;

- nem értékelheti a munkáját a felmért Intézet;
- a törvényt szolgálja és nem a menedzsmentet vagy az alkalmazottakat;
- nem tartozhat érdekvédelmi szervezetekhez.

Az Intézet független értékelőket vagy értékelő csoportokat alkalmazhat a védelmi intézkedések értékelésére, valamint meg kell bizonyosodnia annak függetlenségéről, és a szerződéskötés után is törekedni kell a függetlenség megőrzésére. Ezen értékelés eredményeit gondosan át kell tekinteni, elemezni és a levont következtetéseket, teendőket az intézkedési tervben szükség szerint megjeleníteni.

5.6.5.1. Folyamatos ellenőrzés (3.1.3.8. [3]), {5.16}

Az informatikai biztonsággal összefüggő beszerzéseket az időszakos belső ellenőrzési tervnek megfelelően ellenőrizni kell. Az ellenőrzési tervnek ki kell terjednie a következőkre:

- az ellenőrizendő területek meghatározása;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakorisága;
- az ellenőrzés eredményének értékelésnek módszertana.

Az ellenőrzést az ellenőrzésre kijelölt szervezet, vagy munkacsoport az ellenőrzési tervben foglaltak szerint hajtja végre.
Az ellenőrzés során tett megállapításokból értékelni kell az ellenőrzött terület követelményeknek való megfelelőségét.
Az ellenőrzés megállapításaira, illetve az ellenőrzés értékelésére alapozva intézkedési tervet kell kidolgozni és végrehajtani abban az esetben, ha az ellenőrzés az Intézet által nem tolerálható kockázatot tár fel. Ha az ellenőrzés során személyes felelősség kerül megállapításra, haladéktalanul intézkedni kell a felelősség megfelelő tisztázásáról és a szabályszegés megfelelő szankcionálásáról.
A folyamatos ellenőrzéssel kapcsolatos feladatokat az IBF koordinálja az informatikai beszerzést bonyolító személyek közreműködésével.

5.6.5.2. Folyamatos független értékelés (3.1.3.8.2. [4])

Az Intézetnek független értékelőket vagy értékelő csoportokat célszerű alkalmaznia az elektronikus információs rendszer védelmi intézkedéseinek folyamatos ellenőrzésére. Ennek gyakoriságát rendszerenként az adott elektronikus információs rendszer paramétereinek, besorolásának ismeretében kell a független értékelő segítségével meghatározni, valamint az elektronikus információs rendszerek nyilvántartásában rögzíteni.
A biztonsági ellenőrzések során folytatott folyamatos monitoring folyamat megköveteli, hogy az ilyen értékeléseket vezető értékelők és felmérő csoportok megfelelő szintű függetlenséggel rendelkezzenek.

5.6.6. Fejlesztői változáskövetés (3.3.3.4 [4])

A fejlesztővel kötött szerződésekben ki kell kötni, hogy:

- vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;
- dokumentálja, kezelje és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;
- csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszer szolgáltatáson;

- dokumentálja a jóváhagyott változtatásokat, és ezek lehetséges biztonsági hatásait;
- kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az Intézet által meghatározott személyeknek.

5.6.7. Fejlesztői biztonsági tesztelés (3.3.3.5 [4])

Elő kell írni, hogy az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője:

- készítsen biztonság értékelési tervet és hajtsa végre az abban foglaltakat;
- hajtson végre - a fejlesztéshez illeszkedő módon - egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az Intézet által meghatározott lefedettség és mélység mellett;
- dokumentálja, hogy végrehajtotta-e a biztonság értékelési tervben foglaltakat és ismertesse a biztonsági tesztelés és értékelés eredményeit;
- javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

5.6.8. Fejlesztési folyamat szabványok, eszközök (3.3.3.6 [5])

A fejlesztőt a szerződésben kötelezni kell arra, hogy:

- dokumentált fejlesztési folyamatot kövessen, amelynek keretében:
  - kiemelten kezeli a biztonsági követelményeket,
  - meghatározza a fejlesztés során alkalmazott szabványokat és eszközöket,
  - dokumentálja a fejlesztés során alkalmazott speciális eszköz opciókat és konfigurációkat,
  - nyilvántartja a változtatásokat, és biztosítja ezek engedély nélküli megváltoztatás elleni védelmét,
- az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.

5.6.9. Fejlesztői oktatás (3.3.3.7 [5])

Oktatási kötelezettséget kell előírni az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás szállítója számára, hogy az Intézet által kijelölt személyek - elsősorban az IT infrastruktúra üzemeltetésért felelős személy (IÜFSZ) és az Alkalmazás támogatásáért és üzemeltetéséért felelős személyek (ATFSZ) - a megvalósított biztonsági funkciók, intézkedések és mechanizmusok helyes használatát és működését megismerhessék és elsajátíthassák.

5.6.10. Külső információs rendszerek szolgáltatásai (3.2.3.6 [2]) {16.49}

A szolgáltatási szerződésesekben ki kell kötni, hogy a szolgáltatási szerződés alapján igénybe vett külső elektronikus információs rendszerek szolgáltatásai megfeleljenek az Intézet elektronikus információbiztonsági követelményeinek.
Külső és belső ellenőrzési eszközökkel ellenőrizni kell, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.
Kötelezni kell a szolgáltatót arra, hogy meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

5.6.11. A beszerzések folyamatos ellenőrzése (3.1.3.8.1. [3]), {5.16.}

Az Intézet folyamatba épített ellenőrzési tervet készít és ez alapján hajtja végre az ellenőrzést.

5.6.11.1. Ellenőrzési terv készítése

Az információbiztonsággal összefüggő beszerzéseket az időszakos belső ellenőrzési tervnek megfelelően ellenőrizni kell. Az ellenőrzési tervnek ki kell terjednie a következőkre:

- az ellenőrizendő területekre;
- az ellenőrzések, valamint az ellenőrzéseket támogató értékelések gyakoriságára;
- az ellenőrzés eredményének értékelésnek módszertanára.

5.6.11.2. A védelem szempontjainak érvényesítése a beszerzés során (3.1.3.3.2. [4])

Az IBF-nek meg kell határoznia, hogy miképpen kell védeni az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzett eszköz beillesztéséből adódó kockázatok ellen. Az Intézetnek szerződéses követelményként kell meghatároznia a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések leírását. Ez alapján az IBF dönt arról, hogy ezek megfelelnek-e az Intézet általános védelmi intézkedéseinek, vagy a rendszer védelmi intézkedéseit, védelmi garanciáit szükséges módosítani a szállítás, üzembe helyezés előtt vagy során.

5.6.11.3. Elvárt dokumentáció

A védelmi intézkedések terv-, és megvalósítási dokumentációin felül az alkalmazás fejlesztés során a fejlesztőtől — függetlenül attól, hogy külső, vagy belső fejlesztő, a következő dokumentumokat kell megkövetelni:

- követelmény specifikáció;
- fizikai és logikai rendszerterv;
- rendszerbiztonsági terv;
- felhasználói kézikönyv, mely tartalmazza a következőket:
  - cél és hatókör;
  - fogalmak és rövidítések;
  - a rendszer általános bemutatása;
  - szerepkörök, a felhasználók csoportosítása;
  - felhasználói funkciók: alrendszerenként/képernyőnként leírja a felhasználók számára elérhető funkció használatának módját, feltüntetve az adott funkció elvégzéséhez szükséges szerepköröket is. A dokumentum tartalmazza:
    - a funkció használatának szöveges leírását,
    - a beviteli, illetve kimeneti adatok leírását,
    - adatellenőrzési szabályokat,
    - képernyő képeket,
    - a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját.
    - Szükséges, hogy a kézikönyv adjon magyarázatot az egyes mezőtartalmak összefüggéseiről, határozza meg az esetleges logikailag kapcsolt mezők ellenőrzési szabályait is. Az egyes funkciókhoz, funkciócsoportokhoz kapcsolódó tipikus

használati eset példán keresztül támogassa az adott funkció használatának megértését.

- Használati esetek: a rendszer működési folyamatainak ismertetése, példákkal illusztrálva;
- Konfiguráció, hibaelhárítás:
  - Felhasználói konfigurációk lehetősége;
  - Konfigurációs paraméterek;
- Jellemző hibalehetőségek és azok megoldása:
  - Hibaüzenetek;
  - Hibaelhárítási tevékenységek.

- üzemeltetési kézikönyv;
- rendszerismertető, mely a következőket tartalmazza:
  - a rendszer bemutatása, koncepciója és architekturális vázlata;
  - Futtatási környezet leírása;
  - Kapcsolat más rendszerekkel;
  - Interfészek leírása;
  - Jogosultsági rendszer;
  - Rendszeresen, időszakosan elvégzendő üzemeltetési feladatok:
    - Monitorozás (rendszeres hálózati ill. folyamat monitorozás);
    - Batch futtatás (rendszeresen elvégzendő, döntési pontokat nem tartalmazó vagy teljeskörűen leírható futtatási feladatok);
    - Újraindítás és leállítás (jogosultak és engedélyezők köre, engedélyezés folyamata, újraindítás és leállítás feltételei, értesítés módja és értesítési lánc, végrehajtandó lépések, dokumentálás módja);
    - Outputkezelés (rendszeresen elvégzendő lépések);
    - Biztonsági mentések (rendszeresen elvégzendő lépések);
    - Archiválás (rendszeresen elvégzendő lépések);
    - Rendszerkarbantartás (rendszeresen elvégzendő ellenőrzések);
    - Felhasználó adminisztráció (rendszeresen elvégzendő lépések);
    - Programcsere menedzsment szabályozása és gyakorlata (tartalmazhatja a külső céggel kötött szerződés);
    - A biztonsági események követésének rendje;
    - Karbantartás (tartalmazhatja a külső céggel kötött szerződés); ○ Rendszerhiba esetén szükséges teendők.
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentáció, amely tartalmazza:
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;
  - a fejlesztői módosítások átvezetésének módját;

- az alkalmazást működtető rendszerelemek (operációs rendszer) frissítésének módját,
- a biztonsági funkciók hatékony alkalmazását és fenntartását;
- a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

- üzletmenet-folytonossági terv (BCP),
- katasztrófahelyzet kezelési terv (DRP).

Az infrastrukturális rendszerfejlesztések alkalmával az alábbi dokumentációkat kell elkészíteni:

- rendszerterv;
- rendszerbiztonsági terv;
- üzemeltetési utasítás;
- az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:
  - a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését;
  - a biztonsági funkciók hatékony alkalmazását és fenntartását;
  - a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

A fenti dokumentációtól való egyedi eltérést az Informatikai Osztályvezető (IOV) engedélyezheti.

5.6.11.4. Funkciók - protokollok — szolgáltatások dokumentációja

Az Intézet már a beszerzési folyamat előkészítése során ellenőrzi a használatra tervezett funkciókat, protokollokat és szolgáltatások dokumentációját, amely lehetővé teszi a beszerzett rendszer vagy komponens integrációját.

5.6.11.5. Az ellenőrzés végrehajtása

Az ellenőrzést az Intézet Belső Ellenőrzése az ellenőrzési tervben foglaltak szerint hajtja végre.

5.6.11.6. Az ellenőrzés eredményének értékelése

Az ellenőrzés során tett megállapításokból értékelni kell az ellenőrzött szakmai terület követelményeknek való megfelelőségét.

5.6.11.7. Reagálás az ellenőrzés eredményének értékelésére

Az ellenőrzés megállapításaira, illetve az ellenőrzés értékelésére alapozva intézkedési tervet kell kidolgozni és végrehajtani abban az esetben, ha az ellenőrzés az Intézet által nem tolerálható kockázatot tár fel. Ha az ellenőrzés során személyes felelősség kerül megállapításra, haladéktalanul intézkedni kell a felelősség megfelelő tisztázásáról és a szabálysegés megfelelő szankcionálásáról.

5.7. Üzletmenet (Ügymenet- folytonosság tervezés) (3.1.4.[2], 3.1.4.2. [2]) {7.1}, {7.2}

Az Intézet üzletmenet-folytonossági tervet készít, amely segítséget nyújt abban, hogy kritikus üzleti folyamatok sérülése vagy leállása esetén a lehető legkisebb kieséssel lehessen megvalósítani a visszaállást. Az üzletmenet-folytonossági tervének az alábbi esetekre kell kiterjednie:

- nem tervezett szolgáltatás leállás;
- hosszan tartó szolgáltatás leállás;
- olyan leállás, amit a normális probléma-menedzsment eljárásokon belül nem lehet megoldani;

- olyan leállás, amely komoly károkat vagy veszteségeket okoz.

Az üzletmenet-folytonosság tervben a következő információknak kell szerepelniük:

- eljárások és erőforrások listája, amit a visszaállítás során fel kell használni;
- részletes leírás, amit a felelősök végre tudnak hajtani;
- azon partnerek és belső szereplők azonosítása, akik bevonása indokolt lehet a visszaállítás során;
- a zavar elkerülését segítő részletes útmutatók és a tesztelési eljárások;
- a visszaállításhoz szükséges információk listája;
- a tartalék helyen történő működés szabályai, ha az elsődleges hely nem elérhető;
- az elsődleges helyre való visszatérés eljárásai;
- kritikus, az elektronikus információs rendszer alapfunkcióit támogató rendszerelemek meghatározása;
- alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően;
- hogyan tartja fenn az Intézet az előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is.

Az üzletmenet-folytonossági tervet évenként tesztelni kell. A tesztelés eredményét értékelni kell és az értékelés eredményeképpen el kell végezni a szükséges módosításokat. Az IBF fél évenként ellenőrzi, hogy az informatikai tartalékok folyamatosan működőképes állapotban álljanak rendelkezésre.

Az üzletmenet folytonossági tervet legalább évente felül kell vizsgálni és aktualizálni kell. Aktualizálni kell továbbá minden olyan esetben, amikor az elektronikus információs rendszerben vagy környezetében olyan változás következik be, amely változásokat tesz szükségessé. A felülvizsgálat és kialakítás során figyelembe kell venni az elektronikus információs rendszerrel szemben támasztott biztonsági követelményeket.

Az üzletmenet folytonossági tervet és annak változásait egyeztetni kell a kapcsolódó, hasonló tervekért felelős szervezeti egységekkel, az érintett személyek és szervezeti egységek körében ki kell hirdetni, valamint gondoskodni kell arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

5.7.1. A folyamatos működésre felkészítő képzés (3.1.4.3. [3]), {7.10}

Az Intézet az elektronikus információs rendszer folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;

- a folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben;
- a képzéseket évente el kell végezni az elektronikus információs rendszer mindenkori állapotának megfelelően.

5.7.2. Az üzletmenet-folytonossági terv tesztelése (3.1.4.4. [4])

Az Intézet legalább évente előzetesen lefektetett teszteken keresztül vizsgálja az elektronikus információs rendszerre vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és az Intézet felkészültségének a felmérése céljából. Értékeli az üzletmenet-folytonossági terv tesztelési eredményeit, az értékelés alapján szükség esetén javítja a tervet, a javításokkal kapcsolatban az üzletmenet-folytonossági tervre vonatkozó általános eljárási szabályok szerint jár el.

Az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel egyeztetni kell.
Az üzletmenet folytonossági tervet a tartalék feldolgozási helyszínen is tesztelni kell, hogy az Intézet megismerje az adottságokat, és az elérhető erőforrásokat, valamint értékelje a tartalék feldolgozási helyszín képességeit a folyamatos működés támogatására.

5.7.3. Infokommunikációs szolgáltatások

5.7.3.1. Tartalék infokommunikációs szolgáltatások (3.1.4.7. [4], 3.1.4.7.3. [4])

Az Intézet a lehetőségeihez mérten tartalék infokommunikációs szolgáltatásokat létesít és tart fenn, amely:

- lehetővé teszi az elektronikus információs rendszer alapfunkciói számára azok 24 órán belüli újrakezdését, amennyiben az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen;
- amely csökkenti az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

5.7.3.2. Szolgáltatások prioritása (3.1.4.7.2. [4])

Az Intézet elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására kötött szerződésében ki kell kötni a szolgáltatás-prioritási rendelkezéseket, az Intézet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

5.7.4. Az elektronikus információs rendszer mentései (3.1.4.8.[3]), {7.35}

Az elektronikus információs rendszer mentéseinek és archiválásának szabályait rendszerenként meg kell határozni az alábbiak figyelembevételével.
A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az Intézet rendszerei előre nem látható esemény bekövetkezte után szükség esetén helyreállíthatók legyenek, ezáltal ne sérüljenek az információk, adatok, rendszerek rendelkezésre állásának kritériumai.
Az adatmentésnek és archiválásnak mindig a lehető legfrissebbnek kell lennie. A mentés gyakoriságát ennek megfelelően kell meghatározni. Rögzíteni kell a mentések végrehajtásának idejét, módját és felelősét. Minimálisan a következő mentéseket kell elvégezni (amennyiben a műszaki adottságok lehetővé teszik):

- a szervereken tárolt adatokról automatikus napi mentést kell készíteni;
- a mentésekért felelős rendszergazdának a központi szerverek teljes adattartalmáról napi, heti és havi mentéseket kell készítenie;
- a tranzakció alapú rendszerek esetén tranzakció alapú mentést kell készíteni, ami lehetővé teszi a tranzakció helyreállítást.

Az Intézet naponta mentést végez a következő elemekről, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

- az elektronikus információs rendszerben tárolt felhasználó- és rendszerszintű információkról;
- az elektronikus információs rendszer dokumentációjáról.

Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.
Az archív biztonsági másolatok kezelése esetében az alábbi körülményeket is tisztázni kell:

- biztonsági osztályba sorolás eredménye alapján az archiválási osztályokat, valamint az archiválások gyakoriságát meg kell határozni az egyes rendszerek esetében;
- a külön is mentett és archivált adatok esetében ezeknek körét meg kell határozni;
- az archiválások átvételi pontra történő eljuttatásának folyamatát ki kell dolgozni;
- meg kell határozni a hordozó média típusát, valamint tárolási helyét és körülményeit;
- a megfelelő feladatkörhöz hozzá kell rendelni az archív médiához való hozzáférés jogát is.

Fontos, hogy az archivált rendszerek futtatási környezetét, architektúrájának leírását, teljes dokumentációját is archiválni szükséges, amit minden verzióváltás után frissíteni kell. Fejlesztetett rendszerek esetén lehetőség szerint a dokumentációnak tartalmaznia kell a fejlesztési környezetet is, hogy reprodukálható legyen a rendszer.
A felelős informatikus köteles esetenként, de legalább 30 naponta a mentések elvégzését és megbízhatóságát ellenőrizni, valamint az archív mentések olvashatóságát és helyreállíthatóságát rendszeresen, de legalább évente ellenőrizni kell.

5.7.4.1. Mentési eszközök

Biztosítani kell, hogy a mentett adatok mindig visszaolvashatók legyenek, ezért a mentéseket olyan eszközökkel kell elvégezni, amelyek garantálják a mentett adatok visszaolvashatóságát. Időnként (minimum évenként) próba visszatöltést (vagy ezzel egyenértékű eljárást) kell megvalósítani az alkalmazott eszközök és módszerek megbízhatóságának ellenőrzése céljából. A mentések elvégzéséhez biztosítani kell a megfelelő számú adathordozó egységet. Folyamatosan figyelemmel kell kísérni a mentendő adatmennyiség változását, és ennek megfelelően kezdeményezni új adathordozók beszerzését. Minden médiatípus esetén legalább 10% tartalékot szükséges tartani.
A mentéshez használt mentési médiák használati idejét a gyártó által megadott élettartam figyelembevételével, 10%-os biztonsági tartalékkal kell meghatározni. Az élettartamot figyelembe kell venni mind a többszöri felhasználásnál, mind pedig a hosszú távon megőrzendő adatok tárolásánál. Az élettartamok figyelését a mentésért felelős munkatársaknak kell elvégezniük. Amennyiben egy média élettartama meghaladta a használati időt, a mentésért felelős munkatársnak kell kezdeményeznie a média selejtezését, és az új média beszerzését.

5.7.4.2. A mentett adatok tárolása

A mentéseket mindig biztonságos helyen kell tárolni. Biztosítani kell, hogy a mentett állományok csőtörés, tűz vagy lopás során ne semmisülhessenek meg.
A biztonsági mentéseket és archiválásokat tartalmazó offline adathordozókat minden esetben a szervertől elkülönített helyiségben elzárva kell őrizni.
Tekintettel arra, hogy az Intézet rendszereinek mentései olyan adatokat tartalmazhatnak, amelyek jogszabályi előírás alapján adatbiztonsági szempontból érzékenyek, szükséges, hogy a mentés során ezek az adatok titkosítva, vagy illetéktelenek számára elérhetetlenül kerüljenek tárolásra.
Javasolt, hogy az adathordozók számmal és vonalkóddal is azonosíthatók legyenek. Az adathordozókkal végzett tevékenységeket az azonosító számhoz kötve ajánlatos dokumentálni. Amennyiben nem áll rendelkezésre olyan technika, amellyel a mentési média címkézése a fent említett módon megtehető, kiemelt figyelmet kell fordítani az egyes mentési elemek egyedi azonosítására.

5.7.4.3. Biztonsági tárolási helyszín (3.1.4.5. [4])

Az Intézet kijelöl egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja.
A biztonsági tárolási helyszínnek el kell különülni az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.
A biztonsági tárolási helyszínhez történő hozzáférés érdekében - meghatározott körzetre kiterjedő rombolás vagy katasztrófa esetére - vészhelyzeti eljárásokat kell kidolgozni.

5.7.4.4. Visszatöltési eljárások

Abban az esetben, ha visszatöltésről nem készül elektronikus naplóállomány, a visszatöltési tesztekről vagy az üzemelő rendszerbe történő visszatöltésről jegyzőkönyvet kell készíteni a következő tartalommal:

- visszatöltött rendszerek;
- visszatöltés időpontja;
- visszatöltést végző neve;
- visszatöltött adatmennyiség, amennyiben ez ismert;
- visszatöltési idő (kezdés/vég időpont);
- visszatöltés során szerzett tapasztalatok, észrevételek.

A visszatöltési tapasztalat alapján, szükség esetén elvégzendő a visszatöltéshez kapcsolódó dokumentációk frissítése is. A visszatöltési idő összehasonlítandó a korábbi tesztek eredményével, hogy a visszatöltési időben bekövetkező kedvezőtlen trendek időben észlelhetők legyenek.

5.7.4.5. Mentési feladatok

A mentési tevékenységgel megbízott felelőst vagy alvállalkozót az Informatikai Vezető jelöli ki. A mentésért felelős személy/alvállalkozó feladata:

- mentések ütemezése;
- mentési job-ok beállítása (honnan - hova és mit mentsen);
- mentések elvégzése;
- mentési média ellenőrzése és rendelkezésre állás biztosítása;
- mentés folyamatának ellenőrzése;
- mentés eredményének ellenőrzése.

A mentéseket lehetőleg úgy kell elvégezni, hogy azzal a felhasználók munkáját ne akadályozzák. A rendszergazda feladata ellenőrizni, hogy a meghatározott mentési rend alapján az adatminősítésnek megfelelően a visszaállítási eljárások során is csak az arra jogosult személyek férhessenek hozzá a visszaállítandó adatokhoz.

5.7.4.6. Mentési naplók

A mentések végrehajtásáról naplót kell vezetni, amelynek a következőket kell tartalmaznia:

- a mentés tartalmát;
- a mentés időpontját;
- mentés jellegét (teljes mentés, inkrementális kumulatív, inkrementális, differenciált stb.);
- a mentés eredményét (sikeres / sikertelen, hiba oka).

Amennyiben a mentést mentőrendszerrel végzik, a mentési naplót a mentőrendszer automatikusan generálja. A mentési naplókat ebben az esetben is, - a mentőrendszer nélkül is olvasható formátumban kell tárolni, a mentésekkel azonos biztonsági körülmények között.
Amennyiben a mentésről az adott rendszer nem készít automatikus mentési naplót, a mentés tételes dokumentálása a mentésért felelős személy feladata és felelőssége. A tárolásra, valamint kezelésére vonatkozó előírások ebben az esetben is érvényesek.
A biztonsági eseménynaplókat ajánlott 5 évre visszamenőleg, a napi mentéseket minimum 3 hónapig, az egyedi mentéseket pedig a mentést elrendelő szervezeti vezető utasításának megfelelő ideig őrizni.
Ha az előírt mentéseket valamely okból nem lehet megvalósítani, már meglévő korábbi mentéseket nem szabad törölni.

5.7.4.7. Megbízhatósági és sértetlenségi teszt (3.1.4.8.2. [4])

Negyedévente tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.
Az IT üzemeltetését felelős vezető a mentési média gyártóinak ajánlását figyelembe véve kialakítja az ellenőrzési rendet, amely alapján a mentéseket ellenőrizni kell sértetlenségükkel kapcsolatban. Ez magába foglalja az adathordozókat, melyeken a mentett anyagokat tárolják. Ezeket megbízhatósági szempontok alapján szintén ellenőrzés alá kell vonni.

5.7.5. Minősített adatok, elektronikus dokumentumok tárolása

Biztosítani kell, hogy a tárolóeszközökön levő programok, és adatállományok listája mindig az érvényes állapotot tükrözze vissza. Ezt a dokumentumot a biztonsághoz kapcsolódó többi dokumentummal együtt, azokkal azonos biztonsági szinten kell őrizni. A papír alapú dokumentumhoz kapcsolódó részletes szabályozásokat az Intézet iratkezelési szabályzata tartalmazza, e szabályzatnak megfelelően szükséges eljárni.
Minősített adatokat a 2009. évi CLV. törvény (Mavtv.) által előírt szigorú rendelkezések szerint lehet kezelni, de alapesetben minősített adatot kizárólag papír alapon, vagy a jogszabály alapján erre rendszeresített stand-alone gépen, ill. adathordozókon rejtjelezve lehet tárolni.
Az elektronikus dokumentumokat oly módon kell megőrizni, amely kizárja az utólagos módosítás lehetőségét, a törlési határnapig folyamatosan biztosítja a jogosultak által a hozzáférhetőséget, valamint az elektronikus dokumentumok értelmezhetőségét (olvashatóságát).
Az elektronikus dokumentumokat védeni kell a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen.
Dokumentumba kell foglalni, hogy mely adatállományok és programok nem változtathatók meg, illetve, ha erre sor kerül, akkor az, hogy kinek az engedélyével és ki által végezhető el. A változtatást lehetőleg a tárolóeszközön kialakítható fizikai írásvédelemmel kell megakadályozni. Azon rendszerekben tárolt dokumentumok és adatok védelmét, tárolását és megőrzését a fentieknek megfelelőnek lehet tekinteni, ahol a rendszer szállítója a rendszer ezek feltételek biztosítására vonatkozó zártságra nyilatkozatot ad.
Ha az utólagos módosítás lehetőségének kizárása úgy történik, hogy az elektronikus dokumentumot fokozott biztonságú elektronikus aláírással vagy minősített elektronikus aláírással látják el, és a megőrzésre kötelezett személy a megőrzési kötelezettségének maga tesz eleget, úgy köteles az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény alapján a Nemzeti Média- és Hírközlési Hatóság által határozatban közzétett mindenkori

biztonságos kriptográfiai algoritmussal ellátott időbélyegzőt elhelyeztetni az elektronikus dokumentumon olyan szolgáltatóval, amely e szolgáltatást minősített szolgáltatóként nyújtja.

5.8. Biztonsági események figyelése és kezelése (3.1.5.)

5.8.1. Biztonsági események figyelése (3.1.5.4.[3], 3.1.7.1. [3]) {9.25}, {1.16}

Az Intézet minden informatikai eszközén, folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit. A felhasználóknak figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket. A hiba elhárítására szükség esetén a felhasználó vegye fel a kapcsolatot az illetékes (az alkalmazás üzemeltetéséért felelős, illetve ügyeletes) informatikai munkatárssal.
Minden az informatikai rendszereket érintő vagy az informatikai rendszerekkel összefüggésbe hozható biztonságot veszélyeztető eseményt vagy annak gyanúját haladéktalanul jelenteni kell az Informatikai Osztályvezetőnek (IOV) és az érintett (az alkalmazás üzemeltetéséért felelős, illetve ügyeletes) informatikusnak, illetve mindent meg kell tenni a szükséges bizonyítékok összegyűjtésére.
Az Intézet az incidensek kezelésére célszoftvert alkalmazhat, mely szoftver működésének e szabályozás elemeit szükséges tükröznie.
Ezen felül az Intézet kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott intézményrendszerével (pl. NKI, govCERT, OKFÓ adatbiztonsági szervezeti egység):

- az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek folyamatos oktatásának, képzésének elősegítése érdekében;
- az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása érdekében;
- a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében.

5.8.2. Biztonsági események priorizálása, reagálás a biztonsági eseményekre

A biztonsági incidenseket a következők szerint kell priorizálni és reagálni:
Az **1. prioritású** incidensek kivizsgálását és elhárítását munkaidőben az észlelést követően azonnal, munkaidőn túl 4 órán belül meg kell kezdeni:

- határsértés és illegális tevékenység észlelése (behatolás),
- vírus-vészhelyzet (tömeges fertőzés), vagy központi vírusvédelmi eszköz tartós kiesése,
- adminisztrátori jogosultságok sérülése,
- rendelkezésre állás szerint 3-as, vagy ennél magasabb biztonsági osztályba sorolt rendszer, vagy rendszer elemek teljes, az üzemmenetre jelentős kihatással bíró kiesése,
- informatikával összefüggésbe hozható bűncselekmények bekövetkezésének megalapozott gyanúja.

A **2. prioritású** incidens elhárítását munkaidőben az észlelést követően azonnal, munkaidőn kívül 6 órán belül meg kell kezdeni, ha az 1. prioritású incidens elhárítását nem akadályozza:

- ismétlődő vírusfertőzés, vagy vírusdefiníciós állomány nem frissülése,
- felhasználói jogosultságok sérülése,
- rendelkezésre állás szerint 2-es biztonsági osztályba sorolt rendszernek, vagy rendszer elemeknek az üzemmenetre jelentős kihatással bíró kiesése,
- védendő adatok és információk bizalmasságának, sértetlenségének elvesztése.

A **3. prioritású** incidensek kivizsgálását munkaidőben az észlelést követően kettő órán belül, munkaidőn kívül 8 órán belül meg kell kezdeni. Ilyen például a/az:

- egyszeri vírusfertőzés, vagy helyi vírusvédelmi eszköz kiesése,
- rendelkezésre állás szerint 1-es biztonsági osztályba sorolt rendszer, vagy rendszer elem kiesése,
- információk bizalmasságának, sértetlenségének elvesztése,
- kisebb jogosultsági incidensek (felhasználó elfelejtette a jelszavát, vagy az lejárt stb.),
- szabálysértések bekövetkezésének megalapozott gyanúja.

A **4. prioritású** incidensek kivizsgálását kezelését a folyamatban levő magasabb prioritású incidensektől függően kell megkezdeni. Ilyen például a:

- vírusvédelmi menedzsment eszközök kiesése,
- felügyeleti és menedzsment eszközök,
- munkaállomás működésével kapcsolatos működési hibák,
- belső szabály- és eljárássértések,
- felhasználói hibák.

Az incidensek priorizálása az Informatikai Osztályvezető (IOV) feladata.

5.8.3. A biztonsági események kezelése (3.1.5)

5.8.3.1. Általános alapelvek

Informatikai biztonsági incidens előfordulása esetén az abban érintett felhasználóknak törekedni kell a biztonsági események, zavarok okozta károk minimalizálására, valamint a biztonsági események folyamatos nyomon követésére, annak érdekében, hogy a megfelelő következtetéseket az illetékesek levonhassák. Mérsékelni kell a biztonságot befolyásoló események és működési zavarok következményeit, nyomon kell követni az eseményeket, biztosítani kell a mielőbbi normál üzemre való visszaállást és a tapasztalatokat írásban kell rögzíteni.

Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett munkaállomást, számítógépet / alhálózatot le kell választani a hálózatról, szükség esetén ki kell kapcsolni, vagy a teljes alhálózat működését szüneteltetni kell. Ilyen esetekben fokozottan figyelni kell az adathordozókra is, melyeket az illetékes informatikai munkatársnak vizsgálat céljára át kell adni. A meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

A biztonsági eseményekről tájékoztatást kell küldeni:

- 1-es és 2-es prioritás esetében az Informatikai Osztályvezető (IOV) észrevételeivel kiegészítve a Főigazgatónak (FOIG), a Főigazgatói Hivatal vezetőjének;
- és 4. prioritás esetében az Informatikai Osztályvezető (IOV) számára;
- 1-es és 2-es prioritás esetében a Belügyminisztérium Nemzeti Kibervédelmi Intézet számára.

5.8.3.2. Az incidenskezelés folyamata (3.1.5.1 [3]) {9.1}

Annak érdekében, hogy az informatikai biztonság folyamatosan, minden területen a kívánt biztonsági szinten működjön, a következőket kell érvényesíteni a napi munkavégzés során:

- A biztonsági incidenseket észleléskor — egykapus rend kialakításával — jelenteni kell az Informatikai Osztályra e-mail-en, vagy jegykezelő rendszerben. Ha a hiba jellegéből adódón e-mailben nem lehetséges - telefonon kell megtenni és a dokumentációt később kell elvégezni.

- A bejelentés fogadása után, ha az informatika önálló hatáskörben nem tudja kezelni a felmerült problémát, értesíti az illetékes támogató munkatársat vagy alvállalkozót.
- Amennyiben a probléma megoldható e-mailben nyújtott válaszadással is, a leírt lépéseket a felhasználónak pontról-pontra kell végrehajtania. Amennyiben a felhasználónak küldött problémamegoldó e-mailre 2 napon belül nem érkezett válasz, akkor a problémát lezártnak kell tekinteni.
- Ha a hiba nem oldható meg távolról, a hiba elhárításával megbízott munkatárs/alvállalkozó felkeresi a kezdeményező felet, és a helyszínen hárítja el a hibát az IBF vagy megbízottja felügyelete mellett, az adott rendszerre vonatkozó adatbiztonsági szabályok betartásával. Olyan elektronikus információs rendszerek esetén, amelyek személyes adatokhoz férnek hozzá, ezek védelmére fokozott figyelmet kell fordítani. Ha a hiba nem hárítható el a helyszínen, a munkatárs/alvállalkozó az eszközt dokumentáltan átveszi, és a be- és kiszállításra vonatkozó előírások fokozott figyelembevétele mellett elszállítja hibaelhárításra.
- Távoli segítségnyújtás során a probléma elhárítását végző informatikai munkatárs a felhasználó számítógépe felett, a felhasználó engedélyével ideiglenesen átveheti az irányítást, illetve megtekintheti annak tartalmát. Ilyenkor a felhasználó képernyőjére, aktuális folyamataira az adott munkatársnak teljes rálátása és irányítási lehetősége van. Olyan megoldás alkalmazható csak, amelynél a számítógép felhasználója vizuálisan érzékeli az irányítás átvételét. Olyan elektronikus információs rendszerek esetén, amelyek személyes adatokhoz férnek hozzá, ezek védelmére fokozott figyelmet kell fordítani.
- A biztonsági incidenseket dokumentálni szükséges a következők figyelembevételével:
  - a rögzített incidensekből statisztikai adatként ki lehessen nyerni az egyes fenyegetettségek bekövetkezési valószínűségét (a kockázatelemzéshez szükséges),
  - felhasználói incidensekből statisztikailag ki lehessen nyerni az elkövetési magatartást,
  - üzemeltetési incidensek esetén statisztikailag ki lehessen nyerni a szolgáltatásokra vonatkozó incidensek számosságát,
  - a biztonsági incidensekből folyamatosan levont tapasztalatokat vissza lehessen csatolni a védelmi rendszer tervezése, szervezése folyamataira.
- A szerver oldali és hálózati hibák a felhasználók nagy többségét érintik. Ezen hibaelhárítás a végfelhasználói prioritással szemben előnyt élvez, ezért szükség esetén a végfelhasználói hibaelhárítási folyamat az Informatikai Osztályvezető (IOV) döntésére felfüggesztendő.
- Az incidensek priorizálása az Informatika feladata, az Informatika munkatársainak ezen irányú képzéséért az Információbiztonsági felelős felel. Abban az esetben, ha az incidenst az adott területen illetékes rendszergazda észleli és jelenti be, az incidens priorizálása az ő feladata. Ebben az esetben bejelentés alkalmával az Informatika felé megadja az incidens prioritását is.

5.8.4. Képzés a biztonsági események kezelésére (3.1.5.9. [3]) {9.2}

Az Intézet biztonsági eseménykezelési képzést biztosít az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepköröknek és felelősségnek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;

- a képzéseket évente el kell végezni az elektronikus információs rendszer mindenkori állapotának megfelelően, vagy amikor az elektronikus információs rendszer változásai megkívánj a.

A képzések megszervezése és lebonyolítása az Informatikai Osztályvezető (IOV) feladata, amihez figyelembe kell vennie az Intézeti és külső szabályzók által elvárt tartalmakat és eljárásokat.

5.8.5. A biztonsági események kezelésének tesztelése (3.1.5.9.4.[4])

Évente legalább egy alkalommal tesztelni kell mindegyik kritikus elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességet, előre kidolgozott tesztek felhasználásával, annak érdekében, hogy megállapítható legyen azok biztonsági eseménykezelésének hatékonysága. A tesztelés eredményét dokumentálni kell.
A biztonsági eseménykezelés tesztelését az illetékes munkatársakkal egyeztetve kell végrehajtani. Az egyeztetések jegyzőkönyveit legalább 1 évig meg kell őrizni.

5.8.6. Informatikai incidensek nyilvántartásba vétele (Segítségnyújtás a biztonsági események kezeléséhez) (3.1.5.7 [3]), {9.31}

Az informatikai incidenseket nyilvántartásba kell venni. A nyilvántartást úgy kell vezetni, hogy abból statisztikai információkat lehessen kinyerni az egyes fenyegetettségekre, illetve a következő rendszerelemekre vonatkozóan: bekövetkezési gyakoriság, éves rendelkezésre állási idő, kiesési idő.
A statisztikákat évente elemezni kell, és az Informatikai Osztályvezetőnek meg kell állapítania, hogy:

- melyek az adott incidensek bekövetkezési tendenciái;
- elfogadható mértékű-e (gyakoriságú) az incidens;
- szükséges-e a kontrollokon változtatni, szigorítani, hogy az adott incidens bekövetkezési valószínűsége csökkenjen.

Az incidensek bejelentésével és kezelésével kapcsolatban a felhasználók számára segítséget és tájékoztatást adnak az informatikai osztály munkatársai, valamint az Intézetben bevezetett automatizált támogató eszköz/mechanizmusok.

5.9. Emberi tényezőket figyelembe vevő — személy — biztonság (3.1.6., 3.3.1.4. [2]) {14.1}

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed az Intézet teljes személyi állományára, valamint minden olyan természetes személyre, aki az Intézet elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem az Intézet dolgozója, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

5.9.1. Munkakörök, feladatkörök biztonság alapú besorolása (3.1.6.2. [3]), {14.2}

Minden, felhasználót be kell sorolni biztonsági szempontok alapján a következő kategóriákba:

- **ALAP BIZTONSÁGI OSZTÁLY** (Nem vezető beosztású, nem bizalmas adatokkal történik a feladat(ok) végrehajtása, kritikus rendszerekhez hozzáférés nem szükséges.)
- **FOKOZOTT BIZTONSÁGI OSZTÁLY** (Nem vezető beosztású, nem bizalmas adatokkal történik a feladat(ok) végrehajtása, kritikus rendszerekhez hozzáférés szükséges.)

- **KIEMELT BIZTONSÁGI OSZTÁLY** (Vezető beosztású, bizalmas adatokkal történik a feladat(ok) végrehajtása.)

A munkaköri és feladat besorolásokat rendszeresen felül kell vizsgálni és szükség esetén megfelelően módosítani kell.

5.9.2. Személyi biztonság a munkaerő felvételénél

Az emberi hibák, lopás, csalárd magatartás vagy a létesítmények és az eszközök nem megfelelő használata során fellépő, az előírások szándékos vagy véletlen megsértéséből eredő biztonsági kockázatokat mérsékelni kell, a következők szerint:

- A biztonsági követelményeket a munkaerő-felvételnél, a munkaszerződésekben, valamint a munkaerő foglalkoztatása során egyaránt érvényesíteni kell.
- A munkaerő-felvételi eljárás során — a jogszabályi előírások keretei között — olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező informatikai biztonság oldaláról tekintett alkalmasságáról. Ez különösen fontos az informatikai biztonság szempontjából kiemelt fontosságú munkakörök esetén.

A Humánpolitikai és Munkaügyi Osztály az új munkatárs munkába állása előtt, legkésőbb a munkába állás napján köteles az Informatikai Osztályvezetőt vagy az ezzel megbízott informatikai munkatársát tájékoztatni. A bejelentést írásos formában (nyomtatott, vagy e-mail, vagy online felületen át) kell megtenni. Az új munkatárs hozzáférési jogosultságát az érintett vezető haladéktalanul köteles igényelni az Informatikai Osztályvezetőnél.
A beérkezett igényekre az Informatikai Osztályvezető haladéktalanul köteles visszajelezni, és — amennyiben azok rendelkezésre állnak — a szükséges technikai eszközöket biztosítani.

5.9.3. Adatvagyon kezelése, hozzáférése

Az adatok kezelésével, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott munkavállalók az adatokhoz csak a feladatuk ellátásához szükséges mértékben férhetnek hozzá.
Az adatvagyon felhasználása, elérése, módosítása, másolása, törlése kizárólag a felhasználónak személyre szabottan biztosított jogosultságnak megfelelően történhet.
Minden felhasználó az adatvagyont köteles úgy kezelni, hogy az teljes mértékben megfeleljen az általa ellátott feladatok jellegének, illetve célkitűzéseknek.

5.9.4. Jogosult felhasználók

Az Intézet szervezeti egységének vezetője (SZEV) az irányítása alá tartozó új dolgozó munkába lépését megelőzően írásban köteles a szervezeti egységhez tartozó munkavállalóra vonatkozóan a hozzáférési jogosultság mértékét meghatározni, amit haladéktalanul köteles az Informatikai Osztályvezető részére eljuttatni. A szervezeti egység vezetője (SZEV) a fentiekben említett jogosultságok meghatározása során az adott dolgozó által ellátott feladatokhoz elengedhetetlenül szükséges mértékű jogosultságot köteles meghatározni. Ezzel kapcsolatos döntéséért teljes felelősséggel tartozik. A szervezeti egység vezetője csak olyan jogosultságok megadását kérheti, amellyel ő maga is rendelkezik vagy — felelősségi köréből fakadóan — rendelkezhetne, ezt meghaladó igény esetén a megfelelő szintű felettes jóváhagyása szükséges. Amennyiben a hozzáférési jogosultság mértékét utólag módosítani szükséges, fenti kötelezettségnek a módosításra okot adó körülmény felmerülésétől számított lehető

legkorábbi időpontban, de legfeljebb 2 munkanapon belül, szükség esetén soron kívül, azonnali hatállyal kell eleget tenni.
Az Informatikai Osztályvezető és az adatok mentését, karbantartását végző rendszergazda feladatai ellátásához szükséges mértékig az adatállományokhoz hozzáférhet, az adatokat azonban nem használhatja fel más célra, és nem hozhatja mások tudomására.

5.9.5. Informatikai biztonság a jogviszony létesítésekor

Az Intézettel Felhasználói jogosultságot keletkeztető jogviszonyba kerülő valamennyi személy - a szükséges információk, dokumentumok Intézet által biztosított megismerhetővé tételét, esetlegesen szükséges oktatás megtartását követően - köteles nyilatkozni, hogy az Intézet informatikai biztonsági előírásait megismeri és magára nézve kötelezőnek tekinti. Ugyanilyen tartalmú nyilatkozatot kell tennie abban az esetben is, ha a jogviszony fennállása során válik Felhasználóvá. Az informatikai biztonsággal kapcsolatos szabályzók jelentős mértékű változása esetén a már jogviszonnyal rendelkezőktől is kérhető nyilatkozat.

5.9.6. Informatikai biztonság a munkaköri leírásokban

A munkaköri leírásnak tartalmaznia kell az adott feladatkörre vonatkozó, az informatikai biztonsággal kapcsolatos, az általános szabályozáson túlmenő speciális követelményeket is, a felelősség egyértelmű megjelölésével. A munkaköri leírásnak a rendszer használatával kapcsolatos feladatokat és felelősségeket tartalmaznia kell az ezzel kapcsolatos elvárások, kötelezettségek meghatározása mellett.

5.9.7. Viselkedési szabályok az interneten (3.1.6.9. [1]), {13.4}

Az Intézet internet használati jogokkal rendelkező felhasználói a munkájukkal kapcsolatban korlátlanul használhatják az Intézet által biztosított internet szolgáltatást. Az internet szolgáltatásait azonban erre vonatkozó különleges engedély hiányában (BYOD engedély) csak munkahelyi eszközökön és csak a munkahelyi feladatok ellátására szabad igénybe venni. A felhasználók az Intézet nevében csak a kijelölt felelős előzetes engedélyével tölthetnek fel internetre adatokat, anyagokat.
Az Intézet tulajdonát képező adatbázisok tartalmának interneten keresztül történő hozzáférésének lehetővé tétele csak az erre felhatalmazott felelős (adatgazda) írásbeli engedélyével megengedett. Az engedély megadása ilyen esetben vonatkozhat egyedi esetre vagy egyes rendszerekkel kapcsolatos feladatok elvégzésére az arra felhatalmazott munkatársak részére.
Az internet magán célú használata kizárólag az Informatikai Osztályvezető (IOV) előzetes általános vagy egyedi engedélyezése alapján lehetséges. Ebben az esetben az alábbi szabályokat kell betartani:

- Tilos a pornográf tartalom, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása.
- Az internetről az Informatikai Osztályvezető (IOV) által nem engedélyezett magán céllal tilos fájlokat letölteni.
- Informatikai biztonsági megfontolásokból tilos a csevegő és azonnali üzenetküldő programok használata. Kivétel ez alól az Intézet által biztosított hasonló szolgáltatást nyújtó, illetve az erre kijelölt szoftver használata.

A fenti szabályok alapján követendő szabályok részletes meghatározása az Informatikai Osztályvezető feladata.

5.9.8. E-mail használat

A belső hálózaton hozzáférhető levelezőrendszer munkaeszköznek minősül, adattartalmának ellenőrzésére a munkáltató jogosult. A levelezőrendszer magáncélú használata korlátozott keretek között biztosított az alábbiakban foglaltak szerint.
Az intézményi levelezőrendszer magáncélú levelezésre nem használható. A magáncélú használatot is érintő, szükségképpen megvalósuló adatkezelés (informatikai rendszerben történő tárolás, törlés stb.) során fokozottan érvényesíteni kell a célhoz kötöttség elvét és a levéltitok védelmét. A nem kívánatos adatkezelés elkerülése érdekében a felhasználó köteles magáncélú leveleit — különösen a beérkező leveleket —azonnal, de legkésőbb 48 órán belül törölni/eltávolítani. A felhasználó előzetes tájékoztatását követően az Intézet a levelezést jogosult ellenőrizni.
A felhasználó tudomásul veszi, hogy az Intézet jogosult az email-fiók ellenőrzésére, amelynek során a felhasználót együttműködési kötelezettség terheli.

A felhasználóknak az elektronikus levelező szolgáltatás használatának folyamán az alábbi szabályokat kell betartaniuk:

- A levelek nem képviselhetnek a hatályos magyar jogba ütköző vagy erkölcsileg kifogásolható magatartásformát (pl.: tiltott tartalmak — pornográfia, szerzői jogok megsértése. stb.).
- Tilos kéretlen levelek (spam), láncievelek, hoax-ok, adathalászati célú levelek (phising), illetve bármilyen „nem hasznos" üzenetek akár belső, akár külső e-mail címek felé küldése, továbbítása. (lásd. előzőekben).
- Tilos a felhasználóknak az intézményi e-mail címüket nem feladatuk ellátásához köthetően használni (pl.: regisztráció letöltési weboldalak, online játékoldalak stb.).
- Levelet küldeni csak a levél tartalmában érintett személy(ek) részére szabad.
- Tilos a levelek fejlécének megváltoztatása, hamis levelek küldése.
- Ismeretlen feladótól érkező, gyanús, csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl.: idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait, illetve a kapott linkeket nem szabad megnyitni, e leveleket törölni kell.
- A levelezés nem veszélyeztetheti az intézeti infrastruktúra működését.

Informatikai biztonsági vizsgálat, auditálás, illetve hibakeresés céljából az informatikai rendszer teljes hálózati forgalma megfigyelhető és rögzíthető. Időszakos, illetve rendszeres biztonsági vizsgálat, avagy auditálás során a levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra:

- kéretlen levelek;
- vírusokat tartalmazó levelek;
- informatikai támadásokat megvalósító üzenetek;
- adathalászatot megkísérlő üzenetek.

Az Intézetben az e-mail címeket a következő konvenció szerint kell képezni:

<vezetéknév><keresztnév első betűje>@nyiro-opai.hu.

Az elektronikus levélként érkező hivatalos megkeresések iktatására az Iratkezelési Szabályzat rendelkezéseit kell alkalmazni.

Az elektronikus leveleket kizárólag azon címzettek számára kell továbbítani, akik számára a levelezés ismerete tényleges szükséges, különös körültekintéssel a csoportos levelezőlista vagy ismerten több személy által közösen használt e-mail cím (pl. szervezeti egység címe) esetén.

5.9.9. A felhasználó feladatai a munkahely elhagyásakor (3.1.6.4. [1]), {14.5}

A munkavállaló, amennyiben munkavégzését befejezte, vagy szünetelteti, és felügyelet nélkül hagyja számítógépét, úgy azt zárolni köteles.
A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy az iroda minden helyisége, ablakai, ajtói zártak legyenek, és - ahol van — a biztonsági berendezések (pl. riasztó) élesítve legyenek.
Amennyiben a munkahelyen folyamatos munkavégzés történik, és a számítástechnikai eszközöket többen közösen használják, az eszköz átadáskor a felhasználó köteles meggyőződni arról, hogy valamennyi munkavégzése során használt rendszerből kijelentkezett.

5.9.10. Tiszta asztal, tiszta képernyő szabályok a munkavégzés közben

Az érzékeny és egyéb védendő adatokat tartalmazó dokumentumokat, IT adathordozókat, mobil eszközöket a munka végeztével, illetve hosszabb távollét esetén munkanap közben is megfelelően el kell zárni.
Számítógép és mobil eszközök képernyő asztalaira egyidejűleg minimális, csak a munkával kapcsolatosan szükséges adatok, illetve dokumentumok helyezhetők ki. Az eszközök fizikai elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazásával) gondoskodni kell arról, hogy más személyek ne tudjanak betekinteni a rendszerbe, ne férjenek hozzá a rendszerhez.

5.9.11. A vezetők felelőssége

A vezető felelőssége, hogy megkövetelje az alkalmazottól és alvállalkozóktól, hogy a biztonsági intézkedéseket a meghatározott intézeti szabályzatokkal és eljárásokkal összhangban alkalmazzák. A vezetőknek biztosítaniuk kell, hogy az alkalmazottak és beszállítók:

- ismerjék biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférnek, hogy ezzel is a minimálisra csökkentsék a lehetséges biztonsági kockázatokat;
- vegyenek részt biztonsági oktatásokban;
- legyenek ösztönözve, hogy az Intézet biztonsági szabályzatait teljesítsék;
- alkalmazkodjanak a foglalkoztatás feltételeihez, tartsák be az ide vonatkozó biztonsági szabályzatokat, a biztonságot érintő kérdésekben megfelelő, naprakész jártasságuk legyen.

A felhasználói oktatás a biztonsági elképzeléseket is figyelembe vevő képzési terven kell, hogy alapuljon. Az Informatikai Osztályvezetőnek (IOV) — az informatika biztonságpolitikai elveinek, valamint a saját hatáskörben meghatározott képzési elveknek megfelelően— a Jogi és Humán-gazdálkodási Főosztály vezetővel (HSZV), illetve az Információbiztonsági felelőssel (IBF) egyeztetve ki kell dolgoznia a képzési tervet.

5.9.12. Személyi biztonság a jogviszony megszűnésekor, megszüntetésekor vagy kinevezés módosítás esetén (3.1.6.4. [1]; 3.1.6.5. [3]), {14.5}

A jogviszony megszűnése, megszüntetése, illetve a módosítása megközelítőleg azonos biztonsági kategória, mivel mindhárom az éppen használt adatfeldolgozó eszközök és jogosultságok leadásával jár. A felhasználók feladatainak elhatárolása alapvető biztonsági követelmény, éppen ezért a jogosultságok megvonása teljes mértékben indokolt. Az Intézeten belül másik Szervezeti egységhez átirányított alkalmazottat vagy beszállítót ilyen szempontok alapján gyakorlatilag azonosan kell kezelni a kilépő alkalmazottal vagy beszállítóval.

5.9.13. A jogviszony megszűnésének, megszüntetésnek biztonsági kérdései (3.1.6.4. [1]), {14.5}

A jogviszony megszűnése, megszüntetésekor az Intézet szempontjából biztonsági alapkövetelmény, hogy az alkalmazottak és beszállítók szabályozott módon hagyják el az Intézetet. A jogviszony megszüntetésnek folyamatát úgy kell kialakítani, hogy a használatra átadott eszközök visszaadása, és minden hozzáférési jog visszavonása időben befejeződjön.
A jogviszony megszűnése utáni felelősségek közlésének tartalmaznia kell a folyamatos biztonsági követelményeket és jogi felelősségeket, amelyek még vonatkoznak a kilépő alkalmazottra az egészségügyi Intézet jogi osztálya által meghatározott időszakon át a jogviszony megszűnése után is.
A jogviszony megszűnése után még érvényes felelősségek és kötelezettségek szerepeljenek a felhasználó személyi anyagában írásos formában.

5.9.14. Az eszközök visszaadása

Alapvető biztonsági cél, hogy minden jogviszony megszűnése után az átvett vagyontárgyakat a felhasználó szolgáltassa vissza, ide értve különösen a szoftvereket, dokumentumokat, az informatikai eszközöket, beléptető kártyákat, illetve különféle elektronikus és papíralapú adathordozón tárolt információkat.
Azokban az esetekben, amikor a felhasználó engedélyezés után megveszi az adatfeldolgozásra alkalmas eszközét, vagy engedéllyel rendelkező saját informatikai eszközét (BYOD) használta, a kiléptetési folyamat során az eszközről minden intézeti adatot biztonságosan és véglegesen törölni kell. A raktárban valamennyi, újból felhasználásra kerülő eszközt — biztonságos törlés után - alapszoftverekkel újratelepítve kell tárolni. Használatból kivonáskor — szintén biztonságos törlés után - az eszközök gyári beállításait kell visszaállítani, a felhasználó Intézetre utaló információktól, adatoktól meg kell fosztani.
A kilépett felhasználó munkaállomásán munkavégzéssel összefüggésben tárolt dokumentumait a folyamatos munkavégzés érdekében a munkakör átadás-átvétel során az átvevőnek, ennek hiányában a munkáltatói jogkör gyakorlójára számára megfelelően át kell adni.

5.9.15. A hozzáférési jogok visszavonása

Távozók esetén biztonsági alapkövetelmény, hogy minden az informatikai rendszert érintő hozzáférési jog visszavonása legkésőbb az utolsó munkában töltött napon megvonásra kerüljön. Fontos, hogy az informatikai jogosultságokon kívül visszavonásra kerülő vagy átalakítandó hozzáférési jogok közé tartoznak a fizikai vagy logikai hozzáférések, azonosító, beléptető kártyák, előfizetések. Amennyiben a kilépő alkalmazottnak vagy beszállítónak ismert jelszavai vannak aktív fiókokhoz, ezeket le kell adnia az esetleges munkakör módosulás, illetve szolgálati jogviszony megszűnésekor. A kilépő által használt

fiókokat zárolni kell, ettől csak az Informatikai Osztályvezető (IOV) írásbeli engedélyével lehet eltekinteni.

Biztonsági szempontból szükséges, hogy a felelős vezetők informálják a személyi változásokról, és kezdeményezzék a távozók jogosultságainak (pl. belépési engedélyek, távoli hozzáférések) teljes körű visszavonását. Az adatfeldolgozó eszközök hozzáférési jogait minősített esetben akár még a felmentési idő alatt is ajánlatos csökkenteni vagy megszüntetni.

Az ilyen intézkedést csak különféle kockázati tényezők elemzése után lehet meghozni, amelyek a következők:

- ki kezdeményezte a jogviszony megszüntetését és mi a megszűnés oka;
- milyen mértékű az alkalmazott felelőssége;
- mennyi a pillanatnyilag számára hozzáférhető vagyontárgyak értéke.

5.9.16. Az informatikai biztonsági oktatás és képzés (3.1.7.), {3.2}

Valamennyi felhasználót — feladatának és jogkörének figyelembevételével - megfelelő képzésben kell részesíteni az Intézet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába:

- a biztonsági követelményeket;
- a jogi felelősséget;
- az óvintézkedéseket;
- az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát; általános biztonság tudatossági ismereteket.

Az általános képzést azelőtt kell lefolytatni, mielőtt a belépők megkapnák a hozzáférési jogot (jogosultság) az informatikai rendszerekhez, vagy az adatokhoz.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell az Intézetben, különleges biztonsági képzés is szükséges szerepkörök szerint az informatikai biztonsággal foglalkozók számára. A biztonsági képzés mélységének az Intézeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal kiterjedtebb oktatást is biztosítani kell. Informatikai biztonsági képzési programot kell kialakítani az összes biztonsághoz kapcsolódó igény lefedésére. A képzési eljárásrendet rendszeresen felül kell vizsgálni és körülmények, rendszer változásával frissíteni.

A különleges biztonsági képzésre küldendő alkalmazottak kiválasztásakor a következőket kell figyelembe venni:

- az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet játszóalkalmazott, informatikai rendszerek üzemeltetésében kulcsszerepet játszó alkalmazott;
- Intézeti, projekt és rendszerszintű Informatikai Osztályvezető (IOV);
- a biztonság adminisztrációjáért felelős személy, például a hozzáférés ellenőrzés vagy a címtár kezelés területén.

Minden esetben ellenőrizni kell, hogy a tevékenységekhez szükséges-e különleges biztonsági képzés. A lefolytatott képzéseken készült jelenléti íveket és a kapcsolódó tematikát meg kell őrizni.

5.9.17. Belső fenyegetés (3.1.7.4. [4])

A biztonságtudatossági képzés célja, hogy az érintett személyeket készítse fel a belső fenyegetések felismerésére, és tudatosítsa jelentési kötelezettségüket.

5.9.18. A biztonsági képzésre vonatkozó dokumentációk (3.1.7.6. [3]), {3.13}

Az információbiztonsági képzésen történő részvételt igazoló nyilvántartást kell vezetni. Az aláírt dokumentumokat / online képzés naplóit 3 évig meg kell őrizni.

5.9.19. A munkavállalók felelősségre vonása (3.1.6.7. [1]), {14.12}

Azokkal szemben, akik az Intézet informatikai biztonsági szabályait és eljárásait vétkesen megszegték, a munkaviszonyból származó kötelezettség vétkes megszegése esetén alkalmazható eljárást kell kezdeményezni és lefolytatni. A felelősségi, kártérítési eljárást a Polgári Törvénykönyvről szóló 2013. évi V. törvényben, illetve az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény és a Munka Törvénykönyvéről szóló 2012. évi I. törvényben foglaltak alapján, az Intézet Szervezeti és Működési Szabályzatnak megfelelően szükséges lebonyolítani. Amennyiben a dolgozó magatartása szabálysértés vagy bűncselekmény elkövetésének gyanúját veti fel, az Intézet köteles gondoskodni a szükséges eljárások megindításáról. Az eljárás megindítására vonatkozó döntés meghozatalára a Főigazgató (FOIG) jogosult.

5.9.20. Külső szervezetre vonatkozó követelmények (3.1.6.6. [3]), {14.11}

Az Intézet külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy:

- a külső szervezet határozza meg az Intézettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
- a szerződő fél feleljen meg az Intézet által meghatározott személybiztonsági követelményeknek;
- a szerződő fél az egészségügyi intézményt érintő biztonsági auditokban közreműködjön;
- a szerződő fél dokumentálja és tartassa be a személybiztonsági követelményeket, beleértve azt az esetet, amikor a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az Intézet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az Intézetnek.

Az IBF folyamatosan, de legalább 90 naponta ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

6. Fizikai védelmi intézkedések rendje (3.2.1.2 [2]), {12.1}

Az infrastruktúrát és az információt meg kell védeni a jogosulatlan hozzáféréstől, a sérüléstől, valamint az illetéktelen beavatkozástól.
Gondoskodni kell az illetéktelen behatolást, hozzáférést, károkozást és beavatkozást megakadályozó fizikai-mechanikai, elektronikai és személyi védelem szükséges méretű ...együttes — alkalmazásáról.
Az informatikai biztonsági szabályzatban foglaltak az Intézet kapcsolódó szabályzataiban (tűzvédelmi, belépésekre vonatkozó stb.) foglalt előírásokkal együtt értelmezendők.

6.1. Fizikai belépési engedélyek (3.2.1.3. [2]), {12.2}

Az illetéktelen hozzáférés, a károkozás és az intézeti helyiségekbe való behatolás, valamint az adatok jogtalan elérésének megakadályozása érdekében a lehetséges kockázatokat fel kell mérni és ennek megfelelően biztonsági területeket kell kijelölni.

A zónákba való belépési jogosultságokat úgy kell meghatározni, hogy az egyes személyeket az informatikai rendszerben betöltött szerepük alapján kell hozzá rendelni a helyiségekhez vagy helyiség csoportokhoz.
Az informatikai eszközök fizikai védelme érdekében az Intézet helyiségeit alap esetben a következő biztonsági zónákba kell sorolni:

publikus zóna: vendégek (betegek, látogatók) által is szabadon megközelíthető;

- I-es zóna, közösen használt helyiségben lévő informatikai végberendezések (folyosók, tárgyalók);
- II-es zóna, felhasználói irodák, vizsgálók;
- III-as zóna, rendszergazda irodája (fokozott biztonsági zóna);
- IV-es zóna, szerverterem (kiemelt biztonsági zóna).

Az Intézet informatikai helyiségeinek megfelelő kategóriába besorolása az Informatikai Osztályvezető (IOV) feladata. Az Informatikai Osztályvezetőnek (IOV) a besorolás során figyelembe kell vennie az adott helyiségben elhelyezésre kerülő informatikai eszközöket, tárolt adatokat. Ezért az Informatikai Osztályvezető (IOV) az informatikai zónák kialakítása során egyes helyiségek számára a fenti alap besorolásnál magasabb biztonsági fokozatú zónát is meghatározhat.

6.2. A fizikai belépés ellenőrzése (3.2.1.4. [2]), {12.6}

Az egyes biztonsági zónákba való belépést ellenőrizni kell.

- A fokozott vagy a kiemelt biztonsági osztályba sorolt zónák esetén az állandó belépési jogosultsággal rendelkező személyek be- és kilépését is naplózni kell.
- A támogató feladatot ellátó munkatársak hozzáférését korlátozni kell a fokozott vagy kiemelt biztonsági osztályba sorolt zónákon belül. Ha a hozzáférés indokolt és engedélyezett, akkor is figyelemmel kell őket kísérni. A biztonsági területekhez való hozzáférési jogokat — akár a rendszeres jogosultság felülvizsgálat során - rendszeresen át kell vizsgálni, frissíteni, illetve, ha már nem szükséges, akkor vissza kell vonni.
- Az Információbiztonsági Felelős az éves ellenőrzési tervének keretein belül szúrópróbaszerűen jogosult a belépési naplókat, az eseménynaplókat ellenőrizni, valamint a kiosztott kártyák és az elektronikus információs rendszerben engedélyezett belépések egyezőségét vizsgálni.

6.3. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz (3.2.1.5. [4])

Az Intézet az általa meghatározott biztonsági védelemmel [beléptetőrendszer, kamerarendszer, élőerős védelem stb.] ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

6.4. A kimeneti eszközök hozzáférés ellenőrzése (3.2.1.6. [4])

Az Intézet ellenőrzi az elektronikus információs rendszer kimeneti eszközeihez való fizikai hozzáférést annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá.

6.5. A fizikai hozzáférések felügyelete (3.2.1.7 [3]), {12.17}

A IV-es zónába a belépési engedéllyel rendelkezők listáját az Informatikai Osztályvezető (IOV) állítja össze és vezeti.
Az Informatikai Osztályvezető (IOV) visszavonja a belépési jogosultságot, ha:

- a munkatársnak megszűnik a jogviszonya;
- a belépési kérelmen megjelölt határozott idő lejártát követően.

Az Informatikai Osztályvezető (IOV) azonnal intézkedik a belépési jogosultság megszüntetéséről, hogy ha:

- a belépési kártya elveszett;
- felmerült a gyanú, hogy a belépési kártya idegen kézbe került;
- ha a belépést szabályozó más eszköz, információ kompromittálódott, vagy ennek gyanúja merült fel.

6.6. Behatolás riasztás, felügyeleti berendezések (3.2.1.7.2. [4])

Az Intézet felügyeli az informatikai biztonsággal összefüggő fizikai behatolás riasztásokat és a felügyeleti berendezéseket. A felügyeletet az Informatikai Osztályvezető (IOV) gyakorolja.

6.7. A látogatók ellenőrzése (3.2.1.8 [3]), {12.22}

Külső személyek csak kísérettel tartózkodhatnak az Intézet kritikus (fokozott és kiemelt) biztonsági osztályba sorolt zónáján belül.

6.8. Áramellátó berendezések és kábelezés (3.2.1.9. [4])

Az Intézet védi az elektronikus információs rendszert árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben, külön szabályzat szerint.

6.9. Tartalék áramellátás (3.2.1.9.1. [4])

Az Intézet az elsődleges áramforrás kiesése esetére, a tevékenységhez és kockázati szinthez mérten, rövid ideig működőképes szünetmentes áramellátást biztosít az elektronikus információs rendszer szabályos leállításához vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

6.10. Vészkikapcsolás (3.2.1.10 [4])

Biztosítani kell az elektronikus információs rendszer vagy egyedi rendszerelemek áramellátásának kikapcsolását vészhelyzetben. A vészkikapcsoló berendezésnek könnyen és biztonságosan megközelíthetőnek kell lennie. Meg kell akadályozni, hogy a vészkikapcsolást jogosulatlanul is végre lehessen hajtani.

6.11. Vészvilágítás (3.2.1.11. [3]), {12.31}

Áramszünet esetén automatikus vészvilágítás kell, hogy aktiválódjon, amely biztosítja a vészkijáratokat és menekülési útvonalakat.

6.12. Tűzvédelem (3.2.1.12. [3]), {12.33}

Az Intézet az elektronikus információs rendszerek számára független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket alkalmaz, és tart karban.
A helyiségek tűzvédelmét teljes körű tűzriasztó rendszerrel, valamint az adott helyiség kialakítási módjának megfelelő, automatikus tűzoltó rendszerrel és a helyiség tűzvédelmi besorolásának megfelelő kézi tűzoltó eszközökkel kell biztosítani. A helyiségeket tűzzáró ajtóval kell elválasztani az épület többi részétől.

6.13. Automatikus tűzelfojtás (3.2.1.12.2. [4])

Az Intézet a személyzet által folyamatosan nem felügyelt elektronikus információs rendszerek számára automatikus tűzelfojtási képességet biztosít, amennyiben ennek feltételei rendelkezésre állnak.

6.14. Hőmérséklet és páratartalom ellenőrzés (3.1.2.13. [3]), {12.37}

Az Intézet az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. adatközpont, szerver szoba, központi gépterem) az erőforrások biztonságos működéséhez szükséges szinten tartja a hőmérsékletet és páratartalmat. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben figyeli a hőmérséklet és páratartalom szintjét.

6.15. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem (3.1.2.14. [3]), {12.40}

Az Intézet védi az elektronikus információs rendszert a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró-szelepek hozzáférhetők, és megfelelően működnek, valamint a kulcsszemélyek számára ezek kezelése ismertek. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése során biztosítja, hogy az a víz-, és más hasonló kártól védett legyen, akár csővezetékek kiváltásával, áthelyezésével is.

6.16. Be- és kiszállítás (3.2.1.15 [3]), {12.42}

Az Intézet területére behozhatók, illetve kivihetők információs rendszerelemek. A kritikus biztonsági zónákban (szerverszoba), állandó belépésre nem jogosult személy csakis az Informatikai Osztályvezető (IOV) engedélyével és felügyeletével szállíthat ki-, illetve be információs rendszerelemeket. A kritikus biztonsági zónákba történő be-, illetve kiszállítás alkalmával a szállított rendszerelemről nyilvántartást kell vezetni.

6.17. Az elektronikus információs rendszer elemeinek elhelyezése (3.2.1.16. [4])

Az Intézet úgy helyezi el az elektronikus információs rendszer elemeit, hogy a legkisebb mértékre csökkentse fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.
Az informatikai eszközöket fizikailag is védeni kell a lehetséges veszélyektől és káros környezeti hatásoktól.
Az informatikai eszközök elhelyezése és védelme terén az idő előtti elhasználódásból, meghibásodásból, megrongálódásból eredő kockázatok csökkentésére a rendszergazdának, az egyéb üzemeltető személyzetnek és a felhasználóknak a következő intézkedéseket kell foganatosítani:

- Meg kell oldani az informatikai eszközök biztonsági besorolásuknak megfelelő fizikai hozzáférés védelmét.
- Meg kell teremteni az informatikai eszközök — a gyári specifikációban leírt — megfelelő működési környezetét.
- Óvni kell az informatikai eszközöket a gyári specifikációban leírt környezeti ártalmaktól.
- Az informatikai eszközöket úgy kell elhelyezni, hogy azok ne legyenek kitéve az illetéktelen hozzáférésnek és lehetőleg minimális szinten legyenek kitéve a lehetséges környezeti hatások által előidézett veszélyforrásoknak.
- Különös védelmet igénylő eszközöket elkülönítve kell elhelyezni és tárolni.
- Segédberendezések és eszközök a biztonsági körleteken belül legyenek elhelyezve.

- Az egyes eszközöket csak munkavégzés céljából, szakszerűen azok rendeltetésének megfelelően szabad használni.
- Az Intézet által kezelt adatfeldolgozó eszközöket fizikailag is el kell választani azoktól, amelyekhez harmadik fél hozzáférhet.
- A névtárakat és a belső telefonkönyveket, címjegyzékeket, amelyek érzékeny adatfeldolgozó eszközök helyét azonosítják, nem szabad a nyilvánosság számára elérhetővé tenni.
- Az egyes eszközöket ki kell kapcsolni, ha azokat hosszabb ideig nem használják vagy a munka végeztével. Kivéve akkor, ha ezzel ellentétes állandó vagy eseti írásbeli utasítás nem kerül kiadásra.
- Tilos az egyes eszközök közelében folyadékot, éghető anyagot, illetve az eszköz felett, alatt vagy rajta az eszköz rendeltetésétől eltérő jellegű anyagot, tárgyat elhelyezni és tárolni.
- Tilos az eszközt a telepítési helyéről az Intézet informatikusainak engedélye nélkül elmozdítani. Kivételt képeznek a mobil eszközök.
- Az informatikai eszközökhöz bármilyen más eszközt kizárólag az informatikus engedélyével és közreműködésével szabad csatlakoztatni.

6.18. Karbantartók (3.2.1.19 [3]), {10.18}

Az Intézet az alábbi kialakított folyamat mentén kezeli a karbantartók munkavégzési engedélyeit:

- nyilvántartást vezet a karbantartó szervezetekről vagy személyekről;
- megköveteli a hozzáférési jogosultság igazolását az elektronikus információs rendszeren karbantartást végzőktől;
- Az Intézet ellenőrzi a karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében.
- Felhatalmazást ad az Intézethez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személyeknek arra, hogy felügyeljék a kívánt jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

6.19. Időben történő javítás (3.2.1.19.3 [4])

Az Intézet karbantartási támogatási szerződést köt az elektronikus információs rendszerelemeihez, a szerződéseket nyilvántartja.

7. Logikai védelmi intézkedések

7.1. Általános védelmi intézkedések (3.3.1.1. [2])

Az Intézet megfogalmazza, és az Intézetre érvényes követelmények szerint dokumentálja, valamint az Intézeten belül kihirdeti:

- az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési eljárási folyamatokat;
- felügyeli az elektronikus információs rendszer és környezet biztonsági állapotát;
- meghatározza az információbiztonsággal összefüggő szerepköröket és felelősségi köröket;
- kijelöli az ezeket betöltő személyeket;
- integrálja az elektronikus információbiztonsági engedélyezési folyamatokat az Intézeti szintű kockázatkezelési eljárásba, összhangban az Informatikai Biztonsági Szabályzattal.

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az Intézet hatókörébe tartozó:

- emberi, fizikai és logikai erőforrásra;
- eljárási és védelmi szintre és folyamatra.

7.1.1. Az elektronikus információs rendszer kapcsolódásai (3.3.1.3. [3])

Az Intézet a kapcsolódást szabályozó dokumentumokban szabályozza, és az IBF engedélyéhez kötheti az elektronikus információs rendszerének kapcsolódását más elektronikus információs rendszerekhez. A kapcsolódási formáknak rendszerenként dokumentáltan kell megtörténnie. Dokumentálja az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

7.1.1.1. Belső rendszerkapcsolatok (3.3.1.3.2. [3])

Az Intézet az Informatikai Osztályvezető (IOV) és a IBF írásos engedélyéhez köti az elektronikus információs rendszereinek összekapcsolását.

7.1.1.2. Külső kapcsolódásokra vonatkozó korlátozások (3.3.1.3.3. [3])

Az Intézet a külső elektronikus információs rendszerekhez való kapcsolódásokhoz során a „minden tiltása, kivételek engedélyezése" elvet követi, amely mindennemű kapcsolat tiltásával kezdve az Informatikai Osztályvezető (IOV) és az IBF általírásban jóváhagyott bejövő forgalom kivétel alapú engedélyezését jelenti.

7.2. Tervezés (3.3.2.)

Biztonságtervezést kell végezni mindegyik olyan rendszerfejlesztés, továbbfejlesztés alkalmával, amely hatással lehet az Intézet információbiztonságára nézve. A biztonságtervezéssel kapcsolatos feladatokat az egyes rendszerek teljes életciklusa során el kell látni.
A biztonságtervezési eljárás egyes fázisai a következők:

felmérés;

- az elvárt biztonsági osztály meghatározása;
- követelményrendszer kidolgozása;
- rendszerbiztonsági terv készítése;
- rendszerbiztonsági terv ellenőrzése.

7.2.1. Felmérés

A felmérés során meg kell határozni, hogy a rendszer milyen fizikai, személyi és szoftver környezetben fog üzemelni. Fel kell mérni és rögzíteni kell:

- a rendszer hatókörét, alapfeladatait, biztosítandó szolgáltatásait;
- a rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
- a rendszerben kezelendő adatok érzékenységét (megjelölve azokat az adatköröket, amelyek esetében a rendszer osztályba sorolásánál magasabb szintű védelemre van szükség.);
- a rendszerrel kapcsolatos kockázatokat, fenyegetéseket és gyenge pontokat.

7.2.2. Az elvárt biztonsági osztály meghatározása

A felmérésben rögzített információkra alapozva meg kell határozni a rendszer elvárt biztonsági osztályát.

7.2.3. Követelményrendszer kidolgozása

Ki kell dolgozni a rendszerrel kapcsolatos információbiztonsági követelmények rendszerét. Ennek során a helyzetfelmérésre alapozva meg kell határozni a rendszer fejlesztői/üzemeltetői számára a fizikai, logikai és adminisztratív védelmi követelményeket.

7.2.4. Biztonságtervezési szabályzat (3.3.2.1. [4])

Az IBSZ-ben elfogadott IT biztonsági követelmények alapján az Informatikai Osztályvezető (IOV) elrendelheti a fejlesztésre kerülő rendszerekre vonatkozó részletszabályok kidolgozását egy általános hatályú szabályzatban („Biztonságtervezési Szabályzat"), és/vagy a fejlesztésekhez külön dokumentumban.

7.2.5. Rendszerbiztonsági terv készítése (3.3.2.2. [2]), {13.2}

A rendszertervezés során Rendszerbiztonsági Tervet kell készíteni, amelynek összhangban kell állnia az Intézet által alkalmazott architektúrával. A Rendszerbiztonsági Tervet az egyes rendszerek vonatkozásában a 41/2015. (VII. 15.) BM rendelet 3. sz. melléklete szerinti szerkezetben kell elkészíteni. A kidolgozásáért felelős személyeket az Informatikai Osztályvezető (IOV) jelöli ki.

7.2.6. A rendszerbiztonsági terv audit

Az elkészült rendszerbiztonsági tervet auditálni kell. Ennek során meg kell vizsgálni, hogy az elkészült rendszerbiztonsági terv:

- mennyiben teljesíti a rendszerrel szemben megfogalmazott információbiztonsági követelményeket;
- mennyiben felel meg a költséghatékony védelem elveinek;
- a bevezetése mennyiben felel meg a hatékony rendszerbevezetés elveinek.

Abban az esetben, ha az audit során hiányosságok kerülnek megállapításra, a rendszerbiztonsági tervet javíttatni kell a terv készítőjével. A rendszer éles üzemét csakis elfogadott rendszerbiztonsági terv megléte esetén lehet megkezdeni.

7.2.7. A rendszerbiztonsági terv megismertetése

Az elkészült rendszerbiztonsági tervet, illetve azok változását megismerhetik az arra feljogosított személyek. A rendszerbiztonsági tervet megismerheti a(z):

- a főigazgató (FOIG);
- a Főigazgatói Hivatal vezetője;
- Informatikai Osztályvezető (IOV);
- Információbiztonsági felelős (IBF);
- a főigazgató által erre feljogosított személyek.

7.2.8. A rendszerbiztonsági terv felülvizsgálata

7.2.8.1. Időszaki felülvizsgálat

A rendszerek rendszerbiztonsági tervét legalább 2 évenként felül kell vizsgálni és szükség esetén módosítani kell. A vizsgálat alapja:

- a rendszerbiztonsági terv megvalósulásával kapcsolatos ellenőrzések eredménye;
- az időközben felmerülő, a biztonságtervezéssel és rendszerbiztonsági tervvel összefüggő események.

7.2.8.2. Rendkívüli felülvizsgálat

A rendszerbiztonsági tervet az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell súlyos, a rendszerrel összefüggő incidens bekövetkezése esetén vagy annak környezetébe az információbiztonságra releváns hatással bíró változás esetén.

7.2.8.3. A rendszerbiztonsági terv frissítése

A rendszerbiztonsági tervet automatikusan frissíteni kell minden a tervben rögzített információ változása, illetve új, a rendszerrel összefüggő új információ megismerése esetén.

7.2.8.4. Belső egyeztetések

A rendszer rendszerbiztonsági tervének kidolgozását, illetve elfogadását az illetékes munkatársakkal egyeztetve kell végrehajtani. Az egyeztetések jegyzőkönyveit a rendszer átadási dokumentációjának részeként, annak megőrzési helyén legalább 5 évig meg kell őrizni.

7.2.9. A biztonságtervezés auditja (3.3.2.1. [4])

A biztonságtervezés eljárást auditálni kell, és az ellenőrzés eredményét az Intézet Főigazgatójával (FOIG) meg kell ismertetni.

7.2.10. Cselekvési terv (3.3.2.3. [2])

7.2.10.1. Cselekvési terv készítése

Abban az esetben, ha egy adott elektronikus információs rendszerre vonatkozó biztonsági osztálynak való megfelelés vizsgálatánál hiányosság kerül megállapításra, az IBF-nek cselekvési tervet kell készíteni a hiányosságok kiküszöbölésére. A cselekvési tervben dokumentálni kell a megállapított hiányosságok javítására, valamint a rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésre irányuló tervezett tevékenységeket, valamint az egyes tevékenységek felelőseit és határidőit.

7.2.10.2. Cselekvési terv frissítése

A cselekvési terv végrehajtását 2 évente felül kell vizsgálni és a vizsgálat eredményeképpen az adott helyzetnek megfelelően frissíteni kell.

7.2.11. Személyi biztonság (3.3.2.4. [2]), {14.1}

7.2.11.1. A felhasználókkal szemben támasztott elvárások megfogalmazása

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket a felhasználó

munkaköri leírásának, egyéb számára kiadott utasításnak, valamint az adott rendszer felhasználói dokumentációjának kell tartalmaznia.

7.2.11.2. A rendszer használattal kapcsolatos információk biztosítása

A hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek (belső munkatárs vagy külsős vállalkozó) írásbeli nyilatkozatott kell tennie arról, hogy az érintett rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

7.2.11.3. A felhasználókkal szemben támasztott elvárások felülvizsgálata

Két évente felül kell vizsgálni a rendszerek használatával kapcsolatban a felhasználókkal szemben támasztott elvárásokat. A felülvizsgálatot a rendszergazdáknak kell elvégezniük. Abban az esetben, ha a rendszeres felülvizsgálat során vagy azon kívül megállapítást nyer, hogy a rendszer szolgáltatásai, funkcionalitása, hatóköre megváltozott vagy más okból következően az elvárásokban változás állt be, az illetékes rendszergazdának haladéktalanul jelentenie kell ezt az IBF-nek és tájékoztatnia kell a rendszer felhasználóit.
A tájékoztatás történhet e-mail-ben, vagy nagyobb változás esetén erre a célra megszervezett oktatáson. E-mail tájékoztatás esetén az egyes felhasználóknak igazolható módon vissza kell jelezniük, hogy a tájékoztatást megértették és a jövőben annak alapján járnak el.

7.2.12. Információbiztonsági architektúra leírás (3.3.2.5. [4])

Az Intézet a felhasznált rendszerkomponensek vonatkozó dokumentációja és a tervezett vagy kialakított biztonsági architektúra alapján elkészíti és az elektronikus információs rendszer változásai mellett folyamatosan karbantartja az elektronikus információs rendszer információbiztonsági architektúra leírását, amely:

- összegzi az elektronikus információs rendszer bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló filozófiát, követelményeket és megközelítést;
- megfogalmazza, hogy az információbiztonsági architektúra miként illeszkedik az Intézet általános architektúrájába, és hogyan támogatja azt;
- leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

7.3. Rendszer és szolgáltatás beszerzés (3.3.3. [2])

7.3.1. A rendszer fejlesztési életciklusa (3.3.3.2. [2]), {16.3}

Az Intézet az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikai biztonsági helyzetüket.
A fejlesztési életciklus során információbiztonsági szerepkörök és felelősségek a következő táblázat alapján tekinthetők át:

Feladat	Felelős	Konzulens(ek)	Tájékoztatandó(k)
Követelmény meghatározás	IBF	Főigazgatói Hivatal vezető, IOV, IÜFSZ, IBM	FOIG
Fejlesztés vagy beszerzés	FOIG, IBF	Főigazgatói Hivatal vezető, IOV	IBM
Megvalósítás vagy értékelés	IBF	Főigazgatói Hivatal vezető, IOV, IBM	FOIG
Üzemeltetés és fenntartás	IÜFSZ	Főigazgatói Hivatal vezető, IOV, IBF	
Kivonás (archiválás, megsemmisítés)	IBF, IÜFSZ	Főigazgatói Hivatal vezető, IOV	IBM

7. táblázat - Fejlesztési életciklus során információbiztonsági szerepkörök

7.3.2. Funkciók, portok, protokollok, szolgáltatások (3.3.3.3. [3])

Az Intézet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat, ezt figyelembe véve az Informatikai Osztályvezető (IOV) dönt arról, hogy az adott rendszer integrálható-e.

7.3.3. Fejlesztői követelmények (3.3.3.4. [4], 3.3.3.5. [4])

Az Intézet megköveteli az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

- vezesse végig a változtatásokat az elektronikus információs rendszer, rendszerelem vagy rendszer szolgáltatás tervezése, fejlesztése, megvalósítása, üzemeltetése során;
- dokumentálja, kezelje, és ellenőrizze a változtatásokat, biztosítsa ezek sértetlenségét;
- csak a jóváhagyott változtatásokat hajtsa végre az elektronikus információs rendszeren, rendszerelemen vagy rendszerszolgáltatáson;
- dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;
- kövesse nyomon az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit az Intézet által meghatározott személyeknek;
- készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat;
- hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, vagy regressziós tesztelést, és ezt értékelje ki az Intézet által meghatározott lefedettség és mélység mellett;
- dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit;
- javítsa ki a biztonsági tesztelés és értékelés során feltárt hiányosságokat.

7.4. Biztonsági elemzés (3.3.4.)

Az IBF-nek éves rendszerességgel értékelni kell az Intézet elektronikus információs rendszereinek és azok működési környezeteinek védelmi intézkedéseit az Intézet biztonsági szintjének megfelelő adminisztratív, fizikai és logikai védelmi intézkedések viszonylatában.
Elemezni kell, hogy az adott Szervezeti egység információbiztonsági védelmi intézkedései megfelelően hatékonyak-e és nincs-e szükség azok rövid, közép, esetleg hosszabb távon történő továbbfejlesztésére.
Az értékelés eredményét táblázatba kell foglalni, amelynek egyes oszlopai a következő információkat tartalmazza:

- védelmi intézkedés típusa;
- védelmi intézkedés;
- védelmi intézkedés megfelelősége*;
- javasolt intézkedés rövidtávon;
- javasolt intézkedés középtávon;
- javasolt intézkedés hosszútávon.

*Védelmi intézkedések megfelelősége:

Az elemzés tárgyát képező információbiztonsági intézkedés vagy eljárás megfelelő, változtatás nem szükséges.
Az elemzés tárgyát képező információbiztonsági intézkedés vagy eljárás tartalmaz hibát vagy hiányosságokat, ezek azonban nem kritikusak.
Az elemzés tárgyát képező információbiztonsági intézkedés vagy eljárás kritikus hibát vagy hiányosságot tartalmaz.
A biztonsági helyzet értékelésébe lehetőség szerint külső munkatársat vagy vállalkozást kell bevonni, akinek rendelkezésre áll a jogszabály szerinti képzettség, illetve szakmai gyakorlat.

7.4.1. Biztonsági teljesítmény mérése (3.3.4.4. [3], 3.3.5.2 [3])

Az IBF-nek rendszeres időközönként, évente mérni kell az Intézet biztonsági teljesítményét. A biztonsági teljesítmény mérésére a következő mutatókat kell használni:

- tárgyidőszakban előfordult 1-5 kategóriájú incidensek darabszáma az Intézet egészére (kategóriánként);
- tárgyidőszakban előfordult 1-5 kategóriájú incidensek darabszáma szervezeti egységenként (kategóriánként);
- az előfordult incidensek kategóriáinak összege;
- az előző incidensek kategóriáinak összegének változása az előző időszakhoz képest %-ban kifejezve.
- a független biztonsági auditok során megállapított érték (ha történt),
- az IBF által kidolgozott KPI sablon rendszeres kitöltésével.

7.4.1.1. Biztonsági teljesítmény értékelés (3.3.4.2. [3]), {5.2}

A biztonsági teljesítmény mérőszámainak aktuális értékei alapján:

- meg kell állapítani az Intézet biztonsági teljesítményének tendenciáit;
- azt, hogy a mutatók mennyiben felelnek meg az előzőleg megfogalmazott elvárásoknak;

- az elvárásoknak való esetleges meg nem felelés esetén azok fő okait.

A megállapításokat dokumentált formában az IBF készíti el rendszeresen, de legalább évente. Az elkészült jelentéseket az a Főigazgatói Hivatal vezetőjének egyidejű tájékoztatásával az Informatikai Osztályvezetőnek (IOV) adja át.

7.4.1.2. Speciális értékelés (3.3.4.3. [4])

Az Intézet a védelmi intézkedések értékelése keretében bejelentés mellett, vagy bejelentés nélküli sérülékenység-vizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az Intézet által meghatározott egyéb biztonsági értékeléseket végez vagy végeztet.

7.5. Tesztelés, képzés és felügyelet (3.3.5.)

Mindegyik fejlesztendő alkalmazás esetében meg kell határozni a következőket:

- a tesztelés folyamata;
- a tesztelés szintjei;
- a használt tesztelési típusok;
- a használt tesz tervezési technikák.

7.5.1. Tesztelési, képzési és felügyeleti eljárások (3.3.5.1.1. [3])

7.5.1.1. Teszttervezés

A teszt tervezés folyamat meghatározásának ki kell terjednie a tesztelési terv és a tesztelési dokumentáció meghatározására.
A tesztelési tervben meg kell határozni:

- a tesztelési célokat, tesztelési környezet és az adott alkalmazás teszteléséhez kapcsolódó általános elképzeléseket, a tesztelendő funkciókat;
- az erőforrásokat, szerepköröket, időbeni tervet;
- az egyes tesztelési fázisok hosszát és a fázisból történő kilépés feltételeit;
- a tesztelés sikerességének mérését.

7.5.1.2. Teszt analízis és Design

Az analízis és design fázisban ki kell dolgozni a teszteseteket, amelynek ki kell terjednie az adott teszteset:

- céljára;
- kiindulási környezetének leírására;
- elvégzendő teszt lépéseire;
- teszt adataira;
- elvárt kimeneteleire;
- sikerességi kritériumaira.

7.5.1.3. Végrehajtás

A teszt végrehajtása során naplózni kell a kimeneteket, amelyben rögzíteni kell:

- a tesztkörnyezet komponenseinek verzióját;
- az elvégzett teszt eredményét;

- a felmerült incidenseket;
- a tesztelés időpontját;
- a tesztelést végző munkatárs nevét.

7.5.1.4. Értékelés, beszámolás, kilépés

A teszt értékelése során:

- el kell készíteni a teszt beszámolókat;
- ki kell elemezni a teszt beszámolókat;
- döntést kell hozni a tesztelés folytatásról/abbahagyásáról/felfüggesztéséről.

7.5.2. A tesztelés típusai

A tesztelésnek a következő típusai lehetnek:
Fejlesztői teszt: A fejlesztői tesztelést a fejlesztőknek kell végezniük vagy nem felhasználó kollégáknak. Célja az alapvető működési hibák felderítése.

- Modulteszt: Moduláris rendszer tesztelése során ellenőrizni kell, hogy a modul működése és interfészei a specifikációban meghatározottak szerint valósultak meg.
- Rendszer teszt: Ennek során ellenőrizni kell, hogy a rendszer működése a specifikációban meghatározottak szerint valósul meg és a program hibátlanul működik a specifikációban meghatározott szoftver és hardver környezetben.
- Integrációs teszt: Ennek során ellenőrizni kell, hogy a több rendszer által megvalósított feldolgozás során a különböző rendszerek egymással való együttműködése a specifikációban meghatározottak szerint valósul meg.
- Elfogadási teszt: A megrendelő által ellenőrizni kell, hogy a rendszer a véglegeshez hasonló környezetben a követelmények alapján működik-e. A tesztet a teljes rendszeren minden függőséggel együtt - kell végrehajtani.
- Biztonsági teszt: Biztonsági tesztelésre van szükség, ha a rendszer szenzitív adatokat kezel. Ezen tesztelés során meg kell bizonyosodni arról, hogy a rendszer megfelel-e az elvárt biztonsági követelményeknek.
- Go-live teszt: Egy próbaélesítés, amely során a korábbi rendszerek továbbra is üzemelnek annak érdekében, hogy az élesítéskor keletkező problémák ne befolyásolják a normál üzem működését.
- Teljesítmény teszt: A rendszer teljesítményének (válaszidő, számítási kapacitás...) tesztelése jelentős számú felhasználó vagy automatikus tesztrendszer segítségével.
- A fejlesztési tesztelések tervezése során törekedni kell a legalább háromrétegű (DEV, TEST, PROD) környezet kialakítására és a környezetek közötti szabályozott kibocsátásokra.

7.5.3. Tesztelés kategóriák

- Funkcionális: A rendszer funkciók vizsgálata.
- Nem funkcionális: A teljesítmény, használhatóság, stressz tűrés megvizsgálása.
- Regressziós: Annak megvizsgálása, hogy adott javítás során nem romlanak el más funkciók.

7.5.4. Teszttervezési technikák

- Tesztelő tapasztalata alapján történik.

- Specifikáció alapján történik: Nem ismert a rendszer forráskód architektúrája, tesztelés alapja kizárólag a specifikáció.
- Struktúra alapján történik: Ismert a forráskód architektúra és ez vezérli a tesztelést.
- Hiba alapján történik: A feltárt hiba ad alapot a tesztelés megvalósításához.
- Valószínűség alapján történik: A tesztelés megvalósítása véletlenszerű kiválasztáson alapul.

7.5.5. Sérülékenység teszt (3.3.5.3. [3]), {15.9}

Az Intézet az elektronikus információs rendszerei és alkalmazásai tekintetében sérülékenység tesztet végez, ha azt az elektronikus információs rendszerfejlesztési, üzemeltetési és használati körülményei lehetővé teszik:

- legalább évente, vagy véletlenszerűen, valamint olyan esetben, amikor új lehetséges sérülékenység merül fel az elektronikus információs rendszerrel vagy alkalmazásaival kapcsolatban, megismétli a sérülékenység tesztet;
- a sérülékenység tesztet sérülékenység vizsgálati eszközök és technikák alkalmazásával vagy külső Intézet bevonásával azon elektronikus információs rendszerek tekintetében végzi el, amelyek az Intézet felügyelete, irányítása alatt állnak;
- olyan sérülékenységi teszteszközt kell alkalmazni, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.
- Az elektronikus információs rendszer különleges jogosultsághoz kötött - úgynevezett privilegizált hozzáférést biztosít az Intézet által kijelölt rendszerelemekhez a sérülékenység teszt végrehajtásához.

Az elvégzett teszt eredménye alapján:

- kimutatást készít a feltárt hibákról, valamint a nem megfelelő konfigurációs beállításokról;
- felméri a sérülékenység lehetséges hatásait;
- elemzi a sérülékenység teszt eredményét;
- megosztja a sérülékenység teszt eredményét az Informatikai Osztályvezetővel (IOV), aki dönt a további érintettekről;
- az Intézet az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizálja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal;
- az Intézet meghatározza, hogy egy támadó milyen információkat képes elérni az elektronikus információs rendszerben, és ennek elhárítására javításokat hajt végre.
- A javításokat követően az Intézet sérülékenység teszt megismétlésével visszaellenőrzést végez. A visszaellenőrzés eredményét jelentés formájában elérhetővé teszi a felettese részére.

7.6. Konfigurációkezelés (3.3.6.)

7.6.1. Konfigurációs eljárásrend és nyilvántartások (3.3.6.1. [2]), {6.1}

Az Intézet birtokában lévő informatikai konfigurációs elemek teljes köréről naprakész nyilvántartást kell vezetni, amiért az Informatikai Osztályvezető (IOV) felel. A nyilvántartás és visszakereshetőség biztosítása céljából konfigurációs adatbázist kell létrehozni. A nyilvántartásban kötelezően kell szerepeltetni a következő konfigurációs elemeket:

- hardver elemek;
- szoftver elemek.

A nyilvántartásnak minden eszközre az alábbi adatokat kell tartalmaznia:

- Az eszköz logikailag milyen csoportba tartozik, illetve hol található.
- Az eszköz megnevezése, meghatározása.
- Azonosító, amennyiben az eszköz egyértelmű azonosításához arra szükség van, egyértelmű azonosítót kell hozzárendelni (a mező kitöltése tehát nem minden esetben kötelező).

A konfigurációs nyilvántartás mellett az Intézet gondoskodik hatályos konfigurációkezelési eljárásrend kidolgozásáról.

A nyilvántartás naprakészségéért, a konfigurációs eljárásrendért, a konfigurációk tárolásáért az Informatikai Osztályvezető (IOV) felel.

7.6.2. Alkalmazási rendszerek konfigurációinak nyilvántartása

Az Intézet által használt alkalmazási rendszerek konfigurációinak teljes köréről nyilvántartást kell vezetni. A nyilvántartásban kötelezően kell szerepeltetni a következő elemeket:

- az alkalmazási rendszer megnevezése;
- az alkalmazási rendszer konfigurációs elemei.

7.6.3. Alapkonfiguráció (3.3.6.2. [2]), {6.2}

Az Intézet rendszerenként rögzített alapkonfigurációi kiindulási alapként szolgálhatnak a tovább fejlesztéseknél, illetve sikertelen változtatásoknál visszatérési pontként szolgálhatnak.

7.6.4. Áttekintések és frissítések (3.3.6.2.2. [4])

Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni.

7.6.5. Korábbi konfigurációk megőrzése (3.3.6.2.3. [4])

Változatlan állapotban meg kell őrizni az elektronikus információs rendszer alapkonfigurációját, és annak további verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés.

7.6.6. Magas kockázatú területek konfigurálása (3.3.6.2.4. [4])

Biztonsági szempontokból a Főigazgatói Hivatal vezető és az Informatikai Osztályvezető (IOV) által jóváhagyott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják.

A Főigazgatói Hivatal vezető és az Informatikai Osztályvezető (IOV) által jóváhagyott biztonsági eljárásokat kell alkalmazni, ha a külső helyszíneken használt eszközöket belső használatba vonják.

7.6.7. A konfigurációváltozások felügyelete (változáskezelés) (3.3.6.3. [3]), {6.7}

Az Intézet:

- meghatározza a változáskezelési felügyelet alá eső változástípusokat;
- meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit;
- megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat;

- dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket;
- megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben;
- visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását;
- felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket.

Az Intézetnél a következő tevékenységek tartoznak a változáskezelés hatálya alá:

- fejlesztések, verzióváltások;
- a rendszerelemek cseréje;
- a rendszerműködés módosításai.

7.6.7.1. Előzetes tesztelés és megerősítés (3.3.6.3.2. [4])

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.

7.6.7.2. Változáskezelés alapvető szabályai

A változáskezelést külön rendszer beavatkozási eljárásrendként kell az Informatikai Osztályvezető (IOV) részéről kiadni, melynek meg kell felelnie az alábbiakban felsorolt előírásoknak.
A rendszerkonfiguráció változásokat az alábbiak figyelembevételével lehet elvégezni:

- Új konfiguráció implementálását engedélyeztetni kell. Az implementációt kizárólag a szükséges engedély birtokában lehet megkezdeni. A változás megkezdése előtt az Informatikai Osztályvezető (IOV) engedélyezi a megvalósítandó hardver és szoftver konfigurációt. Az engedélyezett változtatásokat a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján végrehajtja, sikeres végrehajtás esetén a rendszerleírásban dokumentálja.
  - Minden változtatással kapcsolatos bejelentést, véleményezést, döntést és kivitelezést dokumentálni kell.
- Bármely, az egyes konfigurációkat megváltoztató művelethez az Informatikai Osztályvezető (IOV) engedélye szükséges.
- Új konfigurációra történő áttérést kizárólag úgy lehet elvégezni, hogy vissza lehessen állni a megelőző konfigurációra.
- A fejlesztési, tesztelési és üzemeltetési környezeteket logikailag egymástól külön kell választani.
- A változáskezelési előírások betartását és a változáskezelési folyamatot az Informatikai Osztályvezető (IOV) az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

7.6.8. Biztonsági hatásvizsgálat (3.3.6.4. [3]), {6.15}

Az egyes konfigurációkezeléssel kapcsolatos változtatási igényeket, javaslatokat megvalósítás előtt meg kell küldeni az IBF-nek. Az IBF-nek elemeznie kell a konfigurációkezelés végrehajtásával együtt járó kockázatokat és javaslatot kell tennie a kockázatok minimalizálásának módjára.

7.6.9. A változtatásokra vonatkozó hozzáférés korlátozások (3.3.6.5. [4])

Az Intézet belső szabályozásában meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

7.6.10. Új konfiguráció éles üzembeállása

Új konfiguráció éles üzembeállása során a következőket kell betartani:

- Csak adminisztrátori jogosultsággal lehet elvégezni a változtatásokat.
- Ellenőrizni kell, hogy mindegyik konfigurációs lépés megtörtént-e.
- Ellenőrizni kell, hogy jogosulatlan elemek nem kerülnek-e telepítésre. A jogosulatlan elemek észlelése esetén le kell tiltani és törölni azokat.

7.6.11. A működő rendszer konfiguráció figyelése

Az Intézet megbízott munkatársának legalább havonta ellenőriznie kell, hogy a jogosulatlan hardver-, szoftver elemek nem kerültek-e telepítésre. Minősített adatok kezelését végző rendszerek esetében az ellenőrzést legalább hetente el kell végezni.
A jogosulatlan elemek észlelése esetén le kell tiltani, majd törölni azokat, valamint értesíteni az Informatikai Osztályvezetőt (IOV).
Folyamatosan figyelnie kell, hogy illetéktelen behatolás következményeképpen nem lett-e megváltoztatva a konfiguráció.

7.6.12. Konfigurációs beállítások (3.3.6.6. [3]), {6.23}

Az Intézet 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 konfigurációs beállítást, és:

- ezt ellenőrzési listaként dokumentálja;
- elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;
- a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést;
- figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait.

7.6.13. Legszűkebb funkcionalitás (3.3.6.7. [3]), {6.26}

Az Intézet az egyes konfigurációkat csakis a feladatainak ellátására használt legszűkebb funkcionalitással implementálja és használja.
Az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

7.6.13.1. Rendszeres felülvizsgálat (3.3.6.7.2. [4])

Az Intézet meghatározott gyakorisággal átvizsgálja az elektronikus információs rendszert, meghatározza és kizárja, vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

7.6.13.2. Nem futtatható szoftverek (3.3.6.7.3. [4])

Az Intézet meghatározza, rendszeresen felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható szoftverek listáját és megtiltja ezek futtatását.

7.6.14. Elektronikus információs rendszerelem leltár (3.3.6.8. [2], 3.3.6.8.2. [4])

Az Intézet leltárt készít az elektronikus információs rendszer elemeiről. Gondoskodik arról, hogy a leltár:

- pontosan tükrözze az elektronikus információs rendszer aktuális állapotát;
- az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza;
- legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez;
- az Intézetrendszeresen, de legalább negyedévente felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt.

7.6.15. Konfigurációkezelési terv (3.3.6.9. [4])

Az Intézet kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat. Bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére és meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi. Védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

7.6.16. A szoftverhasználat korlátozásai (3.3.6.10. [2]), {6.36}

Az elektronikus információs rendszerrel kapcsolatban a következő szoftverhasználati korlátozásokat kell figyelembe venni:

- Az Intézetnél kizárólag az Informatikai Osztályvezető által jóváhagyott hardver és szoftver elemek használhatók.
- Az Intézet kizárólag jogtiszta szoftvereket használ.
- Az Intézet kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.
- A másolatok, megosztások ellenőrzésére nyomon követi és nyilvántartja a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát.
- Az Intézet ellenőrzi az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.
- Az Intézet felhasználói nem telepíthetnek szoftvereket az Intézet eszközeire.

7.6. Karbantartás (3.3.7.)

Az informatikai eszközök karbantartását folyamatos rendelkezésre állásuk és sértetlenségük érdekében a gyártó útmutatása alapján, előírás-szerűen el kell végezni. A karbantartási ciklus kialakításáért, partnerek szerződtetéséért az Informatikai Osztályvezető a felelős, aki:

- A karbantartások ütemezését és módját éves karbantartási tervben rögzíti, az informatikai eszközök karbantartásának konkrét időpontját 1 héttel előre meghatározza;
- írásban engedélyezi a tervezett karbantartásokat;
- kihirdeti a karbantartott eszközök felhasználói számára a karbantartások várható időpontjait;
- jóváhagyja, nyilvántartja és ellenőrzi az elektronikus információs rendszer karbantartására használt eszközöket.

A karbantartás során:

- Az eszközöket csak jóváhagyást követően lehet leállítani;
- az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani;
- amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor gondoskodni kell annak titkosításáról. A kiszállítást az Informatikai Osztályvezető engedélyezi.

A karbantartás során az Intézet ellenőrzi a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

7.7.1. Távoli karbantartás (3.3.7.4. [4])

Távoli karbantartás végzését az Informatikai Osztályvezető (IOV) engedélyezheti. Távoli karbantartást kizárólag akkor lehet elvégezni, ha annak módja dokumentálva van és szerepel az elektronikus információs rendszer rendszerbiztonsági tervében.

A távoli karbantartás és diagnosztikai tevékenységekről nyilvántartást kell vezetni, amely nyilvántartást megismerhetővé kell tenni az IBF számára.

Elvárás, hogy a távoli karbantartási és diagnosztikai javítások olyan elektronikus információs rendszerből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a szervizelt rendszer biztonsági képességeivel.

A távoli szervizelés végrehajtását követően, mielőtt újra üzembe helyezik az adott elemet, át kell vizsgálni a lehetséges kártékony szoftverek miatt.

Távoli karbantartás esetén a karbantartáshoz szükséges kapcsolatot kizárólag a karbantartás idejére szabad felépíteni a karbantartó részére. Ennek ellenőrzése az Informatikai Osztályvezető (IOV) feladata.

7.7.2. Karbantartók (3.2.1.19 [3]), {10.18}

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor az Informatikai Osztályvezető (IOV) kezdeményezi az Intézet vezetőjénél külső harmadik fél megbízását.

Karbantartási tevékenységet csak olyan külső harmadik fél végezhet, aki érvényes szerződéssel rendelkezik, a titoktartási nyilatkozatot aláírta és dokumentált formában megismerte az Intézet vonatkozó információbiztonsági előírásait.

A karbantartást végző külső felekről az Informatikai Osztályvezetőnek (IOV) nyilvántartást kell vezetni, melynek minimálisan a következőket tartalmaznia:

- a külső fél megnevezése;
- szerződésszám;
- szerződés időtartama;
- szerződéses kapcsolattartó neve, elérhetősége;

– szerződés tárgya, hatálya.

Külső munkavégzése esetén az informatikai terület vezetőjének ki kell jelölnie azokat a személyeket, akiknek folyamatos felügyeletet kell biztosítani a karbantartás során.

A külső féllel kötött szerződésbe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve, hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

7.7. Adathordozók védelme (3.3.8. [4])

Biztosítani kell az adathordozók fizikai védelmét annak érdekében, hogy a dokumentumok, a számítógépek adathordozói, a bemenet/kimenet adatai és a rendszer dokumentációi a jogosulatlan megszerzésétől, módosítástól, eltávolítástól és rombolástól megfelelően védve legyenek. A papír alapú dokumentumok kezelésére vonatkozó irányelveket és biztonsági követelményeket az Intézet Iratkezelési Szabályzata tartalmazza.

Az adathordozók kezelésének legfontosabb biztonsági követelményei:

- Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
- Meg kell védeni a dokumentumokat, a számítástechnikai adathordozókat, az input/output adatokat és a rendszerdokumentációkat a károsodástól, eltulajdonítástól, jogosulatlan megismeréstől.
- Biztosítani kell, hogy az adathordozók kezelése — a vonatkozó iratkezelési szabályok szellemében, — a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjen.
- Minden adathordozót újra alkalmazás előtt, illetve selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell, melynek módszerét egy erre irányuló törlési utasításban az Informatikai Osztályvezető határozza meg. Ha a törlés nem valósítható meg, akkor az adathordozót fizikailag kell működésképtelenné tenni olyan módon, hogy a rajta lévő információ ne legyen visszanyerhető.
- Biztosítani kell az adatok sértetlen és hiteles állapotának megőrzését.
- Minden adathordozót biztonságos környezetben, a gyártó előírásainak megfelelően kell tárolni.

7.8.1. Hozzáférés az adathordozókhoz (3.3.8.2. [2], 3.3.8.7. [2]), {11.2}

Az Intézet elektronikus információs rendszerében a következő táblázat szerint használhatók és hozzáférhetők az adathordozók:

Adathordozó	Feltétel	Felhasználói kör
Beépített adathordozók	Mindennapi munkavégzés során, beszerelve	Felhasználók
Beépített adathordozók	Kiszerelés, mozgatás	IÜFSZ, ATFSZ
Optikai adathordozók	Komponensek telepítése	IÜFSZ, ATFSZ

Adathordozó	Feltétel	Felhasználói kör
Külső, hordozható adathordozók	Komponensek telepítése, Mentések kezelése	IÜFSZ, ATFSZ
Mágneses szalagok	Mentések kezelése	IÜFSZ, ATFSZ
Papír alapú adathordozók	Iratkezelési szabályok szerint	Iratkezelési szabályok szerint

8. táblázat - Hozzáférés az adathordozókhoz

A táblázatban nem szerepelő felhasználási esetek tiltottak, ennek általános bővítése az Informatikai Osztályvezető (IOV) feladata, de írásos engedélyével egyedi kivétel adható.

7.8.2. Adathordozók címkézése (3.3.8.3. [4])

Az Intézet megjelöli az elektronikus információs rendszer adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket, ha ezek rendelkezésre állnak.
Az Intézet működése szempontjából iktatandónak minősített, papír alapú dokumentumokat elektronikus programmal vezérelt adatbázisban kell nyilvántartani, amely minden irathoz egyedi azonosító számot generál. Az ügyiratokat, és az elektronikus iktatással nem nyilvántartott egyéb irategyütteseket az irattározási szabályok alapján kell irattári tételekbe sorolni, irattári tételszámmal ellátni.

7.8.3. Az adathordozók tárolása (3.3.8.4. [4])

Az adathordozókat biztonságos helyen kell tárolni, vagy amennyiben ezek munkaközi példányok, a tartalmukat meg kell semmisíteni.
A fokozott biztonsági osztályba sorolt minősítésű adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces tűzállóságú tároló szekrényben történhet.

7.8.4. Adathordozók szállítása (3.3.8.5. [4], 3.3.8.5.2. [4])

Az Intézet tulajdonát képező számítástechnikai eszközöket, adathordozókat, programokat kizárólag az Intézet Informatikai Osztályvezetőjének (IOV) engedélyével szabad kivinni a munkahelyről. Az Intézet területéről kivitt eszközöket nyilván kell tartani és kriptográfiai védelemmel kell ellátni. Meghibásodott eszköz cseréje esetén adathordozó csak úgy vihető ki, ha arról minden adat visszaállíthatatlan módon törlésre került. A szállítás során be kell tartani a biztonsági eljárásokat.

7.8.5. Adathordozók törlése (3.3.8.6. [2]), {11.8}

Biztonságos törlés az írható és olvasható adathordozók többszörös felülírásával valósul meg, mely során az adatok törlését legalább 3 menetes törlési eljárásokkal vagy ezekkel egyenértékű, az adatok helyreállíthatatlanságát biztosító szoftverrel kell elvégezni. A szoftver a fájlok törlését követően véletlenszerű algoritmus alapján előállított adatokkal írja felül azok fizikai és logikai helyét az adathordozón.

7.8.6. Ismeretlen tulajdonos (3.3.8.7.2. [4])

Az Intézet megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

7.8.7. Adathordozók újrahasznosítása

Védett informatikai rendszerben használt adathordozót olyan szabályozott módszerek alkalmazásával kell törölni, hogy az adatok a későbbiekben ne legyenek helyreállíthatók melynek módszerét a vonatkozó törlési utasítás tartalmazza.

7.8.8. Az adathordozók selejtezése (3.3.8.6.4. [5])

Alapvető biztonsági cél, hogy az adathordozókat visszaállíthatatlanul, dokumentáltan selejtezzék. A különféle szabványokban definiált adattörlési és megsemmisítési eljárások a lehető legkisebbre csökkentik az információ kiszivárgásának kockázatát. Az érzékeny információt tartalmazó adathordozó selejtezési eljárásainak arányosnak kell lenniük az információ érzékenységével, értékével.

- Az adathordozót visszaállíthatatlan módon kell selejtezni, típustól függően fizikai vagy logikai úton.
- Selejtezés során minden adathordozót a legerősebb biztonsági eljárással kell selejtezni.
- Adathordozó selejtezéssel foglalkozó cég igénybevétele esetén kulcsfontosságú biztonsági tényező a megfelelő kvalitású szerződő fél kiválasztása, valamint az informatikai biztonsági feltételek szerződésbe foglalása.
- Azok az adathordozók, amelyeket nem lehet törölhetők, azokat fizikailag meg kell semmisíteni.
- Az adathordozó védelme csak az adatok törlését, valamint a bizalmas adattartalomra utaló valamennyi jelzést eltávolítását követően szüntethető meg.

Papíralapú dokumentáció esetében az Irattári Tervben rögzített őrzési idő leteltével iratselejtezést kell végezni. A selejtezést az Iratkezelési Szabályzatban foglaltak szerint kell végrehajtani. Iratselejtezés csak a felelős vezető előzetes engedélyével és jegyzőkönyv felvételével történhet.
Az informatikai biztonságra vonatkozó iratok és dokumentációk selejtezése csak visszaállíthatatlan iratmegsemmisítéssel történhet meg.

7.8.9. Adathordozók megsemmisítése (3.3.8.1. [2]),

Az adathordozók típusának és fizikai megvalósulásának megfelelő módszert kell választani a megsemmisítéséhez, melynek módszerét a vonatkozó törlési utasítás tartalmazza Az adathordozók megsemmisítése a következő módszerekkel engedélyezett:

- **Mágnesszalagok:** El kell távolítani a tokból, majd mechanikusan be kell zúzni, kémiai úton megsemmisíteni vagy elégetni.
- **Lemezek:** A lemezt szabálytalan alakú darabokra kell vágni, a darabokat deformálni kell vagy elégetni.
- **Merevlemezek:** A mágneses felületet és a mechanikát is érintő mechanikai sérülést kell okozni, amely a lemezt működésképtelenné teszi.
- **Más szilárd anyagú tárolók**: össze kell törni, kémiai úton használhatatlanná tenni vagy el kell égetni.

7.9. Azonosítás és hitelesítés (3.3.9.)

7.9.1. A felhasználók azonosítása (3.3.9.2. [2]), {8.2}

7.9.1.1. Felhasználói azonosítókkal szemben támasztott követelmények

A felhasználó azonosító az informatikai rendszert használó identitásának egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas megjelenítése kell, hogy legyen az informatikai rendszerben. A felhasználók közé sorolandók a természetes személyek, folyamatok, vagy egyéb eszközök egyaránt. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni. Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz, adatokhoz való hozzáférést megfelelően szabályozza (korlátozza) és követhető, ugyanakkor a biztonsági funkciók működése során ellenőrizhető legyen a biztonsági rendszer számára.

7.9.1.2. A felhasználói azonosítók képzésének és kezelésének szabályai

- A felhasználó-azonosítónak minden esetben egyedinek kell lennie, (azaz semmilyen körülmények között sem adható ki különböző felhasználók részére megegyező azonosító). Azonosítási problémák elkerülése végett, csoportazonosítók kiadása tilos, minden esetben egyértelműen meg kell tudni határozni a felhasználó személyét. Kivételt képeznek azok az azonosítók (technikai felhasználók), ahol azokra működési vagy üzemeltetési okokból feltétlenül szükség van, ezek legyenek szakmailag megindokolva, vezető által jóváhagyva és dokumentálva.
- A felhasználói azonosítók képzését lehetőleg egységes névkonvenciós szabályozás alapján kell végezni.
- Tilos más azonosítójának használata. A kapott felhasználói azonosítót haladéktalanul érvényesíteni kell.
- A tartósan távollévő felhasználók felhasználói azonosítóját le kell tiltani, illetve munkába állásukkal egy időben ismét engedélyezni kell.
- Az alkalmazottak áthelyezése kapcsán felmerülő változásokat az áthelyezéssel egyidőben, haladéktalanul át kell vezetni.
- Harmadik személyek, akik valamilyen okból igénybe vehetik az Intézet bármelyik rendszerének szolgáltatásait, csak a kiadáskor előre meghatározott időre, és korlátozott lehetőségeket biztosító felhasználói azonosítót kaphatnak. A részükre kiadott azonosító szerkezetileg feleljen meg az Intézeten belüli alkalmazottak azonosítójával, de legyen egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító egy harmadik (külső) személyé.
- Ha egy felhasználó azonosító 30 napot meghaladóan inaktívnak bizonyul, azonosítóját le kell tiltani és erről a munkahelyi vezetőjét haladéktalanul értesíteni szükséges, megjelölve az érvénytelenítés okát.
- A felhasználókkal alá kell íratni egy nyilatkozatot, amely dokumentálja, hogy megértették a hozzáférés feltételeit, felelősségeit.
- Azonnal zárolni kell az olyan felhasználó azonosítókat, amelyek valószínűleg kompromittálódtak.
- A lezárt felhasználói neveket nem lehet más személynek kiadni, egyezés esetén úgy kell eljárni, mintha a lezárt felhasználói név is használatban lenne.

7.9.1.3. Felhasználói azonosítók nyilvántartása

A felhasználói azonosítókat nyilván kell tartani és mindennemű változást naplózni kell.

7.9.2. Felhasználók hitelesítése (3.3.9.2. [2]), {8.2}

7.9.2.1. A hitelesítők képzéseinek és használatuknak szabályai

Az Intézet informatikai rendszereiben a felhasználók hitelesítésének alapvető módja a jelszó megadása. A felhasználói jelszavak kezelésére a következő szabályokat kell alkalmazni:

- Belépéskor megkapott jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes azonosítása után. Az ideiglenes jelszavak véletlenszerűen generáltak, csak korlátos időtartamig lehetnek érvényesek, megváltoztatásuk kötelező.
- Technikai felhasználók, valamint beépített (privilegizált) felhasználók jelszavait oly módon kell tárolni, hogy csak arra felhatalmazottak férhessenek hozzá, illetve a hozzáférések naplózottak legyenek.
- Amennyiben egy technikai felhasználói fiókhoz többen is hozzáférnek és a hozzáféréshez jogosultak listája változik, a csoport felhasználói fiókokhoz tartozó hitelesítő eszközöket vagy adatokat újra ki kell bocsátani.
- Jelszó alapú hitelesítő rendszer használata esetén a jelszavakat cserélni kell minden esetben, ha kompromittálódnak, vagy illetéktelen személy birtokába jutnak.

7.9.2.2. A hitelesítés kezelése az informatikai rendszerekben (3.3.9.5.2 [4])

A hitelesítésre szolgáló eszközök kiosztásakor ellenőrizni kell az eszközt átvevő egyén vagy eszköz jogosultságát, az átadás tényét dokumentálni kell.

- A jelszavaknak minden felhasználó számára szabadon megváltoztathatónak kell lennie, saját maga által vagy informatikus munkatárs közreműködésével.
- A **felhasználói** jelszavak minőségére vonatkozó szabályokat az IBF határozza meg.
- Az **adminisztrátori** jelszavak minőségére vonatkozó szabályokat az IBF határozza meg.
- A kriptográfiai kulcsok hosszúságának meghatározásakor a vonatkozó szabványokban előírt minimális kulcshosszt és módszereket kell alkalmazni.
- A jelszavak titkosítatlan formában való tárolása az Intézet jogosult személyeken túlmenő személyek számára hozzáférhető rendszereiben szigorúan tilos! (Ez alól kivételt csak a technikai és beépített rendszergazdai jelszavak papíralapú, lezárt borítékban és páncélszekrényben történő tárolása jelenthet.)
- A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani, papír alapon rögzíteni vagy bármely más módon más számára is megismerhetővé tenni tilos.

7.9.2.3. Felhasználói tanúsítványhordozó eszközök nyilvántartása

A kiadott tanúsítványhordozó eszközről naprakész nyilvántartást kell vezetni.

7.9.2.4 Hitelesítésre szolgáló eszközök kezelése (3.3.9.5.3. [4])

Az Intézet:

- ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, szerepkör vagy eszköz jogosultságát;
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

- biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;
- megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;
- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;
- a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló 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.

7.9.2.5. Speciális felhasználókhoz tartozó jelszavak kezelése

- Beépített adminisztrátori fiókok, technikai felhasználók jelszavait lezárt borítékban az Informatikai Osztályvezető (IOV) páncélszekrényében kell őrizni, és/vagy olyan jelszókezelő alkalmazásban, mely a hozzáféréseket naplózza.
- A speciális felhasználók jelszavához csak különösen indokolt esetben lehet hozzáférni.
- A boríték felbontásáról minden esetben jegyzőkönyvet kell készíteni megjelölve a speciális felhasználó igénybevételének pontos okát és a felbontók személyét.
- Jelszókezelő alkalmazásban naplózni kell a hozzáféréseket.
- Gondoskodni kell arról, hogy a szükséges műveletek elvégzése után a speciális felhasználó számára új jelszó kerüljön kiadásra és azt haladéktalanul, lezárt borítékban ismét az Informatikai Osztályvezető (IOV) páncélszekrényébe kell helyezni, és/vagy fel kell vezetni a jelszó kezelő alkalmazásban.

7.9.2.6. Jelszó (tudás) alapú hitelesítés (3.3.9.5.2. [4])

Az Intézet a jelszóra a következő elvárásokat érvényesítheti:

- kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;
- meghatározott számú karakterváltozást kényszerít ki új jelszó létrehozásakor;
- a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást) és nem továbbítja;
- a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

7.9.2.7. Birtoklás alapú hitelesítés (3.3.9.5.3. [4])

- Az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az Intézet által meghatározott minőségi követelményeknek, vagyaz elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:

- ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;
- kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;
- összekapcsolja a hitelesített azonosságot az egyéni fiókkal;
- megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

7.9.2.8. Tulajdonság alapú hitelesítés (3.3.9.5.4. [4])

Az Intézet — a megfelelő technológiai eszközök rendelkezése állása esetén — a felhasználó egyedi (biometrikus) azonosítást lehetővé tevő tulajdonságai alapján végezheti el az azonosítást az alábbiak segítségével:

- ujjlenyomat,
- retina,
- tenyér-erezet,
- írisz,
- arcfelismerés,
- aláírás,
- hang.

7.9.3. Felhasználói fiókok kezelése (3.3.10.2. [2]), {2.2}

Az Intézet elektronikus információs rendszerei központi címtárat használnak, amelyek karbantartása a rendszergazdák feladata az Informatikai Osztályvezető (IOV) felügyeletével. Felhasználói fiókok létrehozására, módosítására csak a felhasználó felettesének (Szervezeti egység vezető, SZEV), az Informatikai Osztályvezető (IOV) jóváhagyásával ellátott írásos igény után kerülhet sor. (Ez alól kivételt az incidenskezelésben és az üzletmenet-folytonossági tervben meghatározott beavatkozások jelenthetnek.)

Az elektronikus információs rendszer fióktípusai:

Fióktípus	Felhasználói kör	Megjegyzés
Rendszergazda	Rendszergazdák	Csak privilegizált műveletek végrehajtásához. A csoport tagjai az informatikai osztály munkatársai, fiók kiadása az Informatikai Osztályvezető (IOV) egyedi jóváhagyásával.
Felhasználó	Rendszergazdák	Mindennapi munkához, a csoport tagjai a rendszergazdai jogokkal is rendelkező felhasználók.
Felhasználó	Felhasználók	Mindennapi munkához, a csoport tagjai az elektronikus információs rendszerhez érvényes hozzáférési engedéllyel rendelkező alkalmazottak.

9. táblázat - Fióktípusok

A BYOD típusú eszközök esetén az eszköz rendszergazdai jogköreinek intézeti rendszergazdákra való korlátozása feltétele lehet az eszköznek az Intézet erőforrásaihoz való kapcsolódónak. Ennek egyedi elbírálását a felhasználó informatikai biztonsági kompetenciáinak, az elérni kívánt erőforrások kockázati szintjének — figyelembevételével az Informatikai Osztályvezető (IOV) végzi.

A rendszergazdák feladata a felhasználói fiókok rendszeres felülvizsgálata, mely során ellenőrizni kell a fiókkezelési követelményekkel való összhangot.

Az elektronikus információs rendszernek — amennyiben a rendszer technikailag azt lehetővé teszi — automatizált mechanizmusokat kell alkalmaznia az elektronikus információs rendszer fiókjainak kezeléséhez, különösen:

- automatikusan eltávolítja, vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, ha azokat 30 napig nem használták,
- automatikusan letiltja a véglegesen inaktív fiókokat,
- a felhasználói fiókok használatának ellenőrzésére (szokatlan viselkedési minták keresése).

Az érintett szervezeti egység vezető felelőssége értesíteni a rendszergazdákat, ha

- egy felhasználói fiókokra már nincsen szükség;
- egy felhasználó kilép vagy áthelyezésre kerül;
- a szervezeti egységhez tartozó elektronikus információs rendszer használata, vagy használatához szükséges feltételek megváltoznak.

7.9.3.1. Személyes vagy megbízható harmadik fél általi regisztráció (3.3.9.5.5. [4])

Az Intézet meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs szervezet folytat le az Intézet által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

A jelenleg támogatott hitelesítési eszközök:

Hitelesítő eszköz	Regisztrációs egység	Jóváhagyó
Jelszó	Informatikai osztály	IBF, SZEV
Kétfaktoros autentikációhoz használt hardver, mobiltoken	EESZT STS rendszer	EESZT üzemeltetés

IO. táblázat - Hitelesítő eszközök regisztrációja

7.9.3.2. Sikertelen bejelentkezési kísérletek (3.3.10.7. [3]), {2.71}

Az Intézet meghatározott esetszámú korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire. Amennyiben a sikertelen bejelentkezési kísérletek száma eléri a korlátot, úgy automatikusan zárolja a felhasználói fiókot egy meghatározott időtartamig, vagy meghatározott idővel késlelteti a következő bejelentkezési kísérletet.

7.9.4. Hálózati hozzáférés

7.9.4.1. Hálózati hozzáférés privilegizált fiókokhoz (3.3.9.2.2. [3]), {8.3}

Az elektronikus információs rendszer — amennyiben a rendszer technikailag azt lehetővé teszi — többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

7.9.4.2. Hálózati hozzáférés nem privilegizált fiókokhoz (3.3.9.2.3. [4])

Az elektronikus információs rendszer — amennyiben a rendszer technikailag azt lehetővé teszi — többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

7.9.4.3. Hálózati hozzáférés privilegizált parancsokhoz (3.3.10.6.7. [5])

A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell.

7.9.5. Helyi hozzáférés

7.9.5.1. Helyi hozzáférés privilegizált fiókokhoz (3.3.9.2.4. [4])

Az elektronikus információs rendszer — amennyiben a rendszer technikailag azt lehetővé teszi — többtényezős hitelesítést alkalmaz a privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

7.9.5.2. Helyi hozzáférés nem privilegizált fiókokhoz (3.3.9.2.7. [5])

Az elektronikus információs rendszer — amennyiben a rendszer technikailag azt lehetővé teszi — többtényezős hitelesítést alkalmaz a nem privilegizált felhasználói fiókokhoz való helyi hozzáféréshez.

7.9.6. Ellenőrzés

Az IBF-nek ellenőriznie kell az azonosítás és hitelesítéssel kapcsolatos előírások maradéktalan betartását, eltérések esetén részletes eljárásrendet kell kialakítania.

7.9.7. A hitelesítésre szolgáló eszköz visszacsatolása (3.3.9.6. [2]), {8.36}

Az elektronikus információs rendszerben csak olyan rendszerelemek használhatók fel, amelyek fedett visszacsatolást biztosítanak a hitelesítési folyamat során.

7.9.8. Hitelesítés kriptográfiai modul esetén (3.3.9.7. [3]), {8.37}

Az Intézet nem használ hardveres kriptográfiai modult.

7.9.9. Azonosítás és hitelesítés (Intézeten kívüli felhasználók) (3.3.9.8. [2]), {8.38}

Harmadik személy csak a kiadáskor előre meghatározott időre, és korlátozott lehetőségeket biztosító személyes felhasználói azonosítót kaphatnak. Ilyen jogosultságot csak különösen indokolt esetben, vezetői kérésre, az Informatikai Osztályvezető (IOV) jóváhagyása esetén lehet kiadni.

7.9.10. Hitelesítés szolgáltatók tanúsítványának elfogadása (3.3.9.8.2. [2])

Az azonosításhoz és a hitelesítéshez felhasznált tanúsítványok csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő a szolgáltatók által kibocsátott

tanúsítványok lehetnek, valamint az Intézet Informatikai Vezetője (IOV) által meghatározott külső és belső tanúsítvány kiadók.

7.10. Hozzáférés az informatikai rendszerekhez (3.3.10., 3.3.10.1. [2]), {2.1}

Az Intézet elektronikus információs rendszereinek ki kell kényszerítenie az azonosítást, ezekben tilos azonosítás vagy hitelesítés nélküli tevékenységeket végezni.

7.10.1. Általános alapelvek

Az információs rendszerek illetéktelen elérésének megakadályozása érdekében megfelelő hozzáférés védelmi rendszert kell kialakítani. Hozzáférés iránti, illetve jogosultság módosítására, hozzáférés törlésére vonatkozó igény csak írásban kérhető. A beérkezett igényeket nyilvántartásba kell venni. A kiadott engedélyek listáját naprakészen kell tartani.

A jogosultságok megadásának alapvető biztonsági intézkedései:

- azonosítani kell, a hozzáférést kérő személyét, a kívánt és adható jogokat, valamint az érintett rendszert,
- a felhasználók hozzáférési jogosultságait a minimálisan szükséges jogok alapján kell megadni,
- a jogosultságok kiosztásának dokumentáltnak és engedélyezettnek kell lenniük,
- a rendszergazdai és egyéb előjogokat a rendes működési használattól eltérő használói azonosítóhoz kell kötni,
- kerülni kell a rendszeradminisztráció előjogainak nem megfelelő alkalmazását.

Minimálisan a következő jogokat kell megkülönböztetni:

- olvasási jog (betekintés);
- létrehozási jog;
- módosítási jog;
- törlési jog.

Az adminisztrációs és naplózási jogoknak el kell különülni a felhasználói jogoktól.

A rendszereknek alkalmasnak kell lenniük a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultsági csoportokat kell kialakítani.

7.10.2. Hozzáférés ellenőrzés eljárásrendje (3.3.10 [2]) {2.1}

Az Intézetnél csak olyan elektronikus információs rendszer használható, amely képes a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

7.10.2.1. Ellenőrzés informatikai rendszerekben

Az informatikai rendszerekben biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága a szerepkörüknek megfelelő legyen. Ennek érdekében:

- A jogosultságokat rendszeres időközönként felül kell vizsgálni.
- Az általános felhasználók esetében: 12 havonta, kiemelt jogosultsággal rendelkező felhasználók esetében legalább 6 havonta.

- Rendszeresen ellenőrizni kell, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók és eszközök rendelkezhessenek.
- A szerepkörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni és az új szerepkörnek megfelelően módosítani kell.
- Az ellenőrzést az Informatikai Osztályvezető által kijelölt személy végzi el.

7.10.2.2. Az operációs rendszerhez való hozzáférés ellenőrzése

Az informatikai eszközök illetéktelen elérésének megakadályozása érdekében az operációs rendszer szintjén rendelkezésre álló biztonsági lehetőségeket is fel kell használni a számítástechnikai erőforrásokhoz való hozzáférés korlátozásához. Ezeknek a következőket kell lehetővé tenniük:

- Az engedéllyel rendelkező felhasználó személyének azonosítása és hitelesítése, szükség esetén a terminál vagy hely azonosítása.
- A sikeres és az eredménytelen hozzáférési kísérletek rögzítése.
- Megfelelő hitelesítési eszközök és — jelszókezelő rendszer használata esetén — minőségi jelszavak biztosítása.
- Különleges rendszergazdai jogosultságok használatának naplózása (Pl. rendszergazda jogosultsággal rendelkező felhasználók esetében).
- Adott esetben a felhasználók csatlakozási idejének korlátozása.
- Amennyiben a kockázatok alapján ez indokolt, más hozzáférést vezérlő módszereket (például ujjlenyomat, chipkártya, kérdés-felelet) is használni kell.
- A távoli hozzáférések esetén — amennyiben az lehetséges — telepített kriptográfiai kulcsot kell alkalmazni.

7.10.2.3. Privilegizált fiókok (3.3.10.6.4. [4])

Az Intézet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

7.10.2.4. Nem privilegizált hozzáférés a biztonsági funkciókhoz (3.3.10.6.3. [4])

Az Intézet kötelezővé teszi, hogy az Intézet által meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják. Ezekben az esetekben a kiemelt jogosultságú felhasználók egy másodlagos fiókkal is kell, hogy rendelkezzenek.

7.10.2.5. Privilegizált funkciók tiltása nem privilegizált felhasználóknak (3.3.10.6.6. [4])

Az elektronikus információs rendszer megakadályozza, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését vagy megváltoztatását.

7.10.2.6. Jogosult hozzáférés a biztonsági funkciókhoz (3.3.10.6.2. [4])

Az Intézet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

7.10.2.7. Legkisebb jogosultság elve (3.3.10.6.1. [4])

Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

7.10.2.8. A felelősségek szétválasztása (3.3.10.5. [4])

Az Intézet szétválasztja az egyéni felelősségeket.
Dokumentálja az egyéni felelősségek szétválasztását;
Az Intézet meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

7.10.3. Hálózati hozzáférés

7.10.3.1. Távoli hozzáférés (3.3.10.13. [3]), {2.100}

Távoli hozzáférés esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.
A távolról csak a kijelölt csatlakozási (hozzáférési) pontokon keresztül szabad csatlakozni az Intézethálózatába. Az Informatikai Osztályvezető (IOV) feladata meghatározni a belépési pontokat, illetve elbírálni a távoli hozzáférések kiadására vonatkozó, írásban vagy elektronikus csatornán érkező kérelmeket.
A távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére kriptográfiai mechanizmusokat kell alkalmazni.
Az Intézet informatikai rendszeréhez kapcsolódni csak VPN csatornán keresztül lehet.
A VPN használatához a szabályzatban meghatározott erősségű autentikáció és autorizáció szükséges. (felhasználónév, jelszó, e-token, stb.)
A távoli hozzáféréseket automatizált módon figyelni és felügyelni kell.

7.10.3.2. Privilegizált parancsok elérése (3.3.10.13.5. [4])

Az Intézet privilegizált parancsok végrehajtásához és biztonságkritikus információk eléréséhez távoli hozzáférést csak meghatározott és elfogadott igény esetén engedélyez, dokumentálja és indokolja a hozzáféréseket a rendszerbiztonsági tervben.

7.10.3.3. Visszajátszás-védelem (3.3.9.2.5. [4])

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

7.10.3.4. Távoli hozzáférés - külön eszköz (3.3.9.2.6. [4])

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

7.10.3.5. Visszajátszás ellen védett hálózati hozzáférés nem privilegizált fiókokhoz (3.3.9.2.8. [5])

Az elektronikus információs rendszer visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a nem privilegizált felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

7.10.4. Biztonságos hitelesítő, bejelentkező eljárások (3.3.13.16. [3])

7.10.4.1. Munkaállomások automatikus azonosítása, hitelesítése

A munkaállomás automatikus azonosítása kötelező, ha fontos és indokolt, hogy egy munkát, vagy tranzakciót csak egy adott terminálról lehessen kezdeményezni.
Technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásokról, címekről lehessen a rendszerekbe belépni.
Egységes munkaállomás névhasználatot kell kialakítani.
A LAN hálózatban biztosítani kell az idegen gép felismerését és az erőforrásokhoz történő hozzáférésének megakadályozását (pl. port security address összerendeléssel), menyiben erre a technikai feltételek rendelkezésre állnak.

7.10.4.2. Biztonságos bejelentkezési eljárások

A számítógéprendszerbe való bejelentkezési folyamatnak minimumra kell csökkentenie az illetéktelen hozzáférés lehetőségét, amennyiben a rendszer azt lehetővé teszi, az alábbi intézkedésekkel.
Csak a bejelentkezés eredményes befejezése után jelenhet meg a használni kívánt rendszerre vonatkozó adat, azonosító, stb.
A bejelentkezés elfogadására vagy elvetésére csupán az összes szükséges adat megadása után kerülhet sor, sikertelenség esetén nem adhatja vissza a hibás, elrontott azonosítót, jelszót.
Korlátozni kell az eredménytelen bejelentkezési kísérletek számát. Rögzíteni kell az eredménytelen kísérleteket, pl. próbálkozásonként egyre nagyobb késleltetést kell alkalmazni, mielőtt további bejelentkezési kísérletet engednek meg, illetve időtúllépés esetén meg kell szüntetni az adatátviteli kapcsolatot.
Minősített esetben vészjelzést kell küldeni a rendszer-kezelőpulthoz, ha elérték a legnagyobb számú bejelentkezési kísérletet.
A jelszóval való visszaélések és az ehhez kapcsolódó biztonsági események könnyebb felderíthetősége érdekében belépés után a rendszer jelezze ki a következőket:

- az előző sikeres bejelentkezés dátumát és időpontját;
- az utolsó sikeres bejelentkezés óta végzett sikertelen bejelentkezési kísérletek részletes adatait.

7.10.4.3. Eszközök azonosítása és hitelesítése (3.3.9.3. [4])

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi, vagy távoli hálózati kapcsolatot létesítene velük.

7.10.5. A rendszerhasználat jelzése (3.3.10.8. [3]), {2.75}

Az Intézet meghatározott rendszer használatra vonatkozó figyelmeztető üzenetet vagy jelzést küldhet a felhasználó számára a rendszerhez való hozzáférés engedélyezése előtt, mely jelezheti, hogy:

- a felhasználó az Intézet elektronikus információs rendszerét használja;

- a rendszer használatot figyelhetik, rögzíthetik, naplózhatják;
- a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár;
- a rendszer használata egyben a felhasználó előbbiekbe történő beleegyezését is jelenti.

7.10.6. Mobil eszközök hozzáférés ellenőrzése (3.3.10.15. [3]), {2.113}

Amennyiben az eszközön helyileg is találhatóak adatok, illetve az Intézet informatikai rendszeréből lokális adathordozóra történő adatáthelyezésre van jogosultsága, akkor az eszközt teljes eszköztitkosítással, tároló alapú titkosítással, vagy más technológiai eljárással kell ellátni az eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére. Az eszköz — bekapcsolt állapotban, zárolás nélkül — soha nem maradhat felügyelet nélkül.
A gyártó előírásait mindig be kell tartani az eszköz védelme érdekében. Alkalmazni kell az azonosítás hitelesítésénél megadott szabályokat.

7.10.7. Vezeték nélküli hozzáférés (3.3.10.14. [3]), {2.108}

Az Intézet rendszereihez közvetlen vezeték nélküli hozzáférés nem alakítható ki. A vezeték nélküli hozzáférési pontok bekötése az elektronikus információs rendszertől elkülönített biztonsági zónába történhet, amelyből meghatározott feltételek mellett lehet eszközöket csatlakoztatni az Intézet belső rendszereihez.
A vezeték nélküli hozzáférést

- minden esetben az Informatikai Osztályvezetőnek (IOV) kell írásban engedélyeznie;
- a biztonsági architektúra tervben fel kell tüntetni és a kriptográfiával szembeni elvárásoknak megfelelően kell konfigurálni;
- azonosítást kell megkövetelnie - amely, ha jelszó alapú- azt 30 naponta meg kell változtatni.

Az Informatikai Osztályvezető (IOV) által nem engedélyezett, a biztonsági zónában vagy a belső hálózatban feltalált hozzáférési eszközöket haladéktalanul blokkolni kell.
A nyílt internet hozzáférést biztosító zónába történő vezeték nélküli kapcsolódás feltételrendszerét az Informatikai Osztályvezető (IOV) dolgozza ki.

7.10.8. Külső elektronikus információs rendszerek használata (3.3.10.16. [2]), {2.115}

Az Intézet rendszereihez külső elektronikus információs rendszert csak az Informatikai Osztályvezető (IOV) engedélyével lehet csatlakoztatni. A csatlakoztatást megelőzően az IBF kockázatelemzést végez a csatlakozás lehetséges kockázataival kapcsolatban és meghatározza a csatlakozás módját. Ebben rögzíteni kell, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az Intézet rendszereihez, valamint meg kell határozni, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani az Intézet által ellenőrzött információkat.

7.10.8.1. Korlátozott használat (3.3.10.16.2. [4])

Az Intézet csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az azáltal ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

- előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelő módon; vagy

– jóváhagyott kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

7.10.8.2. Hordozható adattároló eszközök (3.3.10.16.3. [4])

Külső elektronikus információs rendszer felhasználásának vonatkozásában a hordozható adattároló eszközök használata minden esetben csak az Informatikai Osztályvezető (IOV) egyedi elbírálásával, írásban engedélyezésével történhet.

7.10.9. Információáramlás ellenőrzés érvényesítése (3.3.10.4. [4])

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzéséhez az Intézet által meghatározott információáramlás ellenőrzési szabályoknak megfelelően.

7.10.10. Lezárással járó inaktivitás (3.3.10.11. [4], 3.3.10.10.2. [4], 3.3.10.10. [4])

A bejelentkezett felhasználói tevékenységeket igénylő munkahelyeken 30 perc inaktivitás után vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést:

- Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt;
- A képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni;
- A rendszer megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

A felhasználók kötelessége a munkaszakasz lezárása, amennyiben (akár átmenetileg is) felügyelet nélkül hagyják a munkaállomásukat.

7.10.11. Információ megosztás (3.3.10.17. [4])

Az Intézet elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet.
Az Intézet automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

7.10.12 Nyilvánosan elérhető tartalom (3.3.10.18. [2]), {2.124}

Az Intézet nyilvánosan hozzáférhető rendszerként definiálja az Intézet publikus weboldalát.

Az oldal tartalmáért felelős szervezeti egység vezetőjének gondoskodni kell az azon publikált információk törvényi megfelelőségéről, valódiságáról, és sértetlenségéről. Tilos hatályos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni. A felkerülő tartalmakat minden esetben ellenőriznie kell az adott szervezeti egység vezetőjének és csak a jóváhagyása után publikálhatók az információk. A publikus weboldalnak gondosan szegmentáltnak kell lennie az Intézet belső hálózatától arra alkalmas eszközzel. Gondoskodni kell a weboldal jogosult használata közben történő jogosulatlan elérések megakadályozásáról. Az Intézet weboldalakat

kizárólag a Főigazgató (FOIG) engedélyével, az általa meghatározott tartalmi keretek között hozhat létre.

7.11. Rendszer és információsértetlenség (3.3.11., 3.3.11.2. [2]) {18.1}

Az egyes alkalmazásokhoz és hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse.
A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sérthetetlenségét.
Számítógépes adatvesztés vagy adatsérülés esetén az adatfeldolgozást az adatokat tartalmazó rendszernél azonnal fel kell függeszteni és a kijelölt informatikust azonnal értesíteni kell. Az értesítés történhet e-mail, telefon vagy személyes bejelentés útján. A felmerült probléma tisztázása után a kijelölt informatikus útmutatása szerint lehet csak folytatni a további munkát.
Az integritás sérülésének gyanúja esetén azonnal meg kell kezdeni a körülmények, az okozott kár és a felelősség kivizsgálását. Ez alól kivételt képez, ha az integritássérülésnek következményeképpen várható kár mértéke alacsony és az integritás helyreállítása az adott rendszer eszközeivel megfelelően naplózott módon megoldható (pl. egy téves adatbevitel).

7.11.1. Hibajavítás (3.3.11.3. [2]), {18.2}

Az Intézet azonosítja, az adott rendszerre vonatkozó, a rendszer szállítójával kialakított belső eljárásrendje (pl. kontakt center, ticketing, stb.) alapján jelenti és kijavítja vagy kijavíttatja az elektronikus információs rendszer hibáit.
Telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket az Intézet feladatellátásának hatékonysága, a szóba jöhető következmények szempontjából.
Az Intézet a biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíti vagy telepítteti, beépíti a hibajavítást a konfigurációkezelési folyamatba.

7.11.1.1. Automatizált hibajavítási állapot (3.3.11.3.2. [4])

Az Intézet automatizált mechanizmusokat alkalmaz az elektronikus információs rendszer elemei hibajavítási állapotának meghatározására. Az automatizált felügyeleti környezet működtetése az IT infrastruktúra fejlesztésért és üzemeltetésért felelős személy (IÜFSZ) feladata.

7.11.2. Kártékony kódok elleni védelem (3.3.11.4. [2]), {18.8}

Az Intézetinformatikai rendszereit védeni kell a kártékony kódok ellen. Ennek érdekében a következőket kell betartani:

- A határvédelmi programoknak a szervereken folyamatosan kell működniük. A programoknak folyamatosan vizsgálniuk kell a bejövő hálózati forgalmat (levelezés, web).
- A határvédelmi szoftverrendszer elemeinek (programok, szabályrendszerek, vírusdefiníciós adatbázisok) frissítéséről automatizált módszerrel gondoskodni kell. A frissítések hiba nélküli megtörténtét ellenőrizni kell.
- Hálózati munkaállomások az internethez kizárólag az Intézet internet kijáratán (központi tűzfalán) keresztül csatlakozhatnak.
- Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem üzemeltethető.
- A vírusvédelemnek a klienseken, rezidens módon kell futniuk, azaz a rendszer indulásakor automatikusan indul a program, illetve folyamatosan vírusellenőrzést kell végrehajtani a

klienseken, amely vizsgálatok eredményét ellenőrizni kell. A vírusvédelemnek a rendszer következő komponenseire kell kiterjednie: fájlok, rendszeradatok, webes és e-mail hálózati forgalom.

- A munkaállomásokon valós idejű ellenőrzést (azonnali riasztást) biztosító vírusvédelmet kell használni.
- A felhasználónak tilos vírusirtót, személyes tűzfalat, vagy egyéb biztonsági szoftvert telepítenie.
- Külső helyekről származó adattárolókat (Intézeti okból történő) használat előtt vírusellenőrzésnek kell alávetni és csak akkor lehet használni, ha az adathordozó a vizsgálaton megfelel.
- Vírusfertőzés gyanúja vagy nem üzemszerű működés esetén a felhasználóknak haladéktalanul értesítenie kell a kijelölt informatikust, hogy a szakértők megvizsgálják az eseményt, és hiba esetén gondoskodjanak annak elhárításáról.
- Vírusfertőzés gyanúja esetén az Intézet informatikusai a fertőzött gépet lezárhatják, annak használatát a hiba elhárításáig felfüggeszthetik.
- Az a felhasználó, aki az adatait és adathordozóit a vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól bármilyen indokkal kivonja, az abból eredő károkért teljes felelősséggel tartozik.
- A vírusfigyelmeztetésekkel foglalkozó felelősök (rendszergazdák), feladata, hogy figyelemmel kísérjék a legfrissebb vírusok megjelenésével kapcsolatos híreket. – Vírusfigyelmeztetéssel kapcsolatos levelet csak a rendszergazdák küldhetnek.

7.11.2.1. Központi kezelés (3.3.11.4.2. [4])

Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

7.11.2.2. Automatikus frissítés (3.3.11.4.3. [4])

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

7.11.2.3. Vírustámadás elleni védekezés

A kijelölt informatikus feladata, hogy a felhasználói munkaállomásokra, illetve a mobil gépekre telepített vírusvédelmi rendszerek karbantartásáról gondoskodjon, a felhasználóknak támogatást nyújtson, továbbá a vírusdefiníciós állományok és a keresőmotorok szükséges frissítéseiről gondoskodjon.

7.11.2.4. Vírusvédelmi szoftverek használata

A vírusvédelmi rendszerek kiválasztását az Informatikai Osztályvezetőnek (IOV) a rendszergazdák és az IT infrastruktúra fejlesztésért és üzemeltetésért felelős személy (IÜFSZ) javaslata alapján jóvá kell hagynia. A vírusvédelmi rendszer kiválasztásakor figyelembe kell venni a következő szempontokat:
Nem megfelelő vírusvédelmi rendszer alkalmazásával az Intézet vírusvédelme nem lesz kielégítő.
A nem megfelelő vírusvédelmi szoftver lassítja a műveleteket és túlzott erőforrás igényt támaszthat. A rendszerek lassulása növeli a sebezhetőséget is.
A vírusvédelmi szoftverek vírusdefiníciós állomány állományainak frissítési gyakoriságát.

7.11.3. Szoftver- és információsértetlenség (3.3.11.8. [4])

Az Intézet sértetlenség ellenőrző felügyeleti eszközt alkalmaz a szoftverek és információk jogosulatlan módosításának észlelésére.

7.11.4. Kéretlen üzenetek elleni védelem (3.3.11.9. [S4])

Az Intézet kéretlen üzenetek - úgynevezett spam, levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében.
Új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabályzattal és eljárásrenddel.
Az Intézet központi beállításokkal irányítja a levélszemét elleni védelmet, amely jellegénél fogva valószínűségi döntésekkel akadályozza meg a levelek továbbítását.
Az Intézetben a spam-ek tömeges továbbítását lehetővé tevő nyitott levelező kiszolgáló nem működtethető.

7.11.5. Bemeneti információ ellenőrzés (3.3.11.10. [S4])

Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

7.11.6. Hibakezelés (3.3.11.11. [S4])

Az elektronikus információs rendszer hibajelzéseket generál a hibajavításhoz szükséges információkat biztosítva, ugyanakkor nem nyújt semmi olyan információt, amelyet a támadók kihasználhatnak. A hibajelzéseket kizárólag a meghatározott személyek vagy szerepkörök számára teszi elérhetővé.

7.11.7. Az elektronikus információs rendszer felügyelete (3.3.11.5. [2]), {18.13}

Az Intézet rendszereinek napi üzemeltetéséhez tartozik azok működésének felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.
Az Intézet rendszereinek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg. Ennek érdekében:

- Meg kell ismerni az Intézet rendszereszközeinek, elektronikus információs rendszereinek működését, azok figyelmeztető és hibaüzeneteit, amelyekre alkalmazni kell tudni a szükséges reagálásokat tartalmazó leírásokat.
- Rendszeresen el kell végezni azokat a tevékenységeket, amelyek alapján meg lehet győződni arról, hogy a felügyelt rendszer üzemszerűen működik.
- Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.
- Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.
- Az elektronikus információs rendszer riassza az Intézet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

7.11.8. Biztonsági riasztások és tájékoztatások (3.3.11.6. [3]), {18.37}

Az Intézet folyamatosan figyeli a Nemzeti Kibervédelmi Intézet által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket és folyamatosan figyelemmel kíséri az ezzel kapcsolatos értesítéseket. Szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez. Az IBF kiemelt feladata, hogy a jogszabályban meghatározott események bejelentési kötelezettségének eleget tegyen és kapcsolatot tartson az érintett, külön jogszabályban meghatározott szervekkel.

7.11.9. Memóriavédelem (3.3.11.13. [4])

Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.

7.11.10. A kimeneti információ kezelése és megőrzése (3.3.11.12. [2]), {18.77}

Kimeneti információk az Intézet által külső fél számára és belső használatra készített beszámolók, tájékoztatók, bizonylatok, nyilatkozatok, megrendelők, tranzakciók.
A kimeneti információk kezelésével és szétosztásával kapcsolatban a következők az előírások:

- Gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről.
- Gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódjon.
- Gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat.
- Biztosítani kell, hogy a megsemmisítési eljárások során a kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.
- A rendszer kimenő információit (pl.: EESZT naplók) a vonatkozó jogszabályok, szabályzatok szerint kell megőrizni.

7.11.11. Használatból történő kivonás

Szoftver használatból történő kivonására akkor kerül sor, ha az adott feladat végrehajtása szükségtelenné válik, vagy a végrehajtásra új eljárás került kifejlesztésre, vagy új program került beszerzésre.
A selejtezendő szoftver által kezelt adatokat — a pénzügyi és technikai lehetőségek szabta korlátokon belül — át kell alakítani az új eljárás szerinti formátumra, de meghatározott ideig, a két eljárást párhuzamosan kell használni, hogy a folyamatos működés ne szenvedjen fennakadást. Ezt az időszakot követően a szoftvert selejtezni kell, az élesben használt szoftverektől elkülönítve kell tárolni.

7.12. Naplózás és elszámoltathatóság (3.3.12., 3.3.12.1. [2]), {4.1}

Az Intézetnek az elektronikus információs rendszereiben automatikus naplót és különleges esetekben ideiglenes naplót kell vezetnie az informatikai rendszer biztonsági szempontból lényeges tevékenységeiről.
Lehetőség szerint olyan naplózási architektúrát kell kialakítani, amely azt biztosítja, hogy ahol technikailag lehetséges, a naplózás szerveroldalon és a lehető legkevesebb számú naplóállomány használatával történjen.

A naplóállományokat — amennyiben arra a feltételek adottak — központi napló gyűjtőrendszerben kell összegyűjteni és tárolni. A különböző naplóállományok összefésülését, feldolgozását és elemzését automatizált megoldásoknak kell támogatniuk.
A naplóban — a kapcsolódó felhasználó azonosítóján túl — személyes adat nem lehet.

7.12.1. Biztonsági események naplózása

7.12.1.1. Biztonsági események naplózása

A kivételes és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni, és azt a hozzáférés nyomon követhetősége érdekében meg kell őrizni. Az elszámoltathatóság és auditálhatóság biztosítása érdekében a regisztrálási és a naplózási rendszert (biztonsági napló) úgy kell kialakítani, hogy abból utólag megállapíthatók legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, meg lehet állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy kísérletét. A biztonsági események naplózását végző megoldás kialakításáért és kezeléséért az Informatikai Osztályvezető (IOV) a felelős.

7.12.1.2. Naplózandó események (3.3.12.2. [2]), {4.2}

A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A következő eseményeket (sikeres/sikertelen) feltétlenül naplózni kell:

- rendszerindítások, -leállítások;
- rendszeróra állítások;
- be- és kijelentkezések; az azonosítási és a hitelesítési mechanizmus használata;
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz;
- azonosítóval ellátott erőforrás létrehozása vagy törlése;
- felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.
- rendszerhibák és korrekciós intézkedések;
- programindítások és -leállások, leállítások;
- a kiemelt jelentőségű adatállományok és kimeneti adatok kezelésének visszaigazolása.

Az elektronikus információs rendszernek lehetővé kell továbbá tennie, hogy a jogosult személyek vagy szerepkörök kiválasszák, mely milyen további naplózható események legyenek naplózva az egyes komponensekre, illetve alrendszerekre.

7.12.1.3. A napló adattartalma (3.3.12.3. [2]3.3.12.3.2 [4]), {4.3}

A biztonsági naplóban az egyes eseményekhez kapcsolódóan a következő adatokat is rögzíteni kell:
a felhasználó azonosítása és hitelesítése esetén:

- dátum;
- időpont;
- a felhasználó azonosítója;
- az eszköz (például terminál) azonosítója, amelyről az azonosítási és hitelesítési művelet kezdeményezése történt;
- a hozzáférési művelet kiemelt jelentőségű jellemzői.

az olyan erőforráson kezdeményezett hozzáférési művelet esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:

- dátum;
- időpont;
- a felhasználó azonosítója;
- az erőforrás azonosítója;
- a hozzáférési kezdeményezés típusa;
- a hozzáférés kiemelt jelentőségű jellemzői.

az olyan erőforrás létrehozása vagy törlése esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:

- dátum;
- időpont;
- a felhasználó azonosítója;
- az erőforrás azonosítója;
- a kezdeményezés típusa;
- a művelet kiemelt jelentőségű jellemzői.

a felhatalmazott felhasználók (például rendszeradminisztrátorok) olyan műveletei esetén, amelyek a rendszer biztonságát érintik:

- dátum;
- időpont;
- a műveletet végző azonosítója;
- az erőforrás azonosítója, amelyre a művelet vonatkozik;
- a művelet kiemelt jelentőségű jellemzői.

7.12.1.4. Alapvető naplózási követelmények

Kerüljön naplózásra a biztonságot érintő összes, kiemelt jelentőségű tevékenység.
A naplóállományokat tilos megsemmisíteni, felülírni, módosítani, azokat archiválni kell.
A fokozott és kiemelt biztonsági osztályba sorolt rendszerek biztonsági naplóit egy másik számítógépen is tárolni kell (annak érdekében, hogy védve legyenek a törlés és illetéktelen hozzáférés ellen). Ennek megvalósításáért az Informatikai Osztályvezető (IOV) felelős.
Rögzíteni kell a hibás bejelentkezési kísérletek kiemelt jelentőségű jellemzőt.
A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni és archiválni kell.
A biztonsági eseménynapló fájlok vizsgálatához és karbantartásához a rendszernek megfelelő eszközökkel és ezek dokumentációjával kell rendelkeznie. Ezen eszközök állapotának regisztrálhatónak és dokumentálhatónak kell lennie.
A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.
A biztonsági naplót a létrehozástól folyamatosan karban kell tartani, valamint védeni kell az illetéktelen módosítástól és törléstől, ezért ember számára olvasható formában is el kell tárolni.

7.12.2. Automatikus naplózás (3.3.10.2.5. [BR4])

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

7.12.3. Privilegizált funkciók használatának naplózása (3.3.10.6.5. [4])

Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

7.12.4. Ideiglenes naplózás

Ideiglenes naplózást rendelhet el a naplózandó esemény és a naplózás időtartamának és céljának pontos megjelölésével, írásban:

- az Informatikai Osztályvezető (IOV);
- az Információbiztonsági felelős (IBF).

7.12.5. A rendszer használat megfigyelése

A felhasználók által elvégzett tevékenységeket — az ellenőrizhetőség érdekében — rögzíteni, naplózni kell.
Az informatikai rendszer üzemeltetéséről (a biztonsági napló mellett) üzemeltetési naplót kell vezetni, amelyet az Informatikai Osztályvezető (IOV) által megbízott informatikusnak rendszeresen ellenőriznie kell.
Az informatikai rendszer üzemeltetéséről nyilvántartást (adatkérés, szolgáltatás, feldolgozás stb.) kell vezetni, amelyet az arra illetékes személynek rendszeresen ellenőriznie kell.
Az eseménynaplózási adatokat folyamatosan kell archiválni és karbantartani.
A rendszereseményeket automatikusan kell archiválni, a naplóbejegyzéseket (eseményrekordokat) folyamatosan felül kell vizsgálni, a rendszernek alkalmasnak kell lennie a biztonsági események automatikus detektálására.
A rendszereseményeket automatikusan kell archiválni, a naplóbejegyzéseket (eseményrekordokat) folyamatosan felül kell vizsgálni, a rendszernek lehetőleg alkalmasnak kell lennie a biztonsági események automatikus detektálására.

7.12.6. Kockázati tényezők

A naplózási és ellenőrzési tevékenységek eredményeit rendszeresen felül kell vizsgálni. A felülvizsgálat gyakoriságának az érintett kockázattól kell függenie. A figyelembe veendő kockázati tényezők a következők:

- az alkalmazási folyamatok kritikussága;
- az érintett információ értéke, érzékenysége és kritikussága;
- a rendszerbe való beszivárgásról és a rendszerrel való visszaélésről szóló korábbi tapasztalatok;
- a rendszerkapcsolatok kiterjedtsége (különös tekintettel a nyilvános hálózatokra).

7.12.7. Naplózási információk védelme (3.3.12.9. [2]), {4.25}

Különös figyelmet kell fordítani a naplózó eszközök biztonságára, mert ha meghamisítják, hamis biztonságérzetet kelthetnek. Óvintézkedéseket kell alkalmazni azért, hogy az Intézet meg legyen védve az olyan illetéktelen változtatásoktól és üzemeltetési problémáktól, mint:

- naplózási rendszer, amelyet kiiktattak;

- üzenetfajták, amelyeket rögzítés után módosítottak;
- naplófájlok, amelyeket átszerkesztettek vagy töröltek;
- naplófájlok adathordozói, amelyek kimerültek és ennek következtében vagy nem lehet már velük az eseményekről feljegyzést készíteni, vagy önmagukat írják felül.

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, annak érdekében, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatók legyenek. A naplóinformációk védelme érdekében a következőket kell betartani:

- A naplóban rögzített információkat megváltoztatni, törölni tilos.
- A naplók tartalmának megváltoztatásának megakadályozása érekében lehetőség szerint kriptográfiai mechanizmusokat kell alkalmazni.
- A napló mentéseket, archív állományokat elkülönítetten, elzárva vagy hozzáférhetetlenül kell tartani.

7.12.8. Naplóinformációk figyelése, reagálás a napló információkra (3.3.12.6. [3]), {4.13}

Folyamatosan figyelemmel kell kísérni a naplóállományok bejegyzései alapján generált riasztásokat. Informatikai biztonsági esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén automatikusan információbiztonsági eseménykezelési eljárást kell indítani.

7.12.9. Rendszer órajel szinkronizáció (3.3.12.8. [2]),

Az Intézeten belül, illetve adott biztonsági tartományban működő valamennyi érintett információ-feldolgozó rendszer órajelét szinkronizálni kell egy közösen megállapított pontos időforráshoz. Az órajelek szinkronizációjával kapcsolatos beállításokat jegyzőkönyvezni kell. A jegyzőkönyvben fel kell tüntetni:

- az elvégzett művelet időpontját;
- a beállítást elvégzős munkatárs nevét;
- az elvégzett beállítás leírását.

7.12.10. A naplóbejegyzések megőrzése (3.3.12.11. [2]), {4.38}

Az Intézet a naplóbejegyzéseket meghatározott - a jogszabályi és az Intézeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

7.12.10.1. Naplózás mentése

A naplók tárolását a következő szempontok figyelembevételével kell megoldani:

- A naplóadatoknak sértetlenül rendelkezésre kell állniuk az esetleges elévülési időn belül.
- Biztosítani kell, hogy az adatokban keletkezésük után változtatást már ne lehessen végrehajtani.
- Az információk bizalmasságára tekintettel, az adatok nem juthatnak illetéktelenek kezébe.

Az általános alkalmazás naplókat minimálisan 1 évig meg kell őrizni, kivéve, ha kapcsolódó jogszabály vagy belső szabályozó ennél hosszabb megőrzési időt határoz meg.
A biztonsági (security) naplóbejegyzéseket a biztonsági események utólagos kivizsgálásának biztosítása érdekében — amennyiben a jogszabályi követelmények másképp nem rendelkeznek — legalább a következő időtartamig meg kell őrizni:

- kritikus rendszerek esetén 5 év;
- szerver operációs rendszerek esetén 3 év;
- végponti operációs rendszerek esetén 1 év;
- biztonsági alkalmazások esetén 2 év;
- vagyonvédelmi rendszerek esetén 3 év;
- ügyviteli rendszerek esetén 2 év;
- IPS-es, IDS-ek esetén 2 év;
- hálózati eszközök esetén 2 év;
- minden egyéb rendszer esetén 2 év.

7.12.10.2. Naplóállomány külön mentése

Abban az esetben, ha a naplóállomány külön, az egyes adatbázisoktól elkülönítve kerül mentésre, nyilvántartást kell vezetni, hogy az egyes naplómentések, mely adattárolókon helyezkednek el. A nyilvántartásban fel kell tüntetni:

- a mentési eszköz azonosítóját;
- a mentési eszköz tárolási helyét;
- a mentés időpontját;
- a mentett naplóállomány nevét.

7.12.10.3. Naplóállományok rendszeres mentéseinek felülvizsgálata

Gondoskodni kell a naplóállományok rendszeres mentéseinek felülvizsgálatáról. A naplóállományok mentéseinek felülvizsgálatáról jegyzőkönyvet kell készíteni, amelynek tartalmaznia kell az alábbi információkat:

- az elvégzett felülvizsgálat időpontja;
- a felülvizsgálatot elvégző munkatárs neve;
- az elvégzett felülvizsgálat mely naplóállományokra terjedt ki;
- a felülvizsgálat megállapításai;
- javaslat a felmerült problémák kezelésére.

7.12.10.4. Biztonsági naplók archiválása

A biztonsági naplókat archiválni kell, mint a rendszerhasználat bizonyítékait, hogy ezek az információk (bizonyítékok) későbbi vizsgálatokhoz is felhasználhatóak legyenek.
A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal kell archiválni. Az archiválásról papíralapú vagy elektronikus jegyzőkönyvet kell készíteni. Az archiválási jegyzőkönyvben a következő adatokat kell rögzíteni:

- az archiválás időpontja;
- az archiválást elvégző munkatárs neve;
- az archív állomány elérhetősége;
- az archivált állomány neve;
- az archiválás során alkalmazott szűrési feltételek.

A biztonsági naplók archiválásáról felvett jegyzőkönyveket meg kell őrizni. A biztonsági naplók archiválásáról készített jegyzőkönyvek megőrzési ideje 5 év.

7.12.11. Hozzáférés a naplóállományokhoz (3.3.12.9.2. [4])

7.12.11.1. Naplóállományok írása

A biztonsági eseménynapló (naplófájl) és a jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől.

A naplóállományokhoz írási jogosultsággal az automatikus rendszerek férhetnek hozzá a naplóállományokból. Amennyiben rendelkezésre áll, a központi naplógyűjtőben a kockázatelemzés alapján meghatározott elévülési időig a törlés nem engedélyezett.

7.12.11.2. Lekérdezés a naplóállományokból

Az egyes naplóállományokhoz, vagy azok részeihez olvasási jogosultsággal rendelkezhet (amennyiben munkaköre, feladata ellátásához arra szüksége van):

- a főigazgató (FOIG);
- Főigazgatói Hivatal vezetője;
- az Informatikai Osztályvezető (IOV);
- az Információbiztonsági felelős (IBF),
- az Informatikai Biztonsági Megbízott (IBM),
- az IT infrastruktúra fejlesztésért és üzemeltetésért felelős személy (IÜFSZ).

A fenti felsorolásban nem szereplő munkatársak a naplóállományokat csak az IBF, a Főigazgatói Hivatal vezetője,, vagy az Informatikai Osztályvezető (IOV) által kiadott engedély birtokában tekinthetik meg.

7.12.11.3. Naplóinformációk kiadása külső Intézetek számára

Külső fél részére hatósági, ellenőrzési, hibakeresési okokból a naplófájlokról — szükség esetén személyazonosításra alkalmas adattartalomtól megfosztott — másolat adható ki.

7.12.11.4. Naplóállományból lekérdezési jogosultság dokumentálása

A lekérdezési jogosultságokról naprakész nyilvántartást kell vezetni. A nyilvántartásnak az alábbi adatokat kell tartalmaznia:

- lekérdezési jogosultságot igénylő neve;
- lekérdezési jogosultság kérésének indoka;
- mely naplóállományokra terjed ki a lekérdezési jogosultság kérés;
- a lekérdezési jogosultság időszak;
- a kérelem időpontja;
- az engedélyező neve;
- az engedély megadásának időpontja;
- a lekérdezési jogosultság beállításának időpontja;
- a lekérdezési jogosultság visszavonás beállítás időpontja.

7.12.12. Naplózó rendszer beállításainak módosítása

A naplózó rendszer beállításainak megváltoztatást az erre vonatkozó egy alkalomra szóló engedély birtokában lehet csak elvégezni, melyet az Intézet jogosultság kezelési folyamata szerint kell kérvényezni és kiadni. A naplózó rendszer módosításáról jegyzőkönyvet kell készíteni (vagy a

konfiguráció kezelő rendszerben hitelt érdemlően rögzíteni), amelynek a következő adatokat kell tartalmaznia:

- a módosítást engedélyező neve;
- a módosítás indoka;
- a módosítás engedély megadásának időpontja;
- az elvégzett beállítás módosítás időpontja;
- a módosítást elvégző munkatárs neve;
- az elvégzett módosítás leírásai.

7.12.13. Naplózási beállításokról nyilvántartás vezetése

Az egyes rendszerek naplózási beállításairól naprakész nyilvántartást kell vezetni, amelyet minden változtatást követően haladéktalanul aktualizálni kell.

7.12.14. Hozzáférés korlátozása (3.3.12.9.2. [4])

A naplófunkciók kezelésére csak az Intézet által meghatározott, privilegizált felhasználók jogosultak.

7.12.15. Naplózás ellenőrzése (3.3.12.2.2. [5])

7.12.15.1. Naplózandó események, naplóban rögzítendő adatok körének felülvizsgálata

A naplózandó események és a naplóban rögzítendő adatok körének áttekintése része az IBSZ rendszeres felülvizsgálatának.

7.12.15.2. Kiegészítő információk (3.3.12.3.2. [4])

Szükség esetén az elektronikus információs rendszer a naplóbejegyzésekben további, az Intézet által meghatározott kiegészítő, részletesebb információkat is rögzít.

7.12.15.3. Naplózási beállítások felülvizsgálata

Az elektronikus információs rendszerek esetén évente ellenőrizni kell, hogy az egyes rendszerek tényleges naplózási beállításai megfelelnek-e a nyilvántartott naplózási beállításoknak.
A naplózási beállítások ellenőrzéséről Jegyzőkönyvet kell készíteni, amelynek a következő adatokat kell tartalmaznia:

- az elvégzett ellenőrzés időpontja;
- az ellenőrzést elvégző munkatárs neve;
- az elvégzett ellenőrzés mely rendszerekre terjedt ki;
- az elvégzett ellenőrzés tárgya;
- az ellenőrzés megállapításai;
- javaslat a felmerült problémák kezelésére.

Abban az esetben, ha a rendszerben a tényleges naplózás beállítása eltér az adott rendszer nyilvántartott naplózási beállításától ezt haladéktalanul jelenteni kell az IBF-nek.

7.12.15.4. A naplózás vizsgálata

A naplózást és a naplók folyamatos figyelemmel kísérésének megvalósulását rendszeresen ellenőrizni kell. Az ellenőrzés gyakoriságának az érintett kockázattól kell függenie. A figyelembe veendő kockázati tényezők a következők:

- az alkalmazási folyamatok kritikussága;

- az érintett információ értéke, érzékenysége és kritikussága;
- a rendszerbe való beszivárgásról és a rendszerrel való visszaélésről szóló korábbi tapasztalatok;
- a rendszerkapcsolatok kiterjedtsége (különös tekintettel a nyilvános hálózatokra).

A naplózás ellenőrzéséről jegyzőkönyvet kell készíteni, amelynek tartalmaznia kell a következő adatokat:

- az elvégzett ellenőrzés időpontja;
- az ellenőrzést elvégző munkatárs neve;
- az elvégzett ellenőrzés mely rendszerekre terjedt ki;
- az elvégzett ellenőrzés tárgya;
- az ellenőrzés megállapításai;
- javaslat a felmerült problémák kezelésére.

Naplózási hiba bekövetkeztekor, vagy ennek alapos gyanúja esetén automatikusan információbiztonsági eseménykezelési eljárást kell indítani.
Abban az esetben, ha megállapítást nyer, hogy a naplók figyelése, illetve a naplók riasztásaira alapuló reagálások nem megfelelőek, haladéktalanul jelenteni kell az IBF-nek.

7.12.15.5. Naplózási hiba kezelése (3.3.12.5. [3]), {4.7}

Az elektronikus információs rendszernek naplózási hiba esetén riasztást kell küldenie a felügyeletre kijelölt személyeknek vagy szerepköröknek és a rendszer kialakításától és a hibák ismétlődésétől, jellegétől függően elvégzi a rendszer leállítását vagy az automatikus hibajavítást. Az elektronikus információs rendszer naplózás nélkül nem hajthat végre olyan műveleteket, amelyek naplózása elő van írva.

7.12.15.6. Napló tárkapacitás figyelése (3.3.12.5.2. [5])

Az Intézet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével, továbbá folyamatosan figyelemmel kell kísérni, hogy a naplóállományok számára rendelkezésre áll-e a szükséges tárkapacitás. Abban az esetben, ha a teljes kapacitás 10%-a alá csökken a rendelkezésre álló tárkapacitás, haladéktalanul gondoskodni kell a megfelelő tárkapacitás rendelkezésre állásáról.

7.12.16. Folyamatba illesztés (3.3.12.6.2. [4])

Az Intézet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes, vagy tiltott tevékenységekre és történésekre reagál.

7.12.16.1. Időbélyegek (3.3.12.8. [2]), {4.24}

Az Intézet elektronikus információs rendszereinek belső rendszerórákat kell használniuk a naplóbejegyzések időbélyegeinek előállításához. Az időbélyegeket a naplóbejegyzésekben a koordinált világidőhöz (UTC), vagy a Greenwichi középidőhöz (GMT) rendelhető módon kell rögzíteni.

7.12.16.2. Szinkronizálás (3.3.12.8.2. [4])

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

7.12.16.3. Összegzés (3.3.12.6.3. [4])

Biztonsági incidens esetén az érintett eseményre vonatkozóan az Intézet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett Intézetre kiterjedő helyzetfelmérés érdekében.

7.12.17. A naplók tartalmának elemzése, jelentéskészítés a naplózásról (3.3.12.6. [3]), {4.13}

Rendszeres időközönként elemezni kell a naplóbejegyzéseket. Az elemzésről rendszeresen jelentést kell készíteni. A jelentében rögzíteni kell, hogy:

- az egyes rendszerek naplózási funkciói és beállítása mennyiben biztosítják a naplózással szembeni elvárások teljesülését;
- milyen főbb tendenciák állapíthatók meg az egyes rendszerekben előforduló eseményekből;
- milyen rendszerfejlesztési, illetve beállítási változtatásokat kell végrehajtani az egyes rendszerekben ahhoz, hogy a naplózás hatékonyabb, áttekinthetőbb legyen.

7.12.17.1. Automatikus feldolgozás (3.3.12.7.2. [4], 3.3.12.7. [4])

Az elektronikus információs rendszer biztosítja, hogy

- a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni;
- lehetőség legyen naplócsökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő napló-áttekintési, naplóvizsgálati és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;
- a feldolgozás nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

7.13. Rendszer és kommunikációvédelem (3.3.13., 3.3.13.1. [2])

7.13.1. A határok védelme (3.3.13.6. [2], 3.3.13.6.2. [4], (3.3.13.5. [3]), {17.17}

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt:

- a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső Intézet hálózattól;
- csak az Intézet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez;
- az Intézet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát a működéshez szükséges minimumra;
- az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat;
- véd a túlterheléses (úgynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

7.13.1.1. Az adatátvitel sértetlensége (3.3.13.8. [4])

Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.

7.13.1.2. A hálózati kapcsolat megszakítása (3.3.13.9. [4])

Az elektronikus információs rendszer megszakítja a hálózati kapcsolatot egy munkaszakaszra épülő kétirányú adatcsere befejezésekor, 15 perc inaktivitás után, amennyiben azt az adott rendszer technikailag lehetővé teszi.

7.13.1.3. Biztonságos név/cím feloldó szolgáltatások (úgynevezett hiteles forrás) (3.3.13.16 [3]), {17.69}

Az elektronikus információs rendszer a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó kiegészítő adatokat is biztosít, és ha egy elosztott, hierarchikus névtár részeként működik, akkor jelzi az utódtartományok biztonsági állapotát is, és (ha azok támogatják a biztonságos feloldási szolgáltatásokat) hitelesíti az utód- és elődtartományok közötti bizalmi láncot.

7.13.1.4. Biztonságos név/cím feloldó szolgáltatás (úgynevezett rekurzív vagy gyorsító tárat használó feloldás) (3.3.13.17 [3]), {17.71}

Az elektronikus információs rendszer eredethitelesítést és adatsértetlenség ellenőrzést kér és hajt végre a hiteles forrásból származó név/cím feloldó válaszokra.

7.13.1.5. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén (3.3.13.18 [3]), {17.72}

Azok az elektronikus információs rendszerek, amelyek együttesen biztosítanak név/cím feloldási szolgáltatást az Intézet számára, hibatűrők és belső/külső szerepkör szétválasztást valósítanak meg.

7.13.2 A hálózati szintű hozzáférések menedzsmentje

Az Intézet informatikai rendszerének elemeit adminisztrációs célból az internet felől elérni csak titkosított kapcsolaton keresztül (VPN) megengedett. Az ilyen kapcsolat kiépítésére az Informatikai Osztályvezető (IOV) adhat engedélyt. Minden adminisztrációs tevékenységnek egyértelműen személyhez köthetőnek kell lennie.

7.13.2.1. Kötelező elérési útvonal

Külső hálózatról az informatikai rendszerek csak az erre a célra dedikált védelmi rendszeren (tűzfal, zónák VPN koncentrátor stb.) keresztül lehetnek elérhetőek.

7.13.2.2. Hálózati részek elválasztása

Az internet és az Intézet rendszerei között határvédelmi eszköznek kell biztosítani az elválasztást.

7.13.2.3. Hálózati eszközök, munkaállomások azonosítása és hitelesítése

A távoli rendszerekhez történő automatikus csatlakozás lehetősége egy intézeti alkalmazáshoz való illetéktelen hozzáférést tehet lehetővé, ezért az informatikai rendszerekhez távolról való összes csatlakozást azonosítani és hitelesíteni kell. Ez különösen fontos akkor, ha a csatlakozás egy olyan hálózatot használ, amely kívül esik az Intézet biztonsági rendszerének hatókörén. Technikailag biztosítani kell, hogy csak a központilag nyilvántartott munkaállomásról lehessen a rendszerekbe belépni.

Egységes munkaállomás névhasználatot kell kialakítani, a hálózatban lévő munkaállomások pontos azonosítása érdekében.

7.13.2.4. A hálózatra történő csatlakozás ellenőrzése

Az osztott hálózati munka, különösen a több szervezet által használt hálózat biztonsága szükségessé teszi bizonyos ellenőrző eszközök alkalmazását a felhasználók csatlakozási lehetőségeinek korlátozására. (Ezeket a forgalomszűrő, ellenőrző lehetőségeket, amennyiben szükséges, a gateway és operációs rendszer beállításánál alkalmazni kell.) A korlátozásokat az Informatikai Osztályvezető (IOV) határozza meg. Az alábbi esetekben különösen fontos a korlátozások alkalmazása:

- Elektronikus levelezés.
- Egyirányú adatállomány mozgatás (például mentési rendszerek esetében).
- Adatállomány mozgatása mindkét irányban.
- Meghatározott időponthoz kötött hálózati hozzáférés.
- Az Intézet információs biztonságára kockázatot jelentő szolgáltatásokhoz, rendszerekhez való kapcsolódás.

7.13.2.5. A hálózati útvonal kiválasztások ellenőrzése

Az Intézeten túl terjedő hálózatoknál - ahol megoldható -, javasolt az útvonal-kiválasztást ellenőrző és vezérlőeszközök, módszerek alkalmazása, ahol:

- a rendszerdokumentációban, ha erre lehetőség van, meg kell adni az elérni kívánt eszközök címét, portszámát és egyéb, a biztonsági szűréshez szükséges adatait;
- az útvonalak kialakításáért felelős személyt ki kell jelölni, a feladatot munkaköri leírásában szerepeltetni kell;
- a beállításokat minden esetben tesztelni és jegyzőkönyvezni kell.

7.13.2.6. Használható hálózati protokollok

Az Intézet számítógép hálózata és külső hálózatok közötti kapcsolat során az engedélyezett protokollok továbbíthatók, minden egyéb protokoll továbbítása tilos. Az Intézet számítógéphálózatában alkalmazható külső kommunikációs protokollok köréről — az IBF véleményének figyelembevételével — az Informatikai Osztályvezető (IOV) dönt.

7.13.2.7. Távoli készülékek csatornahasználata (3.3.13.6.5. [41, 3.3.13.7.1. [4])

A távoli rendszerkapcsolatok kialakítása során úgy kell eljárni, hogy a távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel, azaz olyan határvédelmi megoldást kell alkalmazni, amely nem teszi lehetővé a távolról kapcsolódó eszköz számára a saját és az Intézet hálózatának összekapcsolását.

7.13.3. Mobilkód korlátozása (3.3.13.14. [4])

Az Intézet meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat, használati korlátozásokat vezet be, vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra.
Az Intézet engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

7.13.4. Mobil informatikai tevékenység, távmunka (3.3.10.13. [3])

A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie ennek a speciális munkavégzésnek a kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. A mobil számítástechnikai eszközökön az Informatikai Osztályvezetőnek (IOV) gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén az Intézet érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely és eszköz védelméről.

7.13.4.1. Mobil informatikai tevékenység (3.3.10.15. [3])

A mobil eszközök (laptopok, notebook-ok, otthoni munkaállomások, tabletek, mobil telefonok) használóinak mind a fizikai biztonság, mind a logikai védelem területén a jelen IBSZ-ben foglaltakat kell figyelembe venniük. Ezek közül a legfontosabbak:

- A távmunka során is be kell tartani az Intézet szabályzataiban foglaltakat.
- A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
- Ki kell alakítani a mobil informatikai eszközök megfelelő fizikai védelmét.
- A kommunikációhoz védett csatornáról kell gondoskodni.
- Vírus- és behatolás védelmi eszközöket kell biztosítani a mobil eszközökre.
- A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell fordítani.
- A távoli elérésre vonatkozó szabályokat kell alkalmazni.
- A mobil számítástechnikai berendezéseket nyilvános helyeken használóknak ügyelni kell arra, hogy elkerüljék a jogosulatlan személyek általi betekintés kockázatát.
- Kényes üzemeltetési információkat hordozó eszközt nem szabad felügyelet nélkül hagyni, és ha lehetséges, fizikailag el kell zárni vagy különleges zárat kell alkalmazni a berendezés biztosítására.
- A felhasználók részére oktatást kell tartani, hogy növeljék a biztonsági tudatosságot az ilyen jellegű munkavégzésből származó többletkockázattal szemben és a bevezetendő intézkedések elfogadtatásával kapcsolatban.
- A hordozható informatikai eszközök gazdája felelős az eszköz teljes biztonságáért és annak ellenőrzéséért. Ha az eszközt egy csoport használja, ugyanúgy szükséges a biztonsági átvilágítás és a szükséges tudás elve (need-to-know). Ilyen esetekben a csoport egyik tagját kell kijelölni, aki felelős az eszköz biztonságáért.
- Az Intézetnek folyamatosan frissített listát kell tárolnia a rendszerben definiált, jogokkal felruházott felhasználókról.
- Szükséges a kiváltságos account-ok használata. (Pl. rendszer, biztonsági adminisztrátor.) Az összes, jogosultsággal rendelkező felhasználó biztonsági beállításait, egyedileg kell karbantartani.
- A kiváltságos (magas jogosultságokat biztosító, pl. rendszergazdai —) account-ok jelszavait védetten (pl. lepecsételt borítékban) meg kell őrizni erre alkalmas biztonsági konténerben, hogy vészhelyzet esetén is biztosított legyen a rendszerhozzáférés.

- Használaton kívül, a hitelesítési tokent az eszköztől elkülönítve kell tárolni.
- Az IBF-nek és a rendszergazdának meg kell határozniuk azokat a rendszer eseményeket, ahol a felhasználóknak újra kell azonosítania magát.
- A rendszer csak limitált visszacsatolási információt szolgáltathat a felhasználónak a hitelesítési eljárás alatt, így megakadályozza a felhasználót abban, hogy ismerteket szerezzen a hitelesítési folyamatról.
- Lehetővé kell tenni az interaktív kapcsolatok zárolását. Egy előre meghatározott felhasználót egy meghatározott inaktivitás után felül kell írni, vagy törölni kell a kijelzőeszközöket (képernyőket). Az aktuális képernyőtartalmat olvashatatlanná kell tenni, le kell tiltani minden felhasználói tevékenységet, a hozzáférést / kijelzőket és zárolni kell a munkameneteket.
- Meg kell engedni, hogy a felhasználó zárolhassa saját interaktív kapcsolatait (alkalmazásait, munkameneteit), felül kell írnia, vagy törölnie kell a kijelző eszközöket (képernyőket), az aktuális képernyőtartalmat olvashatatlanná kell tennie, le kell tiltania minden felhasználói tevékenységet, a hozzáférést / kijelzőket és zárolnia kell a munkameneteket.
- Amikor az adathordozó a mobil informatikai eszközzel együtt elhagyja a biztonsági területet, továbbra is védeni kell a hozzáférés-védelmi intézkedésekben megfogalmazott szabályok szerint. Hordozható informatikai eszközre csak ellenőrzött környezetben csatlakoztatható nyomtató.
- A törölt adatok (maradék információ) védelmi mechanizmusának gondoskodnia kell arról, hogy a törölt információ többé már ne legyen vagy (ne túl hosszú ideig) legyen hozzáférhető, és ezekre vonatkozó információkat az újonnan létrehozott objektumok (fájlok) ne tartalmazzanak. Ez a védelem szükséges a logikailag már törölt, de fizikailag még elérhető adatok esetében.

7.13.4.2. A távmunka (3.3.10.13. [3])

Távmunka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.
A távmunkát végző csak a kijelölt csatlakozási pontokon keresztül csatlakozhat az Intézet hálózatához. Az Informatikai Osztályvezető (IOV) határozza meg ezeket a belépési pontokat.

7.13.5. Kriptográfiai eszközök (3.3.13.7.2. [4])

7.13.5.1. Digitális aláírás

Különös gondot kell fordítani a magánkulcs titokban tartására, továbbá ajánlatos a nyilvános kulcs sértetlenségét is megóvni. Ezt a védelmet a nyilvánoskulcs-tanúsítványok alkalmazásával kell ellátni.
A digitális aláíráshoz alkalmazott kriptográfiai kulcsoknak különbözniük kell a titkosításra (rejtjelezésre) alkalmazott kulcsoktól. A digitális aláírások alkalmazásakor figyelembe kell venni minden hatályos jogszabályt, amely azokat a feltételeket írja elő, amelyek mellett a digitális aláírás jogilag érvényes, hatályos (legally binding).
Ügyelni kell a magánkulcs bizalmas kezelésére. A magánkulcs kezelését végző (a kulcsgeneráló eszközöket, alkalmazásokat kezelő) személyek fontos és bizalmas munkakört betöltőnek minősülnek.
Az elektronikus aláírás kulcsa és a rejtjelkulcs nem lehet azonos. Az elektronikus aláírás algoritmusát, valamint az alkalmazható kulcsok hosszát az Informatikai Osztályvezető (IOV) hagyja jóvá.

7.13.5.2. Szolgáltatások a le nem tagadhatóságra

A letagadhatatlanság biztosítására automatikus, a felhasználó által nem befolyásolható rendszerek kialakítására kell törekedni a digitális aláírási technikára alapozva.

7.13.5.3. Nyilvános kulcsú infrastruktúra tanúsítványok (3.3.13.13. [4])

Piaci szolgáltatótól nyilvános kulcsú tanúsítványokat úgy szerezhet be, ha a szolgáltató a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szerepel hitelesítés-szolgáltatóként.

7.13.5.4. Kriptográfiai védelem (3.3.13.11. [2])

Az elektronikus információs rendszer csak szabványos, a Nemzeti Média- és Hírközlési Hatóság által biztonságosnak minősített kriptográfiai műveleteket valósíthat meg.

7.13.5.5. Kriptográfiai vagy egyéb védelem (3.3.13.8.2., 3.3.13.7.2. [4])

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

7.13.5. Kulcsmenedzsment (3.3.13.10. [2])

A kulcsmenedzsmentet kötelező jelleggel ki kell alakítani minden elektronikus aláírással, rejtjelezéssel rendelkező rendszerben. A kulcsmenedzsment kialakítása során a hatályos jogi szabályozást, és a PKI-ra vonatkozó nemzetközi szabályozást kell figyelembe venni.

7.13.6.1. A kriptográfiai kulcsok védelme

A rendszerben használt kriptográfiai kulcsok védelme:

- A kriptográfiai kulcsok fizikai, valamint speciális, illetve fokozott biztonságot igénylő esetben rejtjelezéssel megvalósított logikai védelméről is gondoskodni kell.
- Szükség esetén a kulcs-felek megosztásával kell biztosítani a rejtjelkulcsok védelmét.

A kulcshamisítás kockázatának csökkentése érdekében, előzetesen meg kell határozni a kulcsok aktiválásának és visszavonásának dátumait. A kulcs élettartama függ a vélelmezett kockázat mértékétől.

A nyilvános kulcsokkal való esetleges visszaélések kockázatának csökkentése érdekében, csak hitelesített nyilvános kulcsok használhatók a rendszerben. A kriptográfiai szolgáltatók külső szállítóival, például egy hitelesítő hatósággal kötött, a szolgáltatás mértékét meghatározó megállapodásoknak vagy szerződéseknek szabályozniuk kell a felelősség kérdését.

7.13.7. Folyamatok és maradványinformációk védelme (3.3.13.2. [4], 3.3.13.4. [4], 3.3.13.22. [2], 3.3.13.21. [4])

Az elektronikus információs rendszer:

- elkülöníti a felhasználók által elérhető funkcionalitást (beleértve a felhasználói felület szolgáltatásokat) az elektronikus információs rendszer irányítási funkcionalitásától;
- meggátolja a megosztott rendszererőforrások útján történő jogosulatlan vagy véletlen információáramlást;

- elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára, ahol erre a feldolgozás jellegéből adódóan szükség van;
- biztosítja, hogy az alrendszerei védjék a keletkezett maradvány információkat, azok bizalmasságát és sértetlenségét.

7.13.8. Külső kommunikációs szolgáltatások (3.3.13.6.3. [3], 3.3.13.19. [4])

Az Intézet:

- felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;
- minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;
- védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;
- dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt;
- meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol;
- megvédi a munkaszakaszok hitelességét.

8. Informatikai biztonsági ellenőrzés

Az informatikai biztonság ellenőrzése az informatikai biztonság fenntartása érdekében

- évente belső audit keretében dokumentumok értékeléseként;
- jelentős változás esetén rendkívüli audit keretében dokumentum értékeléseként;
- biztonsági incidenst követő felülvizsgálat hatására haladéktalanul;
- szabályozási környezet módosulása esetén haladéktalanul elvárt.

Törvényi megfelelőségi auditok a jogszabályoknak megfelelően akár külső szakértők segítségével is megvalósíthatók.

9. ZÁRÓ RENDELKEZÉSEK

Az Intézet

- mentési, archiválási rendjét,
- naplózási rendjét,
- azonosítási és hitelesítési eljárásrendjét,
- konfigurációkezelési eljárásrendjét,
- biztonsági incidens kezelési eljárásrendjét,
- kockázatelemzési módszertanát vagy más szabályozási elemét,

külön szabályzatban határozhatja meg. A hatályos eljárásrendeknek az e dokumentumban rögzített tartalmi elemeket kell figyelembe vennie.

10. Az informatikai biztonsági szerepek megfeleltetése (szerepbeosztás mátrix)

A jelen szabályzatban meghatározott informatikai biztonsághoz kapcsolódó szerepek az Intézet esetén az alábbi beosztásoknak kerülnek megfeleltetésre:

Informatikai biztonsági szerep	*Beosztás*	*Helyettes*
Intézet vezetője (FOIG)	főigazgató	SZMSZ szerinti helyettes

Informatikai biztonsági szerep	*Beosztás*	*Helyettes*
Szervezeti egység vezetők / Adatgazdák (SZEV / AG)	osztályvezetők	osztályvezető-helyettesek
Jogi és Humán- gazdálkodási Főosztály vezetője (HSZV)	Jogi és Humán-gazdálkodási főosztályvezető	Humánpolitikai és Munkaügyi Osztály osztályvezető
Főigazgatói Hivatal vezetőjefőigazgatói hivatalvezetőinformációbiztonsági felelősInformatikai Osztályvezető (IOV)	Informatikai Osztály osztályvezető	Informatikai Osztály osztályvezető-helyettes
Információbiztonsági Felelős (IBF)	Információbiztonsági Felelős	a főigazgató által esetileg kijelölt személy
Informatikai Biztonsági Megbízott (IBM)	Informatikai Osztály osztályvezető-helyettes	Informatikai Osztályvezető által esetileg kijelölt személy
IT infrastruktúra fejlesztésért és üzemeltetésért felelős személy (IÜFSZ)	Informatikai Osztályvezető által kijelölt személy	Informatikai Osztályvezető által esetileg kijelölt személy
Alkalmazás fejlesztésért felelős személy (AFFSZ)	Informatikai Osztályvezető által kijelölt személy	Informatikai Osztályvezető által esetileg kijelölt személy
Alkalmazás támogatásáért és üzemeltetéséért felelős személy (ATFSZ)	Informatikai Osztályvezető által kijelölt személy	Informatikai Osztályvezető által esetileg kijelölt személy
Fizikai védelemért felelős személy (FVFSZ)	biztonsági szolgálat vezetője	biztonsági szolgálat vezetője által kijelölt személy

12. táblázat — Informatikai biztonsági szerepek

12. Mellékletek

Nincsenek.

13. Kapcsolódó formanyomtatványok, feljegyzések

Nincsenek.