BONYHÁDI KÓRHÁZ ÉS
RENDELŐINTÉZET

BONYHÁDI KÓRHÁZ ÉS RENDELEŐINTÉZET

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

KÉSZÍTETTE:	HAJDU SÁNDOR IBF	DÁTUM
		2025.09.22.
JÓVÁHAGYTA:		DÁTUM
	DR. BARCZA ZSOLT FŐIGAZGATÓ	2025.09.22.
MINŐSÉGÜGYI SZEMPONTBÓL ELLENŐRIZTE:	LAUFER ÉVA ÁPOLÁSI IGAZGATÓ	DÁTUM
	MINŐSÉGÜGYI VEZETŐ	2025.09.22.

A dokumentum kódja:	**SZAB-IG-12**	**Mellékletek száma:**	**0**
Kiadás száma:	**BKR-IKT/193-1/2025.**	**Adatlapok száma:**	**0**
Fájlnév: Információztonsági_szabályzat_BKR_V1.0.0.docx	**-**	**Érvénybelépés időpontja:**	**2025.09.22.**

EZT A DOKUMENTUMOT FÉNYMÁSOLNI ÉS NYOMTATNI CSAK ENGEDÉLLYEL LEHETSÉGES!

A példány sorszáma:	**A példány tulajdonosa: Bonyhádi Kórház és Rendelőintézeti**
Nyilvántartott példány:	**Munkapéldány:**

A Szabályzat a **Bonyhádi Kórház és Rendelőintézet** szellemi tulajdona.
Továbbadása, sokszorosítása engedélyhez kötött.

Tartalomjegyzék

1. Az Információbiztonsági Szabályzat

Az elektronikus biztonságáról szóló 2024. évi LXIX. törvény Magyarország kiberbiztonságárólés a 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről alapján a(z) Bonyhádi Kórház és rendeleőintézet (továbbiakban: Szervezet) Információbiztonsági Szabályzatát az alábbiakban határozza meg:

a) meghatározza a célokat, a Szabályzat tárgyi és személyi (a Szervezet jellegétől függően területi) hatályát,

b) az elektronikus információbiztonsággal kapcsolatos szerepköröket,

c) a szerepkörökhöz rendelt tevékenységeket,

d) a tevékenységekhez kapcsolódó felelősségeket,

e) az információbiztonság Szervezetrendszerének belső együttműködését.

Területi hatálya:

Bonyhádi Kórház és rendeleőintézet

1.1 A dokumentum célja

Az Információbiztonsági Szabályzat (a továbbiakban IBSZ, vagy Szabályzat) azon alapvető biztonsági normákat és működési kereteket határozza meg, melyek érvényesítésével a Szervezet elfogadható szintre csökkentheti az általa végzett adatkezelés és adatfeldolgozás kockázatait, egyúttal hozzájárulnak a vonatkozó jogszabályokban előírt követelmények teljesítéséhez. A Szabályzat rögzíti a hatálya alá eső adatok, információk informatikai rendszeren történő adatfeldolgozásával szemben támasztott alapvető biztonsági követelményeket valamint a legfontosabb Szervezeti feladatokat és felelősségi köröket.

A Szabályzat további célja, hogy iránymutatással szolgáljon a Szervezet informatikai rendszereihez hozzáférési jogosultsággal rendelkező felhasználók számára az informatikai rendszerek helyes használatáról, ismertesse a helyes és biztonságos munkavégzés szabályait, a követendő eljárásokat, továbbá rögzítse a felhasználókkal szemben támasztott elvárásokat és követelményeket. Meghatározza a Szervezet részére az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatokat.

A Szervezetben üzemelő számítástechnikai infrastruktúra hátteret teremt a Szervezetben folyó munkavégzéshez, de mindez csak az informatikai eszközök biztonságos, szabályozott működése mellett válik valóságos előnnyé.

Az információk, illetve adatok rendelkezésre állását, elérhetőségét az arra jogosult felhasználók számára különösen az alábbi feltételek biztosításával kell lehetővé tenni:

- a feladat ellátásához szükséges és elégséges jogkörök,
- az információk, illetve adatok sértetlensége (sérthetetlensége, valódisága),
- az információknak, illetve adatoknak jellegüktől függő bizalmas kezelése,
- az információk és adatok hitelessége, valamint a teljes informatikai, illetve információs rendszer működőképessége.

A Szabályzat célja továbbá, hogy az informatika alkalmazása során biztosítsa a Szervezetben az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, informatikai eszközök valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- munkaállomásokon lekérdezhető adatok körének meghatározását,
- adatállományok biztonsági mentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

Az Információbiztonsági Szabályzat a fenti célok teljesülése érdekében rögzíti a Szervezet elvárt biztonsági szintjének és az általa használt EIR-ek biztonsági osztályba sorolásának megfelelő adminisztratív, fizikai és logikai védelmi intézkedésekkel kapcsolatos követelmények teljesítésével összefüggő folyamatokat, eljárásokat, feladatokat és felelősségeket. A Szervezet vezetőjének célja és feladata, hogy minimalizálja a kliens (felhasználó) oldali kockázatokat.

1.2 A dokumentum hatálya

A Szabályzat **tárgyi hatálya** kiterjed a Szervezet minden informatikai rendszerére, teljes informatikai környezetére, beleértve minden olyan adathordozót és informatikai eszközt, amin a Szervezet adatait tárolják, feldolgozzák, vagy ügyviteli folyamatait támogatják, illetve az azok létrehozásával, működtetésével, használatával kapcsolatos tevékenységekre. Így

- a védelmet élvező elektronikus adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és fizikai megjelenési formájuktól függetlenül;
- a Szervezet tulajdonában, vagy más módon használatában lévő eszközre;
- a fenti eszközök, műszaki dokumentációira;
- az információs rendszerek fejlesztési, szervezési, programozási, üzemeltetési dokumentációira;
- a rendszer és felhasználói programokra;
- és minezek védelmét szolgáló (beleértve e dokumentumot is) gyakorlati ismeretekre és vagy ezek dokumentgációira.

A tárgyi hatály ezenfelül kiterjed minden olyan épületre, helyiségre, ahol a tárgyi hatály alá eső eszközök megtalálhatók, illetve a tárgyi hatálya alá tartozó tevékenységeket végeznek. Így a Szervezet tevékenysége során keletkezett, kezelt, feldolgozott, tárolt

adatokra és információkra, a számítástechnikai eszközbázisra, ezek okmányaira, leírására és felhasználási környezetükre, a szoftverekre, adatbázisokra és a kapcsolódó dokumentációkra, az adatbiztonsági nyilvántartásokra.

A Szabályzat **személyi hatálya** kiterjed valamennyi, a feladatai ellátásához a Szervezet informatikai rendszereit, eszközeit használó, vagy azokhoz hozzáférő felhasználóra, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Szervezetben megbízási, vagy egyéb jogviszony vagy vállalkozói szerződés alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen felhasználó). Ha a Szervezet más személyek (pl: alvállalkozók) is lehetőséget biztosít bármely informatikai rendszerének használatára, akkor rá nézve is kötelező a Szabályzatban foglaltak betartása.

A Szabályzat **időbeli hatálya** szerint a kiadás napján lép hatályba és jelenlegi verziója visszavonásig – vagy a következő kiadásra kerülő verzió hatályba lépéséig – hatályos. Felülvizsgálatát bármely jelentős Szervezeti vagy rendszerelem változása esetén el kell végezni, de legalább a jogszabályban meghatározott időközönként.

Jelen Szabályzatban foglalt elvárások és követelmények a Szervezet vezetőjének jóváhagyásával kerültek kialakításra. Azon biztonsági területek esetében, melyeket jelen Szabályzat nem fed le, vagy részletesen nem szabályoz, a Szervezet vezetője határozza meg a követendő eljárásrendet és az alkalmazandó biztonsági elvárásokat, melyek meghatározásához szükség esetén bevonja az elektronikus információs rendszerek biztonságáért felelős személyt.

E Szabályzatban foglaltak be nem tartása, tartatása a PTk-ban leírt szabálysértés és amely a fenti dokumentumokban megfogalmazott következményeket (eljárást) vonja maga után.

1.3 A dokumentum minősítése, kötelezettségek

Az IBSZ bizalmas minősítésű, korlátozott körben terjeszthető dokumentum. A Szabályzathoz hozzáférési jogosultsággal a Szabályzat személyi hatálya alá tartozók, továbbá a Szervezet vezetője által feljogosított személyek rendelkezhetnek.

A Szervezet vezetőjének felelőssége a Szabályzat napra készen tartása, így a Szervezet vezetőjének feladata biztosítani, hogy szükség szerint, a Szabályzatot érintő jogszabályi, funkcionális, biztonsági, technológiai vagy egyéb változások esetén a Szabályzat felülvizsgálata megtörténjen.

1.4 A dokumentum kiadása, kezelése, felülvizsgálata

A Szervezet vezetőjének feladata és felelőssége az IBSZ kiadása, Szervezeten belüli kihirdetése és rendelkezésre állásának biztosítása (megőrzése).

Az IBSZ személyi hatálya alá tartozók munka- illetve feladatkörüknek megfelelő mértékben kötelesek az IBSZ tartalmát, a benne foglalt előírásokat, különösen a számukra meghatározott feladatokat és felelősségeket megismerni, s ezek tudomásul vételéről nyilatkozatot tenni (*Megismerési nyilatkozat*).

Az IBSZ felülvizsgálatát és frissítését a következő gyakorisággal kell elvégezni:

- események hiányában 2 év;
- információbiztonsággal kapcsolatos jogszabályi változásokat követően;
- az érintett Szervezetben, illetve a szerepkörökben történő jelentős változás esetén;

- új elektronikus információs rendszer bevezetését, használatba vételét megelőzően, illetve
- a védelmi intézkedésekben bekövetkezett jelentős technológiai változásokat követően.

Az IBSZ felülvizsgálatára javaslatot tehet az információbiztonsági felelős. Az IBSZ felülvizsgálatát az információbiztonsági felelős köteles végrehajtani és eredményét dokumentáltan átadni a Szervezet vezetőjének.

1.5 Alapfogalmak

adatközponti szolgáltatás: olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is,

behatolásvizsgálat: az információs és kommunikációs technológia (a továbbiakban: IKT) rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárása és kihasználhatóságának ellenőrzése a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával,

belső Információbiztonsági vizsgálat: olyan biztonsági vizsgálati eljárás, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik,

bizalmasság: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

biztonsági esemény: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

DNS-szolgáltató: olyan Szervezet, amely a következő szolgáltatások valamelyikét nyújtja:

a) autoritatív DNS-szolgáltatás: a domainnév – domainnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű domainnév-nyilvántartó szolgáltatás része,

b) rekurzív DNS-szolgáltatás: olyan DNS-szolgáltatás, amely a felhasználók domainnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő domainnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére,

c) DNS-gyorsítótárazás: a domainnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt domainnévadatok alapján történő kiszolgálása,

domainnév: az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

domainnév-regisztrációt végző szolgáltató: a legfelső szintű domainnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domain regisztrálására,

elektronikus információs rendszer: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

európai kiberbiztonsági tanúsítási rendszer: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti rendszer,

felhőalapú számítástechnikai szolgáltatás: olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez,

felhőszolgáltató: felhőalapú számítástechnikai szolgáltatást nyújtó Szervezet,

gyártó: az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója,

IKT-folyamat: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

IKT-szolgáltatás: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

IKT-termék: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

kiberbiztonsági audit: az elektronikus információs rendszerek tekintetében a kiberbiztonsági követelmények teljesülésére vonatkozó vizsgálat, ellenőrzés,

kiberfenyegetés: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató: olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt,

kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató: olyan Szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról,

közösségimédia-szolgáltatási platform: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással,

kutatóhely: a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából,

legfelső szintű domainnév-nyilvántartó: olyan Szervezet, amelyre egy meghatározott legfelső szintű domaint bíztak és amely felelős egyrészt a legfelső szintű domain kezeléséért – ideértve a legfelső szintű domain alatti domainnevek nyilvántartásba vételét –, másrészt a legfelső szintű domain technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű domainzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a Szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű domainneveket a nyilvántartó kizárólag saját használatra veszi igénybe,

megfelelőségértékelés: az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek,

megfelelőségértékelő Szervezet: a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

megfelelőségi nyilatkozat: a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek,

megfelelőségi önértékelés: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom,

nemzeti kiberbiztonsági tanúsítási rendszer: IKT-termékek, IKT-szolgáltatások és IKT-folyamatok tanúsítására, megfelelőségértékelésére Magyarországon alkalmazandó, az európai kiberbiztonsági rendszerek elvei alapján kidolgozott és a tanúsító hatóság által meghatározott szabályok, műszaki követelmények, szabványok és eljárások átfogó rendszere,

nemzeti kiberbiztonsági tanúsítvány: olyan független harmadik fél által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek,

online piactér: olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást alkalmaz, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal,

rendelkezésre állás: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

sértetlenség: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény szerinti fogalom,

tanúsítás: független harmadik fél által végzett megfelelőségértékelési tevékenység,

tartalomszolgáltató hálózat szolgáltatója: a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója,

távoli sérülékenységvizsgálat: olyan Információbiztonsági vizsgálat, amelynek során

a) az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,

b) automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy

c) a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.

1.6 Kapcsolódó dokumentumok

Jogszabályok

a) a munka törvénykönyvéről szóló 2012. évi I. törvény

b) a büntető Törvénykönyvről szóló 2012. évi C. törvény

c) a polgári Törvénykönyvről szóló 2013. évi V. törvény

d) 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

e) 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

f) 474/2024. (XII. 31.) Korm. rendelet a kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról

g) 475/2024. (XII. 31.) Korm. rendelet az ország védelme és biztonsága szempontjából jelentős szervezetek ellenálló képességéről

h) 59/2024. (XII. 23.) BM rendelet a kritikus szervezet ellenálló képességéért felelős vezető rendszeres továbbképzésére vonatkozó szabályokról

i) 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről.

j) 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól

k) 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

l) 2/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági felügyeleti díjról

m) az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes Szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről szóló 73/2013. (XII. 4.) NFM rendelet

n) a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 187/2015. (VII. 13.). rendelet

o) az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.) szóló 2011. évi CXII. törvény

p) a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény

q) a közokiratokról, a közlevéltárakról, és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény

r) a polgárok személyi adatainak kezelésével összefüggő egyes törvények módosításáról szóló 1999. évi LXXII. törvény

s) a szerzői jogról szóló 1999. évi LXXVI. törvény

t) az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény.

1.7 Szerepkörök

A Szervezet a részletes Szervezeti szerepköröket a *Szervezeti és Működési Szabályzatban*, annak hiányában e dokumentumban és a Szervezeti organogrammban rögzítette.

Bonyhádi Kórház és rendeleőintézet főigazgatója (Szervezet vezetője): az Információbiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat, határoz meg a cselekvési terv teljesülése érdekében.

Az Információbiztonsági feladatok vezetői szintű tervezése, koordinálása, a Szabályzatban előírt kontrollok működtetésének biztosítása és azok működésének felügyelete a Szervezet vezetőjének feladata. A Szervezet vezetőjének felelőssége az ügyvitel kialakítása során a Szervezetre vonatkozó informatikai biztonsággal kapcsolatos jogszabályi követelmények érvényre juttatása.

A Szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b) biztosítja a Szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c) az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,
d) meghatározza a Szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve ~~ki~~adja az Információbiztonsági Szabályzatot,
e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
f) a végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
g) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
h) 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,
i) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
j) ha a Szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
k) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.
m) ellenőrzi a védelmi eszközökkel való ellátottságot
n) előzetes bejelentési kötelezettség nélkül ellenőrízheti az informatika, információbiztonsági folyamatok bármely részét.

A Szervezet vezetője a fenti feladatokat delegálhatja, figyelembe véve az összeférhetetlen feladatok egy személyhez történő delegálását.

Az Információbiztonsági felelős (IBF): az informatikabiztonsággal kapcsolatban szervezi, és szakmai kompetenciájának megfelelően végrehajtja a Szervezet által meghatározott terveket. Kapcsolatot tart és felügyeli a feladatok végrehajtásával megbízott személyt, vagy személyeket.

Az elektronikus információs rendszer biztonságáért felelős személyt a Szervezet vezetője nevezi ki vagy bízza meg. Az elektronikus információs rendszer biztonságáért felelős személy felel a Szervezetnél előforduló információs rendszer védelméhez kapcsolódó feladat ellátásáért. Ennek során

- közreműködik a Szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtésében és fenntartásában;
- támogatás nyújt az előző pontban meghatározott tevékenységek tervezésében, szervezésében, koordinálásában és ellenőrzésében;
- előkészíti a Szervezet elektronikus információs rendszereire vonatkozó Információbiztonsági Szabályzatot;
- előkészíti a Szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását;
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Szervezet információbiztonsági Szabályzatait, szerződéseit;
- elősegíti a törvényi megfelelést a Szervezet valamennyi elektronikus információs rendszerének tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésben és kockázatkezelésben, karbantartásban vagy javításban közreműködők esetében;
- elősegíti a törvényi megfelelést abban az esetben, ha a Szervezet adatkezelési vagy adatfeldolgozó tevékenységre közreműködőt vesz igénybe;
- felülvizsgálja a Szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását;
- a Szervezet vezetőjének kérésre közreműködik az Információbiztonsági incidensek kivizsgálásában.

Az elektronikus információs rendszer biztonságáért felelős személy jogosult a Szervezet tevékenységeihez köthető közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében valamennyi adatot, illetve az elektronikus információs rendszerek biztonságában keletkezetett valamennyi dokumentumot bekérheti.

Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó követelményeket, valamint a feladatköröket részletesen a *7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről,* valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szabályozza.

Az információbiztonsági felelős feladata a változásra vonatkozóan rendelkezésre álló információk alapján megvizsgálni és értékelni a tervezett változtatás információbiztonságra gyakorolt várható hatását, lehetséges kockázatait, s ennek alapján a változtatás – esetleg kiegészítő védelmi intézkedésekkel történő – jóváhagyására, illetőleg a változtatási igény elutasítására javaslatot tenni a Szervezeti vezetője felé.

A rendszergazda **(informatikai rendszerek felügyeletével, kezelésével megbízott személy vagy szervezet)**: a Szervezet vezetőjének iránymutatásával a

szerződésben leírtaknak és e Szabályzatnak megfelelően végzi feladatait. Szorosan együttműködik az elektronikus információs rendszer biztonságáért felelős személlyel az Információbiztonsági követelmények kialakításában és végrehajtásában. A védelem helyi operatív végrahajtásáért a rendszer biztonságos üzemeltetéséért felelős a rendszergazda.

A rendszergazda feladata:

- a hálózati struktúra tervezése, az új elemek becsatlakozásának szabályozása,
- hálózaton működő alkalmazások telepítésének tervezése, telepítése vagy a telepítés szakmai felügyelete, használatuk szabályozása,
- a hálózati forgalom figyelése,
- a hálózati hibák felderítése, az elhárításhoz szükséges intézkedések megtétele,
- a hálózati felhasználók üzemeltetési feladatainak szakmai irányítása.
- a Szervezeti szintű informatikai alkalmazások felügyelete, folyamatos működésük biztosítása,
- az alkalmazás használatához szükséges hálózati- és erőforrás-hozzáférési jogok biztosítása a felhasználók részére,
- az alkalmazásokkal kapcsolatos, felhasználóktól érkező észrevételek fogadása, a szükséges változtatások, módosítások megtétele, regisztrálása,
- a hálózati struktúra nyilvántartása,
- a felhasználók nyilvántartása és tájékoztatása,
- felhasználói programok havi és rendkívüli frissítése,
- új hardver kiegészítők illesztése a már meglévő konfigurációkhoz,
- hardver változtatások végrehajtása hibajavítás vagy elavulás esetében,
- hardver, szoftver nyilvántartási adatok folyamatos frissítése,
- a felhasználók betanításában való közreműködés,
- felhasználói dokumentációk biztosítása,
- az informatikai alkalmazások felügyelete, folyamatos működésének biztosítása.
- a Szervezet informatikai igényeinek (hibák, változások) fogadása, informatikai hibák javítása, informatikai változási igények végrehajtása;
- mentési és naplózási elvárások érvényre juttatása;
- ügyviteli igényeknek megfelelő mentési rend kialakítása és mentési eljárások kidolgozása;
- hatáskörébe tartozó informatikai rendszerek jogosultságadminisztrációs feladatainak ellátása, jogosultság nyilvántartás naprakészen tartása
- a Szervezet elektronikus információs rendszereinek nyilvántartása, beleértve a hardver-, szoftver- és licencnyilvántartás elkészítését
- részvétel az Információbiztonsági stratégia felülvizsgálatában, megvalósításában
- új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása
- a Szervezet elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata
- a saját feladatkörébe tartozó rendszerek felügyelete
- feleleős az infoematikai rendszerek üzembiztonságáért,szerverek adatairól biztonsági másolatok készítéséért és azok karbantartásáért

- gondoskodik a rendszer kritikus részeinek meghatározásáért és újra indíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról
- feladata a védelmi eszközök működésének folyamatos elelnőrzése
- felelős a Szervezetali rendszerek hardver eszközeinek karbantartásáért
- gondoskodik a folyamtos vírusvédelem fenntartásáról
- folyamatosan figyelemmel kíséri és vizsgálja a rendszerek működése és biztonsága szempontjából lényeges paraméterek alakulását, kritikus eseményekkor jelzi a Szervezet vezetőjének ellenőrzi a rendszerek adminisztrációját

Beosztottak, alkalmazottak, külső szereplők (Felhasználó): végrehajtják és betartják az utasításokat, szabályokat. Magatartásukkal segítik a hatékony és biztonságos informatikabiztonság megteremtését. Felhasználó a Szervezet minden munkavállalója, alvállalkozója, foglalkoztatási formától függetlenül, aki az informatikai rendszerekhez jogosultságot kap és azt használja. A felhasználók kötelezettsége a Szabályzatban szereplő, illetve a Szervezet vezetője által előírt védelmi intézkedések körültekintő betartása Alapvető elvárás a felhasználókkal szemben, hogy a napi munkavégzés során az informatikai rendszerek használata során jelen Szabályzat szellemiségével összhangban járjanak el.

A Szervezeti szerepköröket a Szervezet a munkaköri leírásokban, a Szervezet *Szervezeti és Működési Szabályzatában*, megbízási és egyéb szerződésekben rögzítette.

A felhasználó

- elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználó azonosító kódja (user ID) alapján végeztek, csak azon eszközök, alkalmazásokhoz férnek hozzá, amelyre felhatalmazást kaptak;
- megakadályozza a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési kódok titkosságát;
- betart minden, az informatikai rendszerek megfelelő használatára, tárolására és megsemmisítésére vonatkozó szabályt és az eszközöket a céljuknak megfelelően használja;
- a számítástechnikai berendezéseket, programokat előírás, rendeltetés szerint használja;
- jelenti az észlelt incidenseket, sebezhetőségeket, működésbeli problémákat a rendszergazdának és a Szervezet vezetőjenek;
- elvárható gondossággal jár el az adatkezelés során, mind az adatbevitel, mind a kimenő adatok elkészítése alkalmával.

A felhasználónak joga van

- tájékoztatást kapni a helyi felhasználói szabályokról, a rendszergazda személyéről, feladat- és hatásköréről,
- panaszt tenni a rendszergazda intézkedései ellen az adott Szervezeti egység vezető-jénél,
- a számára megítélt erőforrások biztosítását a rendszergazdától kérni,

- a géphez hozzárendelt szolgáltatásokat a felhasználói kategóriába sorolástól függően igénybe venni.

A felhasználó kötelessége

- a felhasználókra vonatkozó szabályok betartása,
- a rendszergazda üzemeltetés tárgykörében tett javaslatainak végrehajtása,
- a gép használatával kapcsolatos fontosabb események, hibák bejelentése a rendszergazdánál,
- más felhasználók figyelmeztetése a szabályok betartására, a nem rendeltetésszerű, illetve Szabályzatokkal ellentétes használat megakadályozása és jelentése,
- az általa felfedezett biztonsági problémák jelentése a rendszergazdának.

A felhasználónak TILOS

- a gépek megbontása, a hardver konfigurációk megváltoztatása,
- az esetlegesen előforduló biztonsági lyukak, hiányosságok kihasználása,
- más felhasználók munkájának zavarása, anyagainak illetéktelen megtekintése, másolása,
- más felhasználó bejelentkezési nevének, illetve jelszavának használata,
- a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása,
- külső forrásból származó hordozható adattárolók felhasználása a rendszergazda által végzett vírusellenőrzés előtt.

Vírusfertőzés (vagy annak gyanúja) esetén a rendszergazdát azonnal értesíteni kell a gépet le kell kapcsolni, s további használatát a rendszergazda intézkedéséig fel kell függeszteni.

Meghibásodás esetén a hiba kijavítását a felhasználó nem kísérelheti meg, azonban meg kell tennie mindazokat a feladatkörén belül eső intézkedéseket, amelyekkel a hálózatot (adatok, gépek) további károsodástól megóvja. Célszerű a géppel való munkát azonnal felfüggeszteni és haladéktalanul értesíteni a rendszergazdát.

A felhasználó nem kísérelheti meg a számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzését. Az erre irányuló próbálkozás, annak sikerétől függetlenül, fegyelmi vétségnek minősül.

Amennyiben a felhasználó a Szabályzatokban foglaltakat vétkesen – szándékosan vagy gondatlanul – megszegi és személyével kapcsolatosan fegyelmi vétség gyanúja merül fel, a rendszergazda a kötelezettségszegésről és annak körülményeiről haladéktalanul írásban tájékoztatja a Szervezet vezetőjét, aki dönt a fegyelmi eljárás megindításáról.

A fegyelmi eljárás lefolytatására, illetve a kártérítési felelősségének megállapítására a mindenkori vonatkozó jogszabályok az irányadók.

A nem alakalmazotti jogviszonyban elkövetett károkozás esetén a kárigény érvényesítése a polgári jog általános szabályai szerint történik.

Harmadik fél szolgáltatásainak igénybe vétele előtt a Szervezet vezetőjének feladata, az elektronikus információs rendszer biztonságáért felelős személlyel együttműködve, az informatikai biztonsággal kapcsolatos kockázatok előzetes felmérése, hogy mely kockázatok értékelése alapján fogja a későbbiekben kötendő szerződést elkészíteni.

Harmadik félnek tilos megengedni a hozzáférést az információkhoz, információfeldolgozó eszközökhöz, amíg a kellő óvintézkedések (pl. megfelelő titoktartási és bizalmassági nyilatkozat aláírása) foganatosítása nem történt meg, és a felek nem állapodtak meg és nem rögzítették ezt a szerződésben.

1.8 Engedélyezési eljárás

A Szervezet vezetője jogosult és köteles a Szervezet hatáskörébe tartozó – jelen IBSZ-ben engedélyezéshez kötött – minden információbiztonsággal kapcsolatos tevékenységgel, intézkedéssel kapcsolatban a szükséges engedélyezési eljárást lefolytatni, különösen az alábbiak esetében:

a) az irányítása alá tartozó munkavállalók munkavégzéséhez szükséges infokommunikációs eszközök biztosítása;
b) a használt, illetve használandó, új rendszerek és azokhoz szükséges jogosultságok, hozzáférések beállítása (a kapcsolódó felhasználói fiókok létrehozása, módosítása, illetve törlése), illetve a rendszer vagy rendszerelem konfigurációjának módosítása;
c) az elektronikus információs rendszereknek helyt adó létesítményekbe, helyiségekbe történő belépés;
d) információs rendszerelemek be- és kiszállítása;
e) az elektronikus információs rendszeren, illetve elemein karbantartás, javítás végrehajtása, a munkavégzés engedélyezése;
f) elektronikus adathordozók használata;
g) távoli, illetve vezeték nélküli hozzáférések;
h) együttműködésen alapuló számítástechnikai eszközök használata;
i) új elektronikus információs rendszer bevezetése;
j) új rendszerelem meglévő EIR-be illesztése;
k) elektronikus információs rendszerének más (helyi, illetve külső) elektronikus információs rendszerekhez történő kapcsolódása.

1.9 Tevékenységek

A Szervezet a tv.-ben meghatározott alaptevékenységét a *Szervezeti és Működési Szabályzatban*, alapító okiratban, vagy más hivatalos dokumentumban rögzítette.

2. SZERVEZET RENDSZEREINEK BESOROLÁSI NYILATKOZATA

Bonyhádi Kórház és rendeleőintézet nyilatkozatban rögzíti, hogy a Szervezet szakemberi által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett a *7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről*, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről rendeletnek való megfelelés szerinti vizsgálatot, mely eredményeként a Szervezet EIR-jeinek ée ezzel a Szervezet biztonsági szintje

„magas" besorolású

A „jelentős" biztonsági osztály esetében közepes káresemény következhet be, mivel:

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

A Szervezet a keretrendszer alkalmazására való felkészülésként a jelentős szint elérésére és fenntartására a következő folyamatokat vezeti be és tartja fenn:

A Szervezetre vonatkozóan meghatározza és dokumentumban rögzíti

- az elektronikus információs rendszerei védelmével kapcsolatos szerepköröket, felelősségeiket, feladataikat és az ehhez szükséges hatásköröket;
- a kockázatmenedzsment stratégiáját, amely leírja, hogy a Szervezet hogyan azonosítja, értékeli, kezeli és felügyeli a biztonsági kockázatokat;
- a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát, amely magába foglalja a védelmi intézkedésekhez kapcsolódó tevékenységek ellenőrzésének gyakoriságát, felügyeletének módszereit és eszközeit.

Az elektronikus információs rendszerekre vonatkozóan meghatározza és dokumentumban rögzíti:

- a rendszer által támogatandó üzleti célokat, funkciókat és folyamatokat,
- a tervezésben, fejlesztésben, implementálásban, üzemeltetésben, karbantartásban, használatban és ellenőrzésben érintett személyeket vagy Szervezeteket,
- az érintett vagyonelemeket,
- a rendszer Szervezeti és technológiai határát,
- a rendszer által feldolgozandó, tárolandó és továbbítandó adatköröket és azok életciklusát,

- a rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését,
- a rendszer helyét a Szervezeti architektúrában, amennyiben a Szervezet rendelkezik vele;

A Szervezet az érintett személyi kör részére biztosítja a Szervezeti, vagy feladathoz rendelt működési terület hatályos információbiztonságot érintő munkautasításokat, belső rendelkezéseket, szabályozásokat, vagy más erre célra szolgáló dokumentumokat:

- az Információbiztonsági Szabályzatot a Szervezetre érvényes rendelkezések szerint az erre jogosult vezető hagyja jóvá;
- az Információbiztonsági Szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;
- a Szervezet az Információbiztonsági Szabályzat be nem tartását fegyelmi ill. jogi eljárás keretében szankcionálja;
- az érintett Szervezet biztonsági kontrollfolyamatai eljárásrendben szabályozottak; mellyek tartalmazzák a kontrollfolyamatok végrehajtásának menetét, módját, időpontját, végrehajtóját, tárgyát, eszközét;
- ezek a folyamatok egyértelműen meghatározzák az információbiztonsági felelősségeket és a biztonságtudatos viselkedést az elektronikus információs rendszerrel kapcsolatba kerülő személyek, valamint az információbiztonságért felelős személyek és Szervezeti egységek tekintetében;
- ezen folyamatokat a Szervezet olyan Szervezeti egységek, vagy személyek felügyelete alá rendeli, akik az adott folyamat végrehajtása érdekében közvetlen kapcsolatban állnak a folyamatban érintett más személyekkel, vagy Szervezeti egységekkel;
- a folyamatokat és végrehajtásukat a Szervezet úgy dokumentálja, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi köre - megállapítható legyen.

A Szervezet nyilatkozatban rögzíti, hogy a szakemberei által biztosított adatok alapján, külsős szakember bevonásával egy kockázatértékelés során végzett a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról és a 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről elvárásokat figyelembe véve, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről felhasználásával végzett vizsgálatának eredményeként a Szervezet rendszereinek biztonsági osztályai a következők:

Az IT biztonsági műszaki követelmények olyan óvintézkedések (ellenintézkedések), amelyeket az informatikai rendszer és a humán erőforrások valósítanak meg, illetve hajtanak végre a rendszer hardware, software vagy firmware összetevőiben megvalósuló mechanizmusok segítségével. Az informatikai rendszerek biztonságát alapvetően adminisztratív, logikai és fizikai biztonsági intézkedésekkel lehet megteremteni.

A Szervezet által működtetett és osztályba sorolt rendszerrel szembeni biztonsági célja

a) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan tárolással, kezeléssel, hozzáféréssel és közléssel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,

b) a tárolt, továbbított vagy egyéb módon kezelt adatok védelme a véletlen vagy jogosulatlan megsemmisítéssel, elvesztéssel, megváltoztatással vagy a hozzáférhetetlenséggel szemben az IKT-termék, az IKT-szolgáltatás és az IKT-folyamat teljes életciklusa alatt,
c) annak biztosítása, hogy a feljogosított személyek, programok vagy gépek kizárólag a hozzáférési jogaik tárgyát képező adatokhoz, szolgáltatásokhoz vagy funkciókhoz férhetnek hozzá,
d) az ismert függőségek és sebezhetőségek azonosítása és dokumentálása,
e) annak rögzítése, hogy a feljogosított személy, program vagy gép mely időpontban és mely védendő adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,
f) annak ellenőrizhetővé tétele, hogy a feljogosított személy, program vagy gép mely időpontban és mely adatokat, szolgáltatásokat vagy funkciókat vett igénybe, használt vagy egyéb módon kezelt,
g) annak ellenőrzése, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok nem tartalmaznak-e ismert sebezhetőségeket,
h) fizikai vagy műszaki biztonsági esemény bekövetkeztekor az adatok, a szolgáltatások és a funkciók rendelkezésre állásának, valamint az adatokhoz, a szolgáltatásokhoz és a funkciókhoz való hozzáférésnek a mihamarabbi helyreállítása,
i) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok kockázatarányosan, alapértelmezetten és tervezetten biztonságosak legyenek,
j) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok szoftvere és hardvere naprakész legyen, és
k) annak biztosítása, hogy az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok vonatkozásában nem állnak fenn közismert sebezhetőségek, továbbá rendelkezésre állnak a biztonságos frissítésükre szolgáló mechanizmusok.

A célokhoz hozott intézkedések és szempontok:

Adminisztratív biztonsági intézkedés: minden olyan védelmi intézkedés, amely technikai eszközökkel nem, vagy csak részben valósítható meg. Ilyen például egy Információbiztonsági Szabályzat elkészítése vagy egy kockázatelemzés elvégzése.

Fizikai biztonsági intézkedések: az adott épület/objektum és az azokban található vagyontárgyak védelmét szolgáló intézkedések, ezek közé tartozik többek között a számítógépterem biztonságának megteremtése (pl.: tűzjelző, riasztó, beléptető rendszer stb.) vagy a munkatársak részére az "üres íróasztal, üres képernyő politika" elrendelése.

Logikai biztonsági intézkedés: az informatikai rendszerben technikailag beállított vagy kikényszerített védelmi megoldás, ilyen lehet egy megfelelő jelszóházirend beállítása vagy a hálózati tűzfalon csak a szükséges portok, protokollok engedélyezése.
Ahhoz, hogy ezeket a célokat el lehessen érni, **bizalmasság, sértetlenség** és **rendelkezésre állás** szempontjából szükséges az egyes rendszerek osztályozása.

Bizalmasság (B): 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.

Sértetlenség (S): az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek.

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

A kockázati érték, nem egy rendszerelem abszolút kockázatos voltát adja meg, hanem a rendszereket állítja sorrendbe, ahol a legnagyobb kockázati értékű rendszer a „leggyengébb láncszeme" és a legnagyobb eséllyel ebben a rendszerben következik be kár, ha nem változtatunk a biztonsági intézkedéseken.

Amennyiben a Szervezet több rendszert is működtet és besorol, abban az esetben a Szervezet által működtetett informatikai rendszerben, olyan biztonsági osztálynak megfelelő követelményeket kell bevezetnie, amelyik a besorolt rendszerek között a legmagasabb besorolású.

Az EIR-ek besorolását tartalmazó részletes lista az *Informatika Biztonsági Szabályzat 1. sz. függelékében* érhető el.

Az Információbiztonsági Szabályzat elsősorban a következő, az érvényes rendeletben meghatározott elektronikus információs rendszerbiztonsággal kapcsolatos területeket szabályozza:

3. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

3.1 Programmenedzsment

Információbiztonsági Szabályzat

A Szervezet vezetője megfogalmazza, dokumentálja, valamint kihirdeti az Információbiztonsági Szabályzatát. Az Információbiztonsági Szabályzatot a Szervezet vezetője hagyja jóvá.

Az Információbiztonsági Szabályzatot szükség szerint, de legalább két évente egyszer az informatika biztonsági rendszer felülvizsgálata során a Szervezet vezetője az IB felelőssel együtt, felülvizsgálja, szükség szerint módosítja. Az Információbiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az Információbiztonsági Szabályzatot felülvizsgálja, szükség szerinti módosítja. A Szervezet vezetője az IBSz-ben rögzíti a Szervezet egyes elektronikus információs rendszereinek (EIR) elvárt és megállapított biztonsági osztályát, melyet a *Cselekvési terv*ben dokumentál.

Az IBSZ tartalmában átfogó képet nyújt a biztonsági követelményekről, valamint a követelményeknek való megfelelés érdekében a Szervezet által működtetett, vagy bevezetni kívánt védelmi intézkedésekről. Meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a Szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat. Leírja az információbiztonságért felelős Szervezeti egységek közötti együttműködést. E dokumentum szerint a Szervezet vezetője elszámoltatható a Szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a Szervezeti eszközök, személyek, más Szervezetek szempontjából számottevőnek tartott kockázatokért. Gondoskodik arról, hogy az információbiztonsági Szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható

Az elektronikus információs rendszerek biztonságáért felelős személy

A Szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt nevez ki (szükség esetén, akár külsős alvállalkozó), a vonatkozó jogszabáji követelmények és Szervezeti szintű információbiztonsági Szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására aki számára biztosítja számára a célok eléréséhez szükséges erőforrásokat. A Szervezet vezetője gondoskodik (alvállalkozó esetén szerződésben elvárja) a biztonságért felelős személy képzettségéről az idevonatkozó rendeletnek megfelelően, továbbá megköveteli az erkölcsi fedhetetlenséget.

Információbiztonságot érintő erőforrások

A Szervezet az információbiztonsági céljaink végrehajtásához és fejlesztéséhez szükséges erőforrásokat beépíti az éves költségvetés tervezésébe és beruházási kérelmeibe, valamint dokumentál minden olyan esetet, amelyek e követelmény alól kivételt képeznek. Gondoskodunk arról, hogy a szükséges dokumentáció összhangban legyen a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel,

szabályozásokkal, szabványokkal és ajánlásokkal. A Szervezet vezetője biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez tervezett forrásokat.

Intézkedési terv és mérföldkövei

A Szervezet vezetője *Intézkedési tervet (Cselekvési terv)* készít az elektronikus információbiztonsági feladatok megvalósításához az ide vonatkozó törvényben meghatározott határidőkkel. Az így elkészített intézkedési tervet legalább évente felülvizsgálja és karbantartja. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett Szervezetre érvényes szint, akkor a Szervezet vezetője a vizsgálatot követő 90 napon belül felülvizsgálatot készít (aktualaizálja a cselekvési tervet) a hiányosság megszüntetése érdekében.

A tervben foglalt feladatok végrehajtásában köteles minden érintett Szervezeti munkavállaló és az IT üzemeltető közreműködni. A tervben foglaltak végrehajtását az információbiztonsági felelős köteles ellenőrizni, s annak eredményéről a Szervezet vezetőjét tájékoztatni, indokolt esetben a terv felülvizsgálatát, módosítását kezdeményezni, továbbá abban szükség szerint közreműködni.

Ebben az intézkedési terv biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó Szervezeti elektronikus információs rendszerek intézkedési tervei

- ki legyenek dolgozva,
- karban legyenek tartva,
- dokumentálják a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket,

hogy megfelelően reagáljanak a Szervezeti műveletek és eszközök, személyek, más Szervezetek kockázataira és a meghatározott jelentési követelmények bemutatásra kerüljenek. A Szervezet áttekinti az intézkedési terveket és mérföldköveket, hogy azok összhangban állnak-e a Szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedések Szervezeti szintű prioritásaival.

Az elektronikus információs rendszerek nyilvántartása

A Szervezet vezetője az elektronikus információs rendszereiről, minden rendszerre nézve egy elektronikus nyilvántartást vezetet, melyet szükség szerint aktualizál. Ez magában foglalja a szoftvereket, hardvereket, hálózati infrastruktúrát és egyéb technológiai eszközöket. A nyilvántartás tartalmazza

a) a rendszerek alapfeladatait;

b) a rendszerek által biztosítandó szolgáltatásokat;

c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Szervezet kezelésében vannak);

d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

e) a rendszert szállító, fejlesztő és karbantartó Szervezetek azonosító és elérhetőségi adatait, valamint ezen Szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait;

f) követi Szervezet EIR-jeiben bekövetkezett változásokat (pl.: új rendszer bevezetése, meglévő rendszer kivezetése)

g) meghatározott gyakorisággal (ha nem történt változás évente) felülvizsgálja az EIR-ek nyilvántartását.

A Szervezet vezetője az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban *(Elektronikus Információs Rendszerelem Leltár)* kezeli.

Biztonsági teljesítmény mérése

A Szervezet kifejleszti az EIR-ei biztonsági mérésének rendszerét, folyamatosan felügyeli a teljesítménymutatókat, és rendszeres jelentéseket készít ezekről. Főbb teljesítménymutatók:

a) a rendszer állapota
   - rendszerfrissítések és azok hatékonysága
   - rendszerek naprakészsége,

b) a kiberbiztonsági rezilienciájának állapota
   - vírusvédelem hatékonysága,

c) a dolgozók biztonságtudatossága
   - egy phishing kampánnyal szembeni ellenállása,
   - képzést követő vizsga eredményei,
   - a felhasználók jelszókezelési szokásai,

d) a Szervezet reakcióideje
   - átlagos biztonsági esemény reagálási idő,
   - sérülékenységek felfedése utáni frissítési és hibakezelési eljárási idő,
   - rendelkezésre állás monitoring.

e) az üzletmenetfolytonosság vonatkozásában
   - az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tesztelés végrehajtási ideje és annak hatékonysága.

Szervezeti architektúra

A Szervezet kifejleszti és fenntartja azt a Szervezetrendszert (arhitektúrát), amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a Szervezeti működésre, az eszközökre, az egyénekre és más Szervezetekre annak érdekében, hogy a biztonsági követelmények és védelmi intézedések integrálása a vállalati architektúrába segítsen annak biztosításában, hogy a biztonsági megfontolások a rendszerfejlesztési életciklus során mindvégig érvényesüljenek, és kifejezetten kapcsolódjanak a Szervezet működési céljaihoz és üzleti folyamataihoz. A Biztonsági Architektúra követelmény az alábbi intézkedések során valósul meg:

- Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
- Rendszerbiztonsági terv
- Információbiztonsági architektúra leírás
- Szervezeti működés és üzleti folyamatok meghatározása
- Biztonsági osztályba sorolás
- A rendszer fejlesztési életciklusa
- Biztonságtervezési elvek
- Fejlesztői biztonsági architektúra és tervezés.

A Szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

A Szervezet működése szempontjából kritikus infrastruktúra és a kulcsfontosságú erőforrások meghatározására és a kapcsolódó infrastruktúra védelmi tervének elkészítésére vonatkozó követelményeket és útmutatást a vonatkozó jogszabályok, végrehajtási rendeletek, irányelvek, szabályok, rendeletek, szabványok és iránymutatások határozzák meg. Így meghatározza:

- melyek a Szervezet működése szempontjából kritikus infrastruktúrák és kulcsfontosságú erőforrások.
- kidolgozza az ezen infrastruktúrák biztonsági tervét. Ez a terv tartalmazza az információbiztonsági kérdéseket, beleértve az EIR védelmét és a kiberbiztonsági fenyegetések kezelését.
- Dokumentálja a biztonsági tervet, beleértve az EIR-re vonatkozó információbiztonsági intézkedéseket. Ez magában foglalja a biztonsági eljárásokat, a kiberbiztonsági fenyegetések kezelésének módszereit, és a Szervezet működése szempontjából kritikus infrastruktúrák és erőforrások védelmének stratégiáit.

Kockázatmenedzsment stratégia

A Szervezet egy átfogó stratégia szerint kezeli az EIR-ek működésével és használatával összefüggő, a Szervezet működéséhez, vagyonelemeihez, a Szervezethez köthető személyekhez, és más Szervezetekhez kapcsolódó biztonsági kockázatokat a személyes adatok kezeléséből fakadó kockázatokat. Az egész Szervezeten belül egységesen alkalmazza a kockázatmenedzsment stratégiát. Szervezeti változás esetén felülvizsgálja és frissíti a kockázatmenedzsment stratégiát, hogy meg tudjon felelni a Szervezeti változásoknak.

A kockázatkezelési stratégia magában foglalja a Szervezet kockázattűrésének meghatározását, a kockázatcsökkentési stratégiákat, az elfogadható kockázatértékelési módszereket, a Szervezet egészére kiterjedő kockázatértékelésének folyamatát, valamint a kockázat időbeli nyomon követésére szolgáló megközelítéseket. A kockázatkezelésért felelős vezető (a Szervezet vezetője és az IBF) összehangolja az információbiztonság irányítási folyamatait a stratégiai, operatív és költségvetési tervezési folyamatokkal.

Engedélyezési folyamatok meghatározása

A Szervezet az engedélyezési folyamatokon keresztül kezeli az EIR-ek és azok környezetének biztonsági állapotát. Kijelöli a Szervezet kockázatmenedzsment folyamatának felelőseit (névvel és felelősségi körrel ellátva az IT engedélyezési jogosultságok táblázatban).

Beilleszti az engedélyezési folyamatot a Szervezet egészét átfogó kockázatkezelési keretrendszerbe.

Az engedélyezési folyamatot összehangolja a folyamatos felügyeleti folyamatokkal, hogy elősegítsék a biztonsági kockázatok folyamatos megértését és elfogadását az érintett Szervezet működésére, eszközeire, személyekre, más Szervezetekre.

Szervezeti működés és üzleti folyamatok meghatározása

A Szervezet meghatározza a Szervezeti célokat és az üzleti folyamatokat, figyelembe véve az információbiztonságot, valamint a Szervezeti működésre, eszközökre, személyekre, más Szervezetekre gyakorolt kockázatokat. Meghatároza a Szervezeti

célokból és üzleti folyamatokból adódó információvédelmi igényeket. Évente a pénzügyi tervezéskor, felülvizsgálja és szükség szerint módosítja a Szervezeti célokat és az üzleti folyamatokat.

Biztonsági személyzet képzése

A Szervezet létrehoz egy a biztonsági személyzet képzését és fejlesztését elősegítő programot, amely biztosítja a feladatok ellátásához szükséges ismeretek, készségek és képességek meghatározását, a biztonsági szerep- és felelősségi körökkel megbízott személyek számára, valamint szabályokat az egyéni képzettségének mérésére és fejlesztésére. Ezek a programok mérhetővé teszik az egyéni teljesítményt, valamint karrierutat biztosítanak a biztonsági szerepköröket betöltők számára, ezzel is ösztönözve a szakembereket a területen való előre lépesre és a nagyobb felelősséggel járó pozíciók betöltésére. E program keretében a Szervezet

- meghatározza azt a tudást, készségeket és képességeket, amelyekre szükség van a biztonsággal kapcsolatos feladatok elvégzéséhez,
- szerepkör-alapú képzési programokat fejleszt azok számára, akik biztonsági szerep- és felelősségi köröket látnak el,
- meglévő szabványokat és irányelveket alkalmaz az egyéni képesítések méréséhez,
- ösztönzi a biztonsági szakembereket a területen való előre lepésre és a nagyobb felelősségfel járó pozíciók betöltésére,
- a munkaerőprogramokat összehangolja a Szervezeti biztonsági tudatosság és képzési programokkal,
- dokumentálja a programban részt vevők előrehaladásáról és fejlődését.
- az oktatási tematikát úgy állítja össze, hogy figyelembe veszi az EIR-ek teszteléseinek és vagy incidensek eredményeinek tapasztalatát.

Tesztelés, képzés és felügyelet

A Szervezet bevezet egy folyamatot, amely biztosítja, hogy a Szervezeti EIR-ekhez kapcsolódó biztonsági tesztelések, képzések és felügyeleti tevékenységek elvégzésére vonatkozó Szervezeti tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek. Felülvizsgálja és összehangolja a terveket a Szervezeti kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész Szervezetre kiterjedő prioritásokkal. A tesztelési, képzési és felügyeleti terveket és tevékenységeket az aktuális fenyegetés- és sérülékenységi vizsgálatok eredményei alapján határozza meg.

Szakmai csoportokkal és közösségekkel való kapcsolattartás

A Szervezet kapcsolatokat alakít ki szakmai csoportokkal és közösségekkel annak érdekében, hogy elősegítse a Szervezethez köthető személyek folyamatos biztonsági oktatását és képzését; naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén; hogy megossza az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket. A szakmai csoportok és közösségek közé tartoznak a speciális érdekcsoportok, szakmai szövetségek, fórumok, hírcsoportok, felhasználói csoportok és a hasonló Szervezetekben dolgozó biztonsági szakemberek csoportjai. Ezen szakmai csoportokkal való kapcsolatot a munkaköri leírásban és vagy megbízásban rögzíti.

Fenyegetettség tudatosító program

A Szervezet a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot vezet be, ami magában foglalja a fenyegetések felderítését és azokról szóló információk megosztását a Szervezeten belül és más Szervezetekkel. Létrehoz egy stratégiát a fenyegetések felderítésére, azonosítására, értékelésére és priorizálására az EIR-en belül. Meghatározza a fenyegetésekkel kapcsolatos információk megosztásának szabályait és eljárásait (megosztandó információk típusát, a megosztás módját és időzítését, valamint a megosztásért felelős személyeket vagy csoportokat). Naplót vezet a fenyegetésekkel kapcsolatos információk megosztásáról, nyomon követi a program hatékonyságát és szükség esetén módosítja azt. (Pl. NKI hírlevél, szakmai csoportokkal való kommunkáció)

Kockázatmenedzsment keretrendszer

A Szervezet azonosítja és dokumentálja a kockázatelemzést, kockázatkezelést és a kockázatok felügyeletét érintő feltételezéseit. A kockázatmenedzsment során figyelembe veszi a prioritásokat és kompromisszumokat; továbbá a kockázattűrő képességet. Megosztja a kockázatmenedzsment tevékenység eredményeit a Szervezet által meghatározott személyekkel. A Szervezetben történő és az EIR-ben történő változásokkor mindig, de legalább évente elvégzi a kockázatmenedzsment keretrendszer szempontrendszerének felülvizsgálatát és frissítését. A kockázatvizsgálat során figyelembe vett prioritások: a releváns rendszerelemek, személyek EIR-ekre gyakorolt hatásai, kockázatainak vizsgálata. A kiemelkedő és nem csökkenthető kockázatokat vagy elviselt (BCP) kockázatként esetenként áthárított kockázatként kell kezelni. A kockázatkezelést a rendszereket ért incidens esetén, de legalább évente, vagy új beszerzéskor kell felülvizsgálni. A kockázatértékelést az IBF vezetésével a management készíti, és az ügyvezető hagyja jóvá. A kockázatértékelést az IBF vezetésével a management készíti, és az ügyvezető hagyja jóvá.

Kockázatkezelésért felelős szerepkörök

A Szervezet vezetője az IBF-et jelöli ki a kockázatkezelésért felelős személynek, aki összehangolja a Szervezeti információbiztonsági irányítási folyamatokat a stratégiai, működési és költségvetés tervezési folyamatokkal. Az IBF biztosítja a kockázatok Szervezeti szintű áttekintését és elemzését, valamint a kockázatmenedzsment Szervezeten belüli egységes működését.

Ellátási lánc kockázatmenedzsment stratégiája

A kockázatkezelésen belül kidolgoz egy a Szervezet egészére kiterjedő, az ellátási lánc kockázatainak kezelésére vonatkozó stratégiát. Az ellátási láncra vonatkozó kockázatkezelés magában foglalja az EIR-ek, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával és selejtezésével kapcsolatos biztonsági kockázatok figyelembevételét. Az ellátási lánc kockázatkezelési stratégiát a Szervezeti és üzleti folyamatok szintjén hajtja végre, valamint az ellátási lánc kockázatkezelési terveit, pedig az EIR-ek szintjén. A változások lekövetése általános kockázatkezelési követés szerint történik. Az ellátási láncokat érintő kockázatkezelést a rendszereket ért incidens esetén, de legalább évente, vagy új beszerzéskor kell felülvizsgálni. Az ellátási lánc kockázatértékelést az IBF vezetésével a management készíti, és az ügyvezető hagyja jóvá együtt kezelve a standard kockázatértékeléssel.

Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói

A Szervezet azonosítja, rangsorolja és értékeli azokat a beszállítókat, amelyek a Szervezet működése szempontjából kritikus technológiákat, termékeket és szolgáltatásokat szállítanak a Szervezet alapvető feladatainak ellátásához. Dokumentálja a beszállítói felülvizsgálatokat, hogy nyomon követhesse a kockázatok változásait és a kockázatcsökkentő intézkedések hatékonyságát.

Folyamatos felügyeleti stratégia

A Szervezet kidolgoz egy felügyeleti stratégiát és folyamatos felügyeleti programot működtet, amely magában foglalja

- a felügyeleti tevékenységek gyakoriságát és módszereit, valamint a mérőszámokat,
- fentart egy programot, amely a felügyeleti stratégia szerint folyamatosan figyelemmel kíséri a mérőszámokat,
- elemzi a felügyeleti és vizsgálati adatok közötti összefüggéseket, hogy meghatározza a védelmi intézkedések hatékonyságát,
- válaszlépéseket tesz a védelmi intézkedések értékelése és a felügyeleti információk eredményei alapján,
- ha nem volt rendkívüli esemény, évente jelentést készít az EIR biztonsági állapotáról a kijelölt személyek számára.
- dokumentálnia a felügyeleti tevékenységeket.

3.2 Hozzáférés felügyelet

Hozzáférés Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A hozzáférés felügyeleti szabályokat meg kell ismertetni a jogosultságot igénylő vezetőkkel és az azokat kiadó érvényesítő rendszergazdákkal. A hozzáférés szabályokat felül kell vizsgálni az incidensek, auditok, jelentős szervezeti változások esetén, de legalább évente.

A hozzáférési szabályok alapvető célja, hogy a szervezetben és a szervezeten kívüli felhasználók a jogosultságuknak és feladatuknak, munkakörüknek megfelelően szűken értelmezett hozzáféréseket megkapják, de annál több joggal ne rendelkezzenek.

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági Szabályzat)* kezeli.

Fiókkezelés

A Szervezet vezetője:

- meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait és ezek típusait;

...értesíti a fiókkezelőket, ha:

- a felhasználói fiókokra már nincsen szükség;

- a felhasználók kiléptek vagy áthelyezésre kerültek;
- az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

...feljogosít az elektronikus információs rendszerhez való hozzáférésre:

- az érvényes hozzáférési engedély,
- a tervezett rendszerhasználat,
- az alapfeladatok és funkcióik alapján;

A Szervezet vezetője évente vagy a fiók és vagy felhasználó változása esetén felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot.

A megbízott személy kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök, adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

A Szervezetben tiltott fióktípus - kockázati alapon - a megosztott, csoportos, vészhelyzeti, névtelen, ideiglenes és vendégfiókok.

Az ideiglenes és vészhelyzeti fiókok rövid távú használatra valók, speciális paraméterekkel ellátva és felügyelve. Az ilyen fiókok létrehozásakor a Szervezetünk megfelelő körültekintéssel járunk el, figyelembe véve a speciális fióktípusokkal együtt járó kockázatokat.

A szervezet vezetője kötelezi, szervezet munkaerejével foglalkozó vezetőjét, hogy ha a munkatárs, vagy külsős megbízott hozzáférése (elbocsátás, áthelyezés, szerződés megszűnésé) megváltozik arról haladéktalanul értesítse a rendszergazdát, vagy a jogosultságot kezelő munkatársat.

A szervezetben a csoport és szerepkört a munkakörökből kell levezetni, kialakítani és a hozzáféréseket kiosztani.

Fiókkezelés – Automatizált fiókkezelés

A Szervezet létrehoz egy automatizált mechanizmust, amely elvégzi az EIR fiókok létrehozását, engedélyezését, módosítását, letiltását és eltávolítását.

Ezt a mechanizmust úgy alakítja ki, hogy értesítést küldjön az EIR fiókkezelőinek, amikor egy fiókot létrehoznak, engedélyeznek, módosítanak, letiltanak vagy eltávolítanak.

E mechanizmus biztosítja, hogy a megszokottól eltérő használat észlelése esetén riasztást küldenek a fiókkezelőknek.

Fiókkezelés – Automatizált ideiglenes és vészhelyzeti fiók kezelés

A Szervezetben tiltott fióktípus a vészhelyzeti fiók. Ám ha mégis ilyet kell létrehozni, akkor azt meghatározott időtartam letelte után automatikusan eltávolítja vagy letiltja.

Fiókkezelés – Fiókok letiltása

A Szervezet az EIR-ben a fiókokat egy automatizmus keretében letiltja

- amennyiben azok lejártak,
- már nem kapcsolódnak a felhasználókhoz vagy egyénekhez,
- megsértik a Szervezeti szabályokat (5 alkalommal rontás után) vagy

- meghatározott ideig inaktívak voltak (30 nap után).

Fiókkezelés – Automatikus naplózási műveletek

E pont a Szabályzat *3.4 pontjában "Naplózható események" és a "Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel"* kontrolloknál kerültek bővebben kifejtésre.

Fiókkezelés – Inaktivitásból fakadó kijelentkeztetés

A Szervezet megköveteli és a rendszerbeállításokban alkalmazza, hogy a felhasználó 10 perc inaktivitási időszak leteltét követően kijelentkezteti.

Fiókkezelés – Használati feltételek

A Rendszergazda a főigazgató utsatására a legkisebb jogosultság elvének betartása, érvényesítésének érdekében a felhasználó fiókokat monitorozhatja, amely magában foglalja a szervezeti keretszabályokat sértő fiókhasználat esetén generált figyelmeztetéseket. A szervezet szükség esetén vagy különleges körülményekor, a rendszerfiókok használatát, korlátozhatja, figyelembe véve a folyamatos működés és betegellátást (pl. a hét bizonyos napjaira, napszakokra vagy meghatározott időtartamra).

Fiókkezelés – Fiókok szokatlan használatának felügyelete

A Rendszergazda a főigazgató utasítására a legkisebb jogosultság elvének betartása, érvényesítésének érdekében a felhasználó fiókokat monitorozhatja, amely magában foglalja fiókokok szokatlan használatának felügyeletét, amely azt jelenti, hogy az érintett szervezet folyamatosan nyomon követi és elemzi a fiókok használatát, így azonosítva azokat a tevékenységeket, amelyek eltérnek a megszokottól. Amennyiben a Rendszergazda szokatlan használatot észlel, arról jelentést készít a Főigazgatónak.

Fiókkezelés – Magas kockázatú személyek fiókjának letiltása

A Szervezet meghatározza azokat a jelentős kockázatokat képviselő személyek fiókjainak kockázatait, amelyek felfedezésétől számított 1 óra időtartamon belül letiltja az érintett felhasználók fiókjait.

Hozzáférési szabályok érvényesítése

Az elektronikus információs rendszer a megfelelő Szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszó fontosságával és a nem megfelelő jelszókezelés következményeivel, mivel egy rosszul megválasztott, könnyen kitalálható jelszó nemcsak a tulajdonosára, hanem a Szervezet informatikai rendszerére is negatív következményekkel járhat.

Alapelvek

- Nem szabad könnyen kitalálható jelszavakat választani. A jelszavakat titokban kell tartani!
- Az induló jelszót első bejelentkezéskor meg kell változtatni. Ha a felhasználónak gyanúja támad, hogy a jelszava kompromittálódott, azonnal meg kell változtatnia!
- A jelszavakat nem szabad kódolatlanul tárolni!

Helyes jelszóválasztás

- nem szabad könnyen kitalálható, személyre jellemző jelszavakat használni
- nem szabad sorozatokat használni (pl abcdefg, 7654321 stb)
- kerülni kell a szótári szavak használatát
- a jelszó tartalmazzon kis és nagybetűket, számokat

Jelszóvédelem

A felhasználóknak különös figyelmet kell, hogy fordítsanak az alábbiakra:

- a jelszót tilos másoknak elmondani, mások előtt a jelszóról beszélni
- a jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti
- tilos közös jelszavakat használni
- a jelszót nem szabad elérhető helyen tárolni, telefonon, e-mailben továbbítani
- a jelszót tilos kérdőívbe, űrlapokba beírni

A felhasználóknak különös figyelmet kell fordítaniuk az alábbiakra:

- A jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti.
- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- Tilos közös jelszavakat használni.
- A jelszót nem szabad leírni és hozzáférhető helyen tárolni.
- A jelszót nem szabad telefonon vagy e-mailben továbbadni.
- Ne használjuk a programok (böngészők) jelszó megSzervezet vezetője funkcióját.
- Jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott vagy erre utaló jeleket lehet észlelni, azonnal meg kell változatni a jelszót és értesíteni kell a rendszergazdát.
- A belépéshez szükséges jelszót biztonságos helyen kell tárolni, soha nem szabad azt a számítógép közelében felírva hagyni.
- Olyan jelszót célszerű választani, amit nem könnyű kitalálni, és a jelszót gyakran meg kell változtatni.
- Óvakodni kell attól, hogy mások jelenlétében gépeljük be a jelszót.
- Amikor nincs szükség a számítógépre, ki kell kapcsolni.

Felelősök, dokumentálás

Azon informatikai rendszerek esetében, melyek támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését a szükséges szabályok, paraméterek, beállásáért a **rendszergazda** felel. A dokumentáció ebben az esetben az informatikai rendszer napló állománya.

Azon informatikai rendszerek esetében, melyek nem támogatják a jelszavakra vonatkozó alapszabályok kikényszerítését az e fejezetben meghatározott elvek szabályok betartásáért, valamint a jelszócserék dokumentálásáért **a Szervezeti egység vezetője** a felelős.

Az EIR a megfelelő Szabályzatokkal összhangban érvényesíti a jóváhagyott logikai hozzáférési jogosultságokat az információkhoz és a rendszer erőforrásaihoz.

A hozzáférési szabályokkal kapcsolatos szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági Szabályzat)* kezeli.

Információáramlási szabályok érvényesítése

A Szervezet blokkolja az olyan külső forgalmat, amely úgy tűnik, mintha az érintett Szervezeten belülről származna, a belső web proxy szerveren kívüli webes kéréseket korlátozza.

Információáramlási szabályok érvényesítése - Titkosított információk áramlásának irányítása

A szervezet szükség szerint az információk dekódolásával, a titkosított információáramlás blokkolásával vagy a titkosított információk átvitelével próbálkozó kommunikációs folyamat megszakításával megakadályozza, hogy titkosított információkkal megkerüljék a meghatározott információáramlás-ellenőrzési mechanizmusokat.

A felelősségek szétválasztása

A Szervezetben a felelősségek szétválasztása magában foglalja az üzleti funkciók és a támogató funkciók különböző személyek, szerepkörök, Szervezeti egységek közötti megosztását, az IT üzemeltetési és IT üzemeltetés-ellenőrzési funkciók különböző személyek, szerepkörök, Szervezeti egységek közötti megosztását, a rendszertámogatási funkciók különböző személyekkel történő elvégzését, valamint annak biztosítását, hogy a hozzáférés-felügyeleti funkciókat kezelő biztonsági személyzet ne kezelje az ellenőrzési funkciókat is.
Így a Szervezet vezetője az EIR-rel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- szétválasztja az egyéni felelősségeket;
- munkakörökben és megbízásokban dokumentálja az egyéni felelősségek szétválasztását;
- meghatározza az elektronikus információs rendszer hozzáférés jogosultságait az egyéni felelősségek szétválasztása érdekében.

Legkisebb jogosultság elve

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi. A Szervezet vezetője a rendszergazda segítségével, munkakör változáskor mindig, de évente legalább egyszer felülvizsgálja a kiosztott jogosultságokat és szükség esetén megszünteti a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat.

Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz

A Szervezet vezetője kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonsági funkciókhoz. A Szervezet vezetője kizárólag az általa meghatározott személyeknek vagy szerepköröknek engedélyez hozzáférést a biztonságkritikus információkhoz. A hozzáféréseket a munkakörük vagy megbízásuk tartalmazza.

Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz

A Szervezet vezetője kötelezővé teszi, hogy a Szervezet 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.

Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz

A hálózati hozzáférés engedélyezésekor gondosan mérlegelnie kell annak kockázatait, tekintettel arra, hogy a hálózati hozzáférés engedélyezése (különösen a privilegizált funkciókhoz) növelheti a biztonsági kockázatokat. Csak kényszerű üzemeltetési okokból engedélyezhető a hálózati hozzáférés a meghatározott privilegizált parancsokhoz, és dokumentálni kell az ilyen hozzáférés indoklását a rendszerbiztonsági tervben.

Legkisebb jogosultság elve – Privilegizált fiókok

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza. A Szervezet változás esetén, de legalább évente felülvizsgálja a kiosztott jogosultságokat és szükség esetén megszünteti a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat.

Legkisebb jogosultság elve – Felhasználói jogosultságok felülvizsgálata

A Szervezet leltárt készített a kiosztott jogosultságokról. Ez magába foglalja az érintett felhasználókat, a jogosultságok fennállásának kezdetét és további, a Szervezet által meghatározott információkat. A Szervezet vezetője a rendszergazda segítségével változáskor, de legalább évente felülvizsgálja a kiosztott jogosultságokat és szükség esetén megszünteti a munkavégzéshez nem szükséges, illetve esetlegesen összeférhetetlen jogosultságokat.

Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása

E pont a Szabályzat 3.4 pontjában "Naplózható események" és a "Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel" kontrolloknál kerültek bővebben kifejtésre.

Legkisebb jogosultság elve – Nem-privilegizált felhasználók korlátozása

A nem privilegizált felhasználókkal szemben védelmet igénylő privilegizált funkciók közé tartoznak a behatolásérzékelési és -megelőzési mechanizmusok vagy a rosszindulatú kódfuttatás elleni védelmi mechanizmusok. A Szervezetben hozzárendeltük a privilegizált felhasználókat a privilegizált funkciókhoz úgy, hogy a nem privilegizált fiókok ne férjenek hozzá olyan privilegizált funkciókhoz, melyekhez nem rendelkeznek megfelelő jogosultsággal.

Sikertelen bejelentkezési kísérletek

A Szervezet korlátot alkalmaz a felhasználó meghatározott időtartamon belüli 5 egymást követő sikertelen bejelentkezési kísérleteire. Ezt túllépve az EIR-je automatikusan zárolja a felhasználói fiókot vagy csomópontot a meghatározott időtartamra, vagy ameddig a rendszergazda fel nem oldja annak zárolását, vagy késlelteti

a következő bejelentkezési lehetőséget a meghatározott algoritmus szerint. Továbbá értesíti a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.

A rendszerhasználat jelzése

Az EIR használata előtt megjelenítünk a felhasználóknak egy meghatározott rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a Szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és tartalmazza, hogy:

- A felhasználók a Szervezet EIR-ét használják.
- A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.
- A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár
- A rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti.

Az EIR mindaddig fenntartja a rendszerhasználati értesítést a képernyőn, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket a rendszerbe való bejelentkezésre vagy a rendszerhez való további hozzáférésre.

A nyilvánosan hozzáférhető rendszerek esetén az értesítés legalább az alábbiakat tartalmazza:

- A felhasználók a Szervezet EIR-ét használják.
- A rendszer használatát megfigyelhetik, rögzíthetik, naplózhatják.
- A rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár.
-

Egyidejű munkaszakasz kezelés

A szervezet vezetője, szükség szerint az EIR-ben meghatározott számra korlátozza az egyidejű munkaszakaszok maximális számát az EIR fiókokra globálisan, fióktípusonként, fiókonként, vagy az előbb felsoroltak bármely kombinációjával

Eszköz zárolása

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- kötelezi a felhasználókat, hogy 5-7 perc inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;
- megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

Eszköz zárolása – Képernyőtakarás

Az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a záró személy nevét is tartalmazhatja – el kell takarni.

A munkaszakasz lezárása

Amennyiben a Szervezet EIR-ben alkalmazható, megteremti azokat a feltételeket, amelyek alapján az EIR automatikusan lezárja a felhasználói munkaszakaszt. Ezek a feltételek tartalmazhatják a felhasználói inaktivitás meghatározott időszakait, célzott válaszokat bizonyos típusú biztonsági eseményekre, vagy a rendszerhasználat időbeli korlátozásait.

Biztosítja, hogy az EIR képes legyen lezárni a munkaszakaszt anélkül, hogy megszakítaná a hálózati kapcsolatokat.

Úgy állítja be az EIR-t, hogy a munkaszakasz lezárása után minden, a felhasználói munkaszakaszhoz kapcsolódó folyamatot leállít, kivéve azokat, amelyeket a felhasználó kifejezetten arra hozott létre, hogy a munkaszakasz lezárása után is folytatódjanak.

Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Nincsenek olyan felhasználói tevékenységek, melyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül végre lehetne hajtani.

Távoli hozzáférés

A Szervezetben csak biztonságos távoli hozzáférés engedélyezett, amely az érintett Szervezet EIR-jéhez kapcsolódik és amely külső hálózatokon, például az interneten keresztül kommunikál. A Szervezet jellemzően titkosított virtuális magánhálózatokat (Teamyouver, VNC) használ a távoli kapcsolatok bizalmasságának és integritásának megőrzése érdekében

Távoli hozzáférés – Felügyelet és irányítás

A Szervezet - a távoli hozzáférési módok felügyeletére és ellenőrzésére, a támadások észlelésére - naplózza a távoli felhasználók kapcsolódási tevékenységeit a különböző rendszerelemeken, beleértve a szervereket, hordozható számítógépeket, munkaállomásokat, okostelefonokat és táblagépeket.

Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által

A Szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében.

Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok

A Szervezet a távoli hozzáféréseket engedélyezett és menedzselt hálózati hozzáférés-felügyeleti pontokon keresztül irányítja.

Távoli hozzáférés – Privilegizált parancsok és hozzáférés

A Szervezet biztosítja, hogy a távoli hozzáférés csak a meghatározott követelményeknek megfelelően lehetséges. Ez magában foglalhatja a kétlépcsős azonosítást, a biztonsági protokollok használatát, és a hozzáférés korlátozását pl.: csak bizonyos IP-címekről vagy eszközökről lehet bejelentkezni. Csak olyan módon engedélyezi a távoli hozzáférést, amely értékelhető bizonyítékot szolgáltat a privilegizált jogosultságot igénylő műveletek végrehajtásához és a biztonságkritikus információk eléréséhez a meghatározott követelményeknek megfelelően és a távoli hozzáférés indokoltságát a rendszerbiztonsági tervben dokumentálja.

Vezeték nélküli hozzáférés

A Szervezet épületeiben vezeték nélküli hálózatához hozzáférést a Szervezet vezetője engedélyével lehet csak létesíteni, illetve igénybe venni. Kivételt képez ez alól – amennyiben az adott telephelyen elérhető – a Szervezet által biztosított, a Szervezet hálózatáról leválasztott, szeparált nyilvános hálózati hozzáférés (pl.: „vendég" wifi), amelyhez a Szervezet munkatársai is csatlakoztathatják saját mobil eszközeiket.

Szervezeti munkavégzés céljára biztosított vezeték nélküli hálózat hozzáférés védelemmel (minimum jelszavas védelemmel) ellátottan és a csatlakoztatható eszközök – például fizikai hálózati címének (MAC address filter) – szűrésével létesíthető.

A Szervezet vezetője:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki a vezeték nélküli technológiák kapcsán;
- engedélyezési eljárást folytat le a vezeték nélküli hozzáférés feltételeként.

Vezeték nélküli hozzáférés – Hitelesítés és titkosítás

A Szervezetben az EIR-ben titkosítással és a felhasználók vagy az eszközök hitelesítésével védi a vezeték nélküli csatlakozás során a hozzáférést.

Vezeték nélküli hozzáférés – Vezeték nélküli hálózat letiltása

A Szervezet minden olyan a rendszerelemekbe ágyazott vezeték nélküli hálózati hozzáférést letilt, amennyiben annak használata nem szükséges.

Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása

A szervezet azonosítja és külön engedélyezési eljáráson keresztül jogosítja fel azokat a felhasználókat, akik jogosultak a vezeték nélküli hálózati funkciók önálló konfigurálására.

Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény

A szervezet olyan rádióantennákat választ ki, alkalmaz és az átviteli teljesítményszinteket oly módon kalibrálja, hogy minimalizálja annak valószínűségét, hogy a vezeték nélküli hozzáférési pontok jelei a szervezet által ellenőrzött határokon túl is foghatók legyenek.

Mobil eszközök hozzáférés-ellenőrzése

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- az engedélyezési és jogosultsági szabályozásában felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre;
- engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás

A Szervezet vezetője teljes eszköztitkosítást, tároló alapú titkosítást vagy más technológiai eljárást alkalmaz az általa meghatározott mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, vagy az információk hozzáférhetetlenné tételére.

Külső elektronikus információs rendszerek használata

A Szervezet vezetője és a külső rendszer működtetője meghatározta, hogy

a) milyen feltételek és szabályok betartása mellett jogosult a felhasználó egy külső rendszerből hozzáférni az elektronikus információs rendszerhez;

b) külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Szervezet által ellenőrzött információkat.

c) külső szolgáltató a Szervezeti rendszeren, azonosítatlan és engedéllyel nem rendelkező tevékenységet nem végezhet.

d) A Szervezet, a külföldi felhő-alapu tárhelyszolgáltatást a nemzeti adatvagyon védelme érdekében fokozott odafigyeléssel és előzetes vizsgálattal vesz igénybe.

Külső rendszerek használata – Engedélyezett használat korlátozásai

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által 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.

Külső rendszerek használata – Hordozható adattárolók használatának korlátozása

A Szervezet vezetője egyedileg korlátozza ill. szükség szerint megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső rendszerekben.

Információmegosztás

A szervezeti információk a szerződések bizalmas információi, a speciális hozzáférésű programokhoz vagy fiókokhoz kapcsolódó minősített információk, a privilegizált információk, a szervet által védett információk és a személyes adatok. Védelmi szintjüket az információk besorolásával oldjuk meg (nyilvános, bizalmas, titkos).

A Szervezet elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói

mérlegelés szóba jöhet. A Szervezet meghatározza az információ tartalma, típusa, biztonsági kategóriája vagy speciális hozzáférési programja vagy fiókja alapján, hogy kivel és hogyan osztható meg. Az információhoz történő hozzáférési korlátozások magukban foglalhatják a titoktartási megállapodásokat.

Nyilvánosan elérhető tartalom

A Szervezet vezetője

a) kijelöli a Szervezet vezető beosztású munkatársát, aki jogosult a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Szervezettel kapcsolatos bármely információ közzétételére. A Szervezetben csak a Szervezet vezetője által engedélyezett információkat lehet közzétenni. Minden más információ közzététele TILOS!

b) a kijelölt személyt képzésben részesíti annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános információkat;

c) közzététel előtt átvizsgálja a javasolt tartalmat;

d) meghatározott gyakorisággal átvizsgálja a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolítja azokat;

e) a Szervezet vezetője nyilvánosan elérhető rendszerként definiálja például a Szervezet publikus weboldalát;

f) a publikus felületeken való közzétételt és a médiával való kommunikációt a Szervezet vezetője szabályozza, a Szervezet külső kommunikációjáért a Szervezet vezetője a felelős.

g) a Szervezeti honlap (domaine.hu) tartalommenedzsmentjét egy külsős megbízott, megbízási szerződés keretében végzheti;

h) a Szervezeti ügyintézéssel kapcsolatos dokumentációk, határozatok, rendeletek a Szervezet vezetőjének jóváhagyását követően kerülnek nyilvánosságra;

i) a publikált információk csak nyilvános adatokat és információkat tartalmazhatnak.

A Szervezet vezetője legalább évente áttekinti a honlapot és nem nyilvános adat kikerülése esetén eltávolítatja azt.

Az Információbiztonsági felelős időszakos ellenőrzés keretében szintén ellenőrzi a honlap jogszabályoknak való megfelelését.

Amennyiben a Szervezeti honlap, külsős adatokat felhívásokat, egyéb információkat tartalmaz, annak valódiságtartalmáért a külsős által megadott (vagy felhelyezett) adatok tartalmáért a külsős tárhelybérlő a felelős. A jogszabályba vagy közerkölcsbe ütköző adatok információk kihelyezését megtagadjuk.

3.3 Tudatosság és képzés

A Szervezet vezetője biztosítja

- hogy a felhasználók rendelkezzenek a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel;

- a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását,
- mely képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az óvintézkedéseket, valamint az informatikai eszközök helyes használatát, az Információbiztonsági előírtakat;
- hogy a felhasználók ismerjék a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is minimálisra csökkentség a lehetséges biztonsági kockázatokat, és alá kell írniuk az erről szóló nyilatkozatot;
- hogy minden felhasználónál tudatos legyen abban, hogy a biztonsági szabályok megsértése szankciókkal jár.

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a képzéssel kapcsolatos eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Szervezet képzésével kapcsolatos egyéb szabályokat egy külön dokumentumban *(Képzési Szabályzat)* kezeli.

Szerepkörök, felelősségek, szabályzat és eljárásrendek

A Szervezet vezetője rendszeres gondoskodik az információs rendszer felhasználóinak rendszeres képzéséről. A képzések gyakoriságát az információs rendszerek változásainak és egyéb igényeknek a figyelembevételével határozza meg, de évente legalább egyszer belső oktatáson vesz részt minden munkavállaló. A Szervezetbe újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben részesítik. Rendkívüli oktatást tart a Szervezet rendszereiben történő jelentős változás vagy a Szervezet rendszereiben történő incidens után.

A Szervezet vezetője:

a) felelős a képzési kritériumok meghatározásáért

b) biztosítja a képzéshez a szükséges erőforrásokat

c) gondoskodik a képzések fontosságának tudatosításáról a teljes Szervezetben

Az IBF:

a) felelős a képzési rendszer kialakításáért, fenntartásáért

b) felelős a szükséges oktatások megtartásáért, megtartatásáért

A munkatársak:

a) felelősek a képzési előírások betartásáért, a képzések során leadott anyagok elsajátításáért

Biztonságtudatossági képzés

A Szervezet vezetőjének felelőssége, hogy a Szervezet elektronikus információs rendszereinek felhasználói biztonságtudatossági képzések formájában megismerjék az alapvető biztonsági követelményeket. A biztonságtudatossági képzés az új felhasználók esetén már a kezdeti képzés részét képezi, továbbá a képzést legalább évente megismételjük, illetve minden olyan elektronikus információs rendszerben vagy munkakörben történő változás esetén, mely ezt indokolttá teszi.

A képzés

- felhívja a munkatársak figyelmét az Információbiztonsági Szabályzati rendszerben bekövetkezett változásokra;
- ismerteti azokat a sebezhetőségeket, melyek a felhasználó nem-biztonságtudatos magatartását használják ki;
- ismerteti az azonosított, súlyosnak minősített szabálysértéseket;
- felhívja a figyelmet, hogy a megadott súlyos szabálysértések ismételt elkövetése milyen szankciókat von maga után.
- a Szabályzatokban, jogszabályokban, szerződésekben előírt követelmények felfrissítése érdekében ismerteti a betartandó szabályokat, kötelezettségeket, egy-egy az oktatásra kijelölt biztonsági terület esetében (pl. hozzáférés védelem témakörében a jelszókezelési szabályok stb.).

Az oktatásokon való részvétel kötelező a Szervezet informatikai rendszereihez hozzáférők számára, amely jelenlétet az oktatás végén szükség szerint a jelenléti ív aláírásával igazolnak.

Biztonságtudatossági képzés – Belső fenyegetés

A Szervezet vezetője a biztonságtudatossági képzések részeként, hangsúlyt helyez az érintett személyeknek a belső fenyegetések felismerésére való felkészítését, hogy tudatosítsa jelentési kötelezettségüket. A képzésben és tudatosításban hangsúlyt fektetünk arra, hogy a hibákat, incidenseket ne titkolják el, hanem jelentsék a Szervezet vezetőjenek.

Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés

A Szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére. A pszichológiai manipuláció magában foglalja az adathalászatot, a nyílt információ felhasználásával végrehajtott megszemélyesítést (pretexting), a megszemélyesítést, a csalizást (baiting), az ajándékozást bejelentkezési adatokért cserébe (quid pro quo), a témaeltérítést (thread-jacking), a közösségi média oldalakon található információk kártékony célra történő felhasználását (social media exploitation) és a szoros követést (tailgating)

Szerepkör alapú biztonsági képzés

A Szervezet minden, munkaköri feladatai ellátása során valamely általa használt EIR felhasználására kötelezett munkavállalója számára biztosítja feladatainak és szerepkörének megfelelő mértékben az adott EIR felhasználására, annak biztonsági követelményeire vonatkozóan rendelkezésre álló információkat, dokumentációkat, továbbá az ezzel kapcsolatban esetlegesen elérhető (pl.: központi üzemeltető által biztosított) képzésen történő részvételt.

A szerepköralapú képzést igénylő szerepek közé tartoznak a vezetők vagy a menedzsment tagjai, EIR tulajdonosok; engedélyező tisztviselők; biztonsági tisztviselők; adatvédelmi tisztviselők; beszerzési tisztviselők; rendszer tervezőmérnökök; rendszermérnökök; szoftverfejlesztők; biztonsági mérnökök; rendszer-, hálózati és adatbázis-adminisztrátorok; központi naplózás adminisztátorai; konfigurációkezelési tevékenységeket végző személyek; ellenőrzési tevékenységeket végző személyek; rendszerszintű szoftverhez hozzáféréssel rendelkező személyek; vészhelyzeti és

biztonsági eseménykezelési feladatokat ellátó személyek; adatvédelmi feladatokat ellátó személyek; és személyes adatokhoz hozzáféréssel rendelkező személyek

Új rendszer bevezetése esetén a Szervezet vezetője felelőssége a felhasználók oktatásának biztosítása. Az új rendszerhez hozzáférés csak azoknak a felhasználóknak adható, akik részesültek a képzésben és ezt aláírásukkal igazolták.

A biztonsági eseményekből és az auditokon levont tanulságokat, be kell építeni az oktatásokba az adott munka, vagy szerepkör szerint. Ezeknek a megtétele az IBF feladata.

A biztonsági képzésre vonatkozó dokumentációk

A Szervezet dokumentálja és egyúttal nyomonköveti az általános- és a szerepkör alapú biztonságtudatossági képzéseket. A dokumentálás magában foglalhatja magát a képzési anyagot, illetve a képzés lebonyolításával kapcsolatos egyéb dokumentációkat is pl.: jelenléti ívek használata, automatikusan generált részvételi igazolás.

A Szervezet a vonatkozó hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat figyelembe véve meghatározott ideig őrzi meg a képzésről készült dokumentumokat.

3.4 Naplózás és elszámoltathatóság

Naplózás és elszámoltatthatóság Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a naplózással kapcsolatos eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A szervezet vezetője kinyilvánítja, hogy a naplózás az incidensek és ezáltal a szervezettel kapcsolatos támadások mind a megelőzés mind a felderítés szempontjából egyik létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére. A szervezet vezetője, a naplózás megfelelőségi kritériumainak megállapítására két célt tűzött ki. A tervezett naplóellenőrzések végrehajtása (mérőszám 100%) és a sikeres nem felderített incidensek száma, ami a naplóelemzésből kiderült volna (0%).

A Szervezet a naplózással kapcsolatos egyéb szabályokat egy külön dokumentumban (*Naplózási Szabályzat)* kezeli.

Naplózható események

A Szervezet kialakítja az informatikai rendszerek naplózási rendszerét (Windows naplófájlok, adatbázisok log fájlok), hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét. A naplózási rendszer kialakítása rendszergazda feladata. A naplóellenőrzéseket is a rendszergazda vizsgálja felül, az IBF ellenőrzése mellett. A naplózással kapcsolatos eljárások és elszámoltathatóság felülvizsgálatát meg kell tenni minden incidens, audit, esetén, de legalább évente egyszer. A szervezet egyszerű struktúrájából adódóan a naplózási tevékenység a rendszergazda feladata és kiterjed a teljes szervezetre. Nem tagolódik egységekre, és így nem szükséges egységek közötti összehangolásra, együttműködésre.

A Szervezet vezetője az érintett elektronikus információs rendszerre vonatkozó rendszerbiztonsági tervben

a) meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;

b) egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő Szervezeti egységgel, hogy növelje a kölcsönös támogatást és hogy iránymutatással segítse a naplózható események kiválasztását;

c) megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához;

d) a számon kérhetőség és hibakezelés biztosítása érdekében az informatikai eszközöknek az informatikai rendszer működéséről és különösen az Információbiztonsági eseményekről helyi naplóállományt generál;

e) felelősséget vállal, hogy a kialakított naplózási rendszer a szükséges mértékben biztosítsa a számon kérhetőséget és az auditálhatóságot, tegye lehetővé a bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, melyek a rendszer biztonságát érintik;

f) ha másként nem rendelkezik, az informatikai eszközök minimálisan az alapértelmezett naplózási beállítások szerinti eseményeket naplózza. Az adott informatikai eszköz üzemeltetéséért felelős személy, ha azt az üzemeltetési, üzemeltethetőségi szempontok indokolják saját hatáskörben módosíthatja az alapértelmezett naplóbeállításokat, az Szervezet vezetője tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel vizsgáltatja. Meghibásodás esetén a naplóállományok vizsgálata a hibajavításban eljáró üzemeltető feladata.

Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekből gyűjt elegendő információt ahhoz, hogy ki lehessen mutatni, milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

A naplóbejegyzések minimális tartalma:

- milyen típusú esemény történt;
- mikor történt az esemény;
- hol történt az esemény;
- miből származott az esemény; és
- mi volt az eseménynek a kimenetele, valamint
- az eseményhez kapcsolódó személyek, alanyok, objektumok.

Naplóbejegyzések tartalma – Kiegészítő naplóinformációk (opciós követelmény)

Az EIR a naplóbejegyzésekben további, a Szervezet által meghatározott kiegészítő információkat is rögzíthet.

Az EIR-t úgy alakítja ki, hogy képesek legyenek a naplóbejegyzésekben a minimálisan elvárt információkon túl kiegészítő információk hozzáadására is, azért, hogy

- a Szervezet megfontolás után további információk hozzáadását tegye lehetővé a naplóbejegyzésekhez, (beleértve, de nem kizárólag, az alkalmazott hozzáférés-

felügyeleti szabályokat vagy az adatáramlási szabályokat, valamint a csoportfiókok felhasználóinak egyéni azonosítóit).
- a Szervezet megfontolhassa a kiegészítő naplóbejegyzési információ korlátozását csak azokra az információkra, amelyekre kifejezetten szükség van a naplózási követelmények teljesítéséhez.

Naplózás tárkapacitása

A Szervezet elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket. A tárhelyigényeket a rendszergazda jelzi a Szervezet vezetőjének, aki gondoskodik a fejlesztés forrásainak biztosításáról.

Naplózási hiba kezelése

A Szervezet kialakít egy naplózási hibakezelő megoldást, amely képes azonosítani a naplózási tevékenységhez kapcsolódó szoftver- és hardverhibákat, vagy a naplóbejegyzések rögzítési mechanizmusának hibáit, hogy egy esetleges naplózási hiba esetén:

- riasztja a meghatározott személyeket vagy szerepköröket,
- a Szervezet által meghatározott időn belül,
- szükség szerint további meghatározott intézkedéseket hajt végre.

Naplózási hiba kezelése - Tárhelykapacitás figyelmeztetés

A szervezet által működtetett EIR- naplózását úgy állítja be, hogy amikor a naplózási tárhelye eléri a maximális kapacitás egy bizonyos százalékát, meghatározott időn belül figyelmezteti a Rendszert működtető rendszergazdát.

Naplózási hiba kezelése - Valós idejű riasztások

A szervezet által működtetett EIR-t (amennyiben az ezt a funkciót tudja) úgy állítja be, hogy az riasztást küld a rendszert üzemeltető rendszergazdának, ha a meghatározott, valós idejű riasztást igénylő hibaesemények közül bármelyik bekövetkezik. Ezáltal minimalizálni lehessen a lehetséges károkat.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

A Szervezet felülvizsgálja, elemzi és jelentést készít a Szervezet által végzett információbiztonsági naplózás eredményéről (beleértve a fiókok használatának, távoli hozzáférésnek, vezeték nélküli kapcsolatnak, mobil eszköz csatlakozásnak, konfigurációs beállításoknak, a rendszerkomponens leltárának, karbantartó eszközök használatának és nem helyi karbantartásnak, fizikai hozzáférésnek, hőmérsékletnek és páratartalomnak, berendezések szállításának és eltávolításának, az EIR interfészeinél történő kommunikációnak, valamint a mobil kód vagy az internetes hanghívás (VoIP) használatának monitorozásából eredő naplózást). Az eredményeket a Szervezet vezetője és szükség szerint az IBF vizsgálja.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Automatizált folyamatintegráció

A Szervezet automatizált mechanizmusokat (például a SIEM) használ az incidenskezelés, folyamatos felügyelet, üzletmenet-folytonosságra vonatkozó

eljárásrend, gyanús tevékenységek kivizsgálása és az azokra adott válaszok naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Naplózási tárhelyek összekapcsolása

A Szervezet összegyűjti a különböző tárhelyeken található naplóbejegyzéseket (az EIR által generált naplóbejegyzéseket, a hálózati forgalommal kapcsolatos naplóbejegyzéseket, az alkalmazások által generált naplóbejegyzéseket, valamint az egyes adatbázisok által generált naplóbejegyzéseket is) hogy azonosítsa a mintázatokat, a rendellenességeket és a potenciális biztonsági fenyegetéseket. A Szervezt törekszik arra, hogy implementálni tudjon egy naplóelemző eszközt vagy szolgáltatást (pl.: SIEM rendszer) amely képes összegyűjteni, elemezni és összekapcsolni a naplóbejegyzéseket.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Felügyeleti képességek integrálása

A szervezet egyesíti a naplók elemzését a sérülékenységmenedzsment során keletkezett információkkal, a teljesítményadatokkal, a rendszerfelügyeleti információkkal vagy egyéb forrásokból begyűjtött információkkal a nem megfelelő vagy szokatlan tevékenységek azonosításának javítása érdekében.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Összevetés a fizikai felügyelettel

A szervezet összeveti a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert adatokkal, a szokatlan, nem odaillő, gyanús vagy rosszindulatú tevékenységek azonosítására vonatkozó képességek fejlesztése érdekében.

Naplóbejegyzések csökkentése és jelentéskészítés

A Szervezet biztosítja, egy naplócsökkentési megoldással, amely képes manipulálni a gyűjtött naplóinformációkat és egy összefoglaló formátumba szervezni azokat, hogy így könnyebben értelmezhetők és testre szabható jelentéseket generálók legyenek az elemzők számára.

Naplóbejegyzések csökkentése és jelentéskészítés – Automatikus feldolgozás

A Szervezet gondoskodik arról, hogy a naplóbejegyzések automatikusan feldolgozhatók, rendezhetők és kereshetők legyenek a meghatározott adatmezők tekintetében.

Időbélyegek

A Szervezet vezetője a Szervezet által üzemeltetett rendszereknél és hálózatnál, elektronikus információs rendszer belső rendszerórákat követel meg a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a Szervezet által meghatározott időmérési pontosságnak.

Naplóinformációk védelme

A Szervezet vezetője a Szervezet által üzemeltetett rendszereknél fizikai és logikai követelmények támasztásával, megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A naplóbejegyzések hozzáférését úgy kell kialakítani, hogy ahhoz, csak a Rendszergazda férhessen hozzá. Megsemmisülés esetén, mentésből visszaállítható legyen, melyet szintén csak a Rendszergazda végezhet el. Mivel a rendszergazda kizárólagos hozzáféréssel rendelkezik a napló információkhoz, így a szervezet nem alkalmaz automatikus riasztási információt jogosulatlan napló hozzáférések esetén.

Naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken

A szervezet a saját működtetésű EIR-nél törekszik a naplóbejegyzéseinek tárolását egy olyan tárhelyen tartani, amely fizikailag elkülönült az EIR-től vagy a rendszerelemeitől. Ezzel segít biztosítani, hogy az EIR kompromittálása ne eredményezze a naplóbejegyzések kompromittálását.

Naplóinformációk védelme – Kriptográfiai védelem

A szervezet kriptográfiai eszközöket alkalmaz a naplóinformációk és a naplókezelő eszköz sértetlenségének védelmére.

Naplóinformációk védelme – Privilegizált felhasználók hozzáférése

A Szervezet vezetője a naplózási funkciók kezeléséhez csak egy meghatározott jogosultsági szinttel rendelkező felhasználói csoportnak vagy felhasználói szerepeknek ad hozzáférési jogosultságot, hogy azok személyek vagy szerepkörök, akik privilegizált hozzáféréssel rendelkeznek egy rendszerhez, és akik egyben az adott rendszer által végzett naplózás tárgyát is képezik, ne befolyásolhassák a naplózási információk megbízhatóságát.

Letagadhatatlanság

A szervezet szükség szerint különböző technikákat vagy mechanizmusokat, (pl. digitális aláírások és digitális üzenetátvételi elismervények) alkalmaz a letagadhatatlanságot elősegítésére. Így bizonyítékot szolgáltat arra, hogy egy személy vagy a nevében futó feldolgozási folyamat végrehajtott egy a szervezet által meghatározott, a letagadhatatlanság követelménye alá eső tevékenységet.

Naplóbejegyzések megőrzése

A Szervezet vezetője a Szervezet által üzemeltetett rendszereknél a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett Szervezeten belüli információ megőrzési követelményeknek megfelelő – időtartamig összhangban a naplótárhelyek kapacitásával, megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében. A szervezetben alapértelmezésben a naplóbejegyzések nem törlődnek. Megőrzési időre vonatkozóan nincs elvárt határidő.

Naplóbejegyzések létrehozása

A Szervezet vezetője a Szervezet által üzemeltetett rendszereknél:

a) biztosítja a naplóbejegyzés generálási lehetőségét a meghatározott, naplózható eseményekre;

b) lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;

c) naplóbejegyzéseket állít elő a szükséges eseményekre, a meghatározott tartalommal.

A dolgozókat a belépéskor, és az éves oktatás keretében tájékoztatjuk, hogy mit, mikor, hogyan miért, naplózunk. Tájékoztatjuk, hogy ehhez nem kell engedély, csak tájékoztatás. Indokoljuk, hogy a Szervezeti EIR-eket, csak Szervezeti tevékenységgel kapcsolatban, munkára lehet használni. Továbbá tájékoztatjuk a jogszabályban biztosított jogairól.

Naplóbejegyzések létrehozása – Az egész rendszerre kiterjedő és időbeli naplózási nyomvonal

A szervezet által működtetett EIR amennyiben ezt a funkciót támogatja, a szervezet által meghatározott rendszerelemekből származó naplóbejegyzésekből egy rendszerszintű naplót állít össze, amely a szervezet által meghatározott tűréshatáron belüli időbélyegek alapján kerül összekapcsolásra.

Naplóbejegyzések létrehozása – Felhatalmazott személyek változtatásai

A szervezet által működtetett EIR amennyiben ezt a funkciót támogatja, szükség szerint lehetőséget biztosít a rendszert működtető rendszergazdának, hogy megváltoztassa az egyes rendszerelemek naplózását a meghatározott eseménykritériumok alapján egy meghatározott időtartamon belül. Ezzel könnyítve a naplócsökkentést, az elemzést és a jelentéstételt.

3.5 Értékelés, engedélyezés és monitorozás

Biztonságértékelési szabályok, Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti az értékelés, monitorozás ellenőrzési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A szabályokat minden rendkívüli esemény, incidens, auditok alakalmával de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást az IBF végzi a rendszergazdával a management döntései alapján.

A Szervezet az értékeléssel, engedélyezéssel és monitorozással kapcsolatos egyéb szabályokat egy külön dokumentumban (*Biztonságértékelési Szabályzat)* kezeli.

Biztonsági értékelések

A Szervezet vezetője megköveteli a szerződésekben, hogy a védelmi intézkedések értékelői többek közt az IBF és az EIR-t működtető informatikus, vagy rendszergazda rendelkezzenek a szükséges készségekkel és technikai szakértelemmel a hatékony értékelési tervek kidolgozásához és a rendszerspecifikus, hibrid, közös (több Szervezetet érintő, ágazati stb.) és az információbiztonsági irányítási rendszert érintő védelmi intézkedések értékelésének elvégzéséhez. Így pl. a kockázatkezelési koncepciók és

megközelítések általános ismerete, valamint a hardver, szoftver és firmware rendszerelemek átfogó ismerete és tapasztalata. Továbbá megköveteli, hogy az EIR-ek és az EIR-ekhez kapcsolódó szoftverek, hardverek beszerzésénél, dokumentált biztonsági értékelést végezzenek, az engedélyezés során.

Biztonsági értékelések – Független értékelők

A Szervezet vezetője független értékelőket vagy értékelőcsoportokat alkalmaz az EIR védelmi intézkedéseinek értékelésére. Független értékeléseket a Szervezeten belüli szereplők is végezhetnek, vagy a Szervezeten kívüli köz- vagy magánszektorbeli Szervezetekkel köthetnek szerződést.

Biztonsági értékelések – Kiberbiztonsági audit

A Szervezet vezetője a vonatkozó tv-ek szerint - kiberbiztonsági követelményeknek való megfelelés bizonyítására kétévente a tevékenység végzésére jogosult, független auditor (a továbbiakban: auditor) által kiberbiztonsági auditot végeztet.

Biztonsági értékelések – Speciális értékelések

A szervezet szükség szerint a védelmi intézkedések értékelése céljából rendszeresen bejelentett, vagy bejelentés nélküli:

- mélységi monitorozást végezhet;
- biztonsági berendezéseket alkalmazhat;
- automatizált biztonsági teszteseteket hajthat végre;
- sérülékenységszkennelést végezhet;
- rosszhiszemű felhasználó teszteket hajthat végre;
- belső fenyegetettség értékelést végezhet;
- teljesítmény- és terhelési teszteket hajthat végre;
- adatvesztés vagy adatszivárgás értékelést végezhet;
- a szervezet által meghatározott egyéb biztonsági értékeléseket végezhet.

Információcsere

A Szervezet vezetője az EIR-ek információcseréje során, figyelembe veszi az új vagy megnövekedett fenyegetésekkel kapcsolatos kockázatokat, amelyek akkor merülhetnek fel, amikor az EIR-ek más rendszerekkel cserélnek információt, amelyek eltérő biztonsági követelményekkel és védelmi intézkedésekkel rendelkeznek. Ez magába foglalja a Szervezeten belüli és a Szervezeten kívüli rendszereket is. Így:

- szabályozza az információcserét az EIR és más rendszerek között,
- dokumentálja az EIR interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét,
- rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat,
- figyelembe veszi a kockázatot,
- ha az EIR-eknek ugyanaz az engedélyező tisztviselője, akkor nem készítünk megállapodásokat. De a rendszerek közötti interfész jellemzőit a megfelelő biztonsági tervekben rögzítjük.
- Az esetleges külső megállapodásokat évente felül kell vizsgálni és az eredmény tükrében a vezetés dönt a hosszabbításról.
- A támadásokkal kapcsolatos információkat a szervezet megossza a kijelölt hatóságok CSIRT-el, de erre vonatkozó megállapodások nincsenek rögzítve.

Információcsere – Átviteli engedélyek

A szervezet annak megelőzése érdekében, hogy jogosulatlan személyek és rendszerek információtovábbítást végezzenek a védett rendszerekben, szükség szerint a védett rendszert független eszközökkel ellenőrzi, hogy az információtovábbítást megkísérlő személy vagy rendszer jogosult-e erre. Az adattovábbítás elfogadása előtt gondoskodik róla és ellenőrzi, hogy a kapcsolódó rendszerek között adatokat továbbító személyek vagy rendszerek rendelkeznek-e az adatátvitelhez szükséges jogosultságokkal. (pl.: hitelesített SMTP-továbbítók)

Az intézkedési terv és mérföldkövei

A Szervezet vezetője és az IBF olyan intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására. Így a Szervezet, előre meghatározza azokat a lépéseket, amelyeket meg kell tennie annak érdekében, hogy kijavítsa az EIR védelmi intézkedéseinek értékelése során feltárt gyengeségeket vagy hiányosságokat, valamint csökkentse vagy megszüntesse az EIR ismert sérülékenységeit.

Engedélyezés

A Szervezet vezetője maga látja el (eseteként átruházza) az engedélyezésért felelősi feladatokat, aki az EIR-ért felel. Maga látja el azt a felelősi feladatot, aki a Szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel. Maga biztosítja, hogy az EIR használatbavételét megelőzően:

- engedélyezi a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását;
- engedélyezteti a rendszer működését.
- engedélyezi a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.
- rendszeresen felülvizsgálja(tatja) az engedélyeket.

Folyamatos felügyelet

A Szervezet vezetője kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a Szervezeti szintű stratégiával összhangban. A folyamatos felügyelet eredményeként az IBF kockázatkezelési intézkedéseket hajt végre, mikor több olyan, funkció alapján csoportosított védelmi intézkedés hatékonyságát felügyelik, akkor a problémás védelmi intézkedések esetén, a problémát kiváltó okok elemzésre is szükség lehet.

Folyamatos felügyelet – Független értékelés

A Szervezet vezetője a független értékelést alkalmaz (külső auditor megbízásával és külső IBF megbízásával) az EIR-ben lévő védelmi intézkedések folyamatos ellenőrzésére.

Folyamatos felügyelet – Kockázatmonitorozás

A Szervezet vezetője biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:

- a hatékonyság ellenőrzését;
- a megfelelés ellenőrzését;

- a változások nyomon követését.

Folyamatos felügyelet – Független szakértő vagy csapat

A szervezet szükség szerint, független szakértőt vagy csapatot alkalmaz az EIR vagy a rendszerelemek behatolásvizsgálatának elvégzésére. (Pl. ilyen biztonsági intézkedésnek lehet tekinteni NBSZ NKI, vagy az arra jogosult gazdálkodó szervezet által végrehajtott Ibtv. szerinti sérülékenységvizsgálatot, amennyiben az magába foglalta a behatolásvizsgálatot is.)

Belső rendszerkapcsolatok

A Szervezet vezetője engedélyezi a Szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását. Belső rendszerkapcsolatok részét képezhetik mobiltelefonok, notebookok és asztali számítógépek, tabletgépek, nyomtatók, másolók, faxgépek, szkennerek, szenzorok és szerverek. Az érintett Szervezet a belső rendszerkapcsolatokat nem különálló esetenként hagyja jóvá, hanem közös jellemzőkkel és/vagy konfigurációval, valamint interfésszel rendelkező kategóriákkal dolgozik, beleérte a meghatározott feldolgozási, továbbítás és tárolási képességekkel rendelkező nyomtatókat, szkennereket és másolókat, vagy a specifikus alapkonfigurációval rendelkező okostelefonokat és táblagépeket Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét. Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat. Évente, felülvizsgálja minden belső kapcsolat további szükségességét.

3.6 Konfigurációkezelés

Konfigurációkezelési Szabályzat és eljárásrendek

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központilag tárol információkat így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a konfigurációkezelési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A szabályokat minden rendkívüli esemény, incidens, auditok alakalmával de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást az IBF végzi a rendszergazdával a management döntései alapján.

A szervezet vezetője, a konfigurációkezelés megfelelőségi kritériumainak megállapítására egy célt tűzött ki. A tervezett konfiguráció ellenőrzések végrehajtása (mérőszám 100%).

A Szervezet a konfigurációkezeléssel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Konfigurációkezelési Szabályzat)* kezeli.

Elektronikus információs rendszerek nyilvántartása

A Szervezet vezetőjének a felelőssége, hogy a Szervezet teljeskörű, naprakész nyilvántartást vezessen a Szervezetben használt elektronikus információs rendszerekről. A nyilvántartás minimum tartalmazza az elektronikus információs rendszer

- nevét;
- funkcióját;
- nyújtott szolgáltatását;
- licencszámát;
- szakterületi felelőst és elérhetőségét;
- üzemeltetési felelőst és elérhetőségét;
- továbbá releváns esetben a külső elérhetőségeket.

A rendszergazda feladata a nyilvántartás elkészítése és az évente történő felülvizsgálata.

Alapkonfiguráció

A Szervezet által használt desktopok, laptopok és szerverek esetében egy alapkonfigurációs nyilvántartását készítjük el, és azt folyamatosan aktualizálunk. Az EIR alapkonfigurációi a rendszerek csatlakoztathatósági, üzemeltetési és kommunikációs szempontjait foglalják magukban. A nyilvántartás elkészítéséért és frissítéséért a rendszergazda felel.

A nyilvántartásnak legalább az alábbi tételeket kell tartalmaznia:

- alapértelmezett hardver;
- alapértelmezett operációs rendszer;
- alapértelmezetten telepítendő programok;
- alapértelmezett alkalmazott policy beállítások;
- alkalmazandó biztonsági beálltások;

Az alapkonfigurációs szabályokat minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást az IBF végzi a rendszergazdával a management döntései alapján.

Alapkonfiguráció – Automatikus támogatás a pontosság és a napra készségérdekében

Automatizált eszközök használhatók az érintett Szervezet szintjén, a Szervezeti célok és az üzleti folyamatok szintjén vagy rendszerszinten munkaállomásokon, szervereken, notebook számítógépeken, hálózati elemeken vagy mobil eszközökön. A Szervezet automatizált mechanizmus(oka)t alkalmaz az EIR naprakész, teljes, pontos és állandóan rendelkezésre álló alapkonfigurációjának karbantartására.

Alapkonfiguráció – Korábbi konfigurációk megőrzése

A Szervezet megőrzi az EIR alapkonfigurációjának a 3 darab korábbi verzióit, hogy szükség esetén lehetővé váljon az erre való visszatérés. Az alapkonfigurációk korábbi verzióinak megőrzése a visszaállítás támogatása érdekében tartalmazza a hardvert, a szoftvert, a firmware-t, a konfigurációs fájlokat, a konfigurációs nyilvántartásokat és a kapcsolódó dokumentációt.

Alapkonfiguráció – Rendszerek és rendszerelemek konfigurálása magas kockázatú területekre

A Szervezet védelmi intézkedéseket vezet be a rendszeresen utazó személyek által használt hordozható számítógépek (pl.: notebook, mobil) esetében. Az intézkedések magukban foglalják kockázatos helyek meghatározását, a rendszerelemek szükséges konfigurációinak meghatározását, illetve annak biztosítását, hogy az utazás megkezdése előtt a rendszerelemek rendeltetésszerűen legyenek konfigurálva, valamint az utazás befejezését követően a rendszerelemekre vonatkozó intézkedések alkalmazását. A speciálisan konfigurált notebookok közé tartoznak a megtisztított merevlemezzel, korlátozott alkalmazásokkal és szigorúbb konfigurációs beállításokkal rendelkező számítógépek. A hordozható eszközökre az utazásból való visszatérés után alkalmazott intézkedések közé tartozik a hordozható eszköz vizsgálata a fizikai manipuláció jeleinek feltárására, valamint a lemezmeghajtók biztonságos törlése és újbóli telepítése. A hordozható eszközökön tárolt információkkal kapcsolatban az adathordozók védelmére vonatkozó védelmi intézkedések nyújtanak iránymutatást.

A konfigurációváltozások felügyelete (változáskezelés)

Az EIR konfigurációváltozásainak felügyelete alatt a Szervezethez köthető EIR-ekre vonatkozó változási javaslatokat, azok indoklását, megvalósítását, tesztelését, felülvizsgálatát, illetve az ezek alapján elrendelt EIR-ben végrehajtott változásokat (pl.: frissítések és módosítások) érti a Szervezet. A konfigurációváltozás felügyelete magában foglalja az alapkonfigurációk, az EIR konfigurációs elemeinek, a működési eljárások, valamint a rendszerelemek konfigurációs beállításainak változásait, illetve a sérülékenységek javítását, a nem tervezett vagy engedély nélküli változásokat. Így új rendszer- vagy egyéb nagyobb frissítések esetén a Szervezet vezetője fontolóra veszi, hogy a konfiguráció ellenőrzésére vagy a változtatásokkal kapcsolatos tanácsadó testületekbe bevonja a fejlesztői terület képviselőit is. A változtatások ellenőrzése magában foglalja az EIR-ekben végrehajtott változtatások előtti és utáni tevékenységeket, valamint az ilyen változtatások végrehajtásához szükséges ellenőrzési tevékenységeket. A konfigurációváltozások felügyeletével kapcsolatos egyéb elvárások a *"Fejlesztői változáskövetés"* kontrollnál kerültek kifejtésre.

A konfigurációváltozások felügyelete - Automatizált dokumentáció, értesítés és változtatási tilalom

A szervezet a dokumentumok kiadásánál alkalmazott ellenőrző és felülvizsgáló kiadó mechanizmusokat alkalmaz:

- az EIR-ben javasolt változtatások dokumentálására;
- a jóváhagyásra jogosultak értesítése a javasolt változtatási igényekről;
- azon változások kiemelésére, amelyeket még nem hagytak jóvá vagy késedelmesen hagytak jóvá;
- a még nem jóváhagyott változások végrehajtásának megakadályozására;
- az EIR-ben végrehajtott változások teljes dokumentálására;
- a jóváhagyásra jogosultak értesítésére a jóváhagyott változtatások végrehajtásáról.

A konfigurációváltozások felügyelete – Változások tesztelése, jóváhagyása és dokumentálása

A Szervezet biztosítja, hogy a tesztelés ne zavarja a Szervezeti célokat és üzleti funkciókat támogató rendszerüzemeltetést. Így a teszteket végző személyek vagy csoportok megismerik és tudomásul veszik a biztonsági Szabályzatokat és eljárásokat, az EIR biztonsági szabályait és eljárásait, valamint a specifikus létesítményekkel vagy folyamatokkal kapcsolatos egészségügyi, biztonsági és környezeti kockázatokat. Ha az EIR-eket a teszteléshez le kell kapcsolni, a teszteket lehetőség szerint a tervezett rendszerleállások idejére kell ütemezni. Ha a tesztelés nem végezhető el az üzemi EIR-eken, a Szervezet vezetőjének kompenzációs intézkedéseket kell alkalmaznia. A Szervezet dokumentálja az EIR változtatásait, beleértve a változtatások leírását, a tesztelési eredményeket és a jóváhagyás részleteit. A dokumentációt alapesetben a rendszergazda őrzi.

A konfigurációváltozások felügyelete – Kriptográfia kezelése

A szervezet az általa meghatározott védelmi intézkedésekhez szükség szerint használ kriptográfiai mechanizmusokat. Amennyiben a rendszerelemek tanúsítványokat használnak azonosításra és hitelesítésre, akkor a folyamatban, figyelni kell a tanúsítványok lejáratát.

Biztonsági hatásvizsgálatok

A Szervezet rendszereiben csak az végezhet biztonsági hatásvizsgálatokat, aki(k) rendelkeznek a szükséges készségekkel és technikai szaktudással az EIR-ben tervezett változások, valamint a biztonsági következmények elemzéséhez. A biztonsági hatásvizsgálatok magukban foglalják a biztonsági tervek, Szabályzatok és eljárásrendek áttekintését az EIR tervezési dokumentációjának és működési eljárásainak a változások hatásának áttekintését a Szervezet ellátási láncában érintett partnereivel és az egyéb érdekelt felekkel.

Biztonsági hatásvizsgálatok – Különálló tesztkörnyezetek

Amennyiben a szervezet alkalmaz ilyet, akkor elkülönített tesztkörnyezetben vizsgálja a változtatásokat, mielőtt azokat éles rendszerben alkalmazná, keresve a biztonsági hatásokat, amelyek hiányosságokból, sérülékenységekből, kompatibilitási problémákból vagy szándékos rosszindulatból adódhatnak. Ha fizikailag elkülönített tesztkörnyezetek nem kerülnek megvalósításra, akkor logikai elkülönítést kell alkalmazni.

Biztonsági hatásvizsgálatok – Követelmények ellenőrzés

A Szervezet gondoskodik arról, hogy a rendszermódosítások után ellenőrizze, hogy a védelmi intézkedések helyesen lettek bevezetve. Az új vagy módosított biztonsági intézkedések megfelelően működnek, és hogy ezek az intézkedések biztosítják a kívánt eredményeket. Az ellenőrzés során figyelembe veszi az EIR biztonsági követelményeit. A fenti vizsgálatról készített jegyzőkönyvet és benne az ellenőrzési folyamatot – bizonyíthatóság céljából - megőrizzük.

A változtatásokra vonatkozó hozzáférés korlátozások

A Szervezet vezetője, csak a meghatározott személyeknek engedélyezi az EIR-ekhez való hozzáférést a változtatások kezdeményezése céljából. A hozzáférési korlátozások

közé tartoznak a fizikai és logikai hozzáférés-felügyeletek (az ezekre vonatkozó biztonsági követelmények *a "Hozzáférés-ellenőrzés érvényesítése"* és *"A fizikai belépés ellenőrzése"* kontrolloknál kerültek bővebben kifejtésre), a szoftverkönyvtárak, a munkafolyamatok automatizálása, az adathordozón található könyvtárak, az absztrakt rétegek (azaz a külső interfészekbe, nem pedig közvetlenül az EIR-ekbe implementált változtatások) és a változtatási időablakok (azaz a változtatások csak meghatározott időpontokban történnek).

A változtatásokra vonatkozó hozzáférés korlátozások - Automatizált hozzáférés-érvényesítés és naplóbejegyzések

Az szervezet szükség szerint naplózza a konfigurációváltozások alkalmazásához kapcsolódó rendszer-hozzáféréseket, hogy biztosítsa a konfigurációváltozások felügyeletének végrehajtását, és hogy támogassa az utólagos intézkedéseket, ha a szervezet jogosulatlan változtatásokat fedez fel. Így:

- automatizált módon érvényesíti a hozzáférési korlátozásokat, és
- automatikusan előállítja a naplóbejegyzéseket.

Konfigurációs beállítások

A Szervezet meghatározta a Szervezeti szintű, egységes konfigurációs elvárásokat, melyeket a konfigurációkezelési Szabályzatban dokumentált. A Szervezet a Szervezeti szinten meghatározott konfigurációs elvárásokból származtatja az elektronikus információs rendszerelemekben alkalmazott biztonsági konfigurációs beállításokat. Ezeknek a beállításoknak a szükséges minimum elvet kell képviselniük, összhangban az üzemeltetési követelményekkel.

A konfigurációs beállítások meghatározásához szükség szerint alkalmazzuk a központilag előírt biztonsági konfigurációs beállításokat (common secure configuration), melyek elismert, sztenderdizált és jól bevált referenciák, illetve amelyek útmutatásul szolgálhatnak az EIR biztonságos konfigurálásához pl.: biztonsági útmutatók (hardening guide/security reference guide).

A Szervezet vezetőjének feladata, hogy az EIR-kezeléséért felelős személy, elvégezze a konfigurációs beállításokat az EIR összes elemében. Ez magában foglalja a hardver, szoftver és firmware rendszerelemek beállításait, amelyek befolyásolhatják az EIR biztonsági állapotát vagy funkcionalitását pl.: rendszerleíró adatbázis (registry) beállításokat, a fiók-, fájl- vagy könyvtár beállítások, valamint a funkciók, protokollok, portok, szolgáltatások és távoli kapcsolatok beállításai.

A Szervezet vezetője az EIR-kezeléséért felelőst megbízza, hogy szükséges mértékben azonosítja, dokumentálja, majd azt elfogadja a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.

A Szervezet figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változásait a Szervezeti Szabályzatokkal és eljárásokkal összhangban.

Konfigurációs beállítások – Automatizált kezelés, alkalmazás és ellenőrzés

A szervezet az általa meghatározott automatizált mechanizmusok segítségével irányítja, alkalmazza és ellenőrzi a szervezet által meghatározott rendszerelemek konfigurációs beállításait.

Konfigurációs beállítások – Reagálás a jogosulatlan változtatásokra

A Rendszergazdának lépéseket kell tenni a szervezet által meghatározott konfigurációs beállítások jogosulatlan módosításaira válaszul. A konfigurációs beállítások jogosulatlan megváltoztatására adott válaszok közé tartozik a felelős szervezeti személyzet figyelmeztetése, a meghatározott konfigurációs beállítások visszaállítása vagy - szélsőséges esetekben - az érintett rendszerfeldolgozás leállítása. Az ilyen eseményeket jelenteni kell a főigazgatónak.

Legszűkebb funkcionalitás

A Szervezet az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinek a felügyeletét és konfigurációs beállításait a legszűkebb funkcionalitás elvének megfelelően, a nem szükséges funkciók, portok, protokollok, szolgáltatások korlátozásával, illetve tiltásával határozza meg és dokumentálja. A nem helyben üzemeltetett, illetve külső szolgáltatótól igénybe vett EIR-ek esetében a rendszer tulajdonosa határozza meg és dokumentálja az adott EIR használatához szükséges és elégséges konfigurációs beállításokat. Továbbá meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

Legszűkebb funkcionalitás – Rendszeres felülvizsgálat

A Szervezet a rendszerek jelentős módosulásai esetén, de legalább évente átvizsgálja az EIR-ek vagy rendszerelemek által nyújtott funkciókat, portokat, protokollokat és szolgáltatásokat. Az átvizsgálás során kizárjuk, vagy letiltjuk a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat. Az ilyen technológiai átmenetek során lehet, hogy a régebbi és az újabb technológiákat egyszerre kell alkalmazni, és a lehető legkorábban vissza kell térni a minimálisan szükséges funkciókhoz, portokhoz, protokollokhoz és szolgáltatásokhoz. Szervezet vezetője eldöntheti, hogy mely funkciót, portot, protokollt és/vagy szolgáltatást tartja relatíve biztonságosnak, vagy a biztonsággal kapcsolatos döntést más Szervezetek értékelése alapján hozhatja meg. A nem biztonságos protokollok közé tartozik például a Bluetooth, az FTP és a *peer-to-peer* hálózatok. A Szervezet vezetője a rendszergazda által, kikapcsolja vagy eltávolítja azokat a funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat, amelyeket szükségtelennek vagy nem biztonságosnak ítél.

Legszűkebb funkcionalitás – Program futtatásának megakadályozása

A Szervezet vezetője, tiltja minden olyan program futtatását ami nem az érintett Szervezet Szabályzatai, viselkedési szabályai és/vagy a szoftverhasználatot tiltó hozzáférési megállapodások és a fejlesztő vagy gyártó előírásai (beleértve a szoftverlicencelést és a szerző jogokat) szerint történik. A korlátozások közé tartozik az automatikus futtatás funkció tiltása, a program futtatásának jóváhagyására jogosult szerepkörök korlátozása, bizonyos szoftverprogramok engedélyezése vagy tiltása, vagy az egyszerre futtatott programok számának korlátozása, valamint a hordozható (portable) programok futtatásának tiltása.

Legszűkebb funkcionalitás - Engedélyezett Szoftverek — Kivételes Engedélyezés

A Szervezet azonosítja az EIR-ben futtatható szoftvereket. A Szervezetben alkalmazzuk az alapértelmezett tiltás és a kivétel alapú engedélyezés szabályát az EIR-en futtatható szoftverek esetében. Ez azt jelenti, hogy csak azok a szoftverek futtathatók, amelyeket kifejezetten engedélyeztek. A Szervezetben rendszeresen felülvizsgáljuk és szükség esetén frissítjük az EIR-ben engedélyezett szoftverek listáját. Ez azt jelenti, hogy a Szervezetnek folyamatosan nyomon kell követnie az EIR-ben futó szoftvereket, és frissítenie kell az engedélyezett szoftverek listáját, ha új szoftverek kerülnek bevezetésre, vagy ha a már engedélyezett szoftverek engedélye lejár vagy visszavonásra kerül.

Rendszerelem leltár

Az elektronikus információs rendszerelem leltár a Szervezet hardver, szoftver és firmware nyilvántartása. A nyilvántartás elkészítése és naprakészen tartása a rendszergazda feladata.

A nyilvántartás kiterjed:

- az informatikai eszközök leltári és műszaki adataira;
- az informatikai eszközökre telepített szoftverekre, azok licencnyilvántartására, külön rögzítve;
- a megvásárolt licencekre;
- a Szervezet megrendelésére fejlesztett termékek licenceire.
- Leltár kategóriák:
- Hardver: szerverek, munkaállomások, hálózati eszközök, IoT/OT berendezések
- Szoftver: operációs rendszerek, alkalmazások, adatbázisok, middleware
- Adatok: adatbázisok, fájlrendszerek, logok, érzékeny adatállományok
- Szolgáltatások: felhő, SaaS, külső partnerek által nyújtott rendszerek
- Felhasználói fiókok és jogosultságok (különösen adminisztrátori és rendszerfiókok
- A rendszerelem-leltár fő tartalmi elemei:
- 1. Azonosító adatok: Egyedi azonosító (eszköz ID, sorszám). Eszköz vagy rendszer neve. Típus/kategória (pl. szerver, hálózati eszköz, alkalmazás, adatbázis, végponti eszköz, IoT/OT). Gyártó, modell, verzió.
- 2. Hálózati és technikai adatok:
- IP-cím, MAC-cím. Operációs rendszer és verzió. Telepített szoftverek és verziók
- Hálózati szerep (pl. tűzfal, router, adatbázis-szerver). Fizikai vagy virtuális. lhelyezkedés (pl. szerverterem, felhőszolgáltatás)
- 3. Tulajdonosi és felelősségi adatok: Tulajdonos (szervezeti egység vagy személy)
- Rendszergazda / felelős kezelő neve. Üzleti felelős (akihez az eszköz/szolgáltatás kötődik)
- 4. Funkcionális és üzleti besorolás:. Milyen üzleti folyamatot támogat? Kritikalitási szint (pl. magas – üzletmenet szempontjából létfontosságú). Adatosztályozás (pl. nyilvános, belső, bizalmas, szigorúan bizalmas)

- 5. Élettartam és karbantartás: Beszerzés/üzembe helyezés dátuma. Garancia/szolgáltatási szerződés adatai. Frissítési/patch státusz. Tervezett kivezetés dátuma
- 6. Biztonsági jellemzők: Hozzáférés típusa (pl. belső, internet felől elérhető). Hitelesítési mód (pl. jelszó, MFA, tanúsítvány). Naplózási beállítások. Sérülékenységvizsgálat állapota. Mentési/DR (disaster recovery) státusz

A leltárspecifikációk tartalmazzák a beérkezés dátumát, a költséget, a modellt, a sorozatszámot, a gyártót, a beszállítói információt, az elem típusát és a fizikai helyszínt. Az informatikai eszközök, illetve azok használatát érintő változások szabályozott keretek között történő végrehajtását az elektronikus információs rendszer biztonságáért felelős személy időszakosan ellenőrzi.

A rendszerelem leltárban kerülni kell az elemek kettős elszámolását. A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni. A vonatkozó számviteli tv. szerint a leltári adatokat 10 évig meg kell őrizni. A bizonylat elekrtonikus formában is megőrízhető, ha biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását , folyamatos olvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

Rendszerelem leltár – Frissítések a telepítés és eltávolítás során

A Szervezet a rendszergazda által, az elektronikus információs rendszerelemek leltárát frissíti minden egyes rendszerelem telepítése, eltávolítása és frissítése alkalmával.

Rendszerelem leltár – Frissítések a telepítés és eltávolítás során

A rendszergazda a rendszerelemek leltárát frissíti minden egyes rendszerelem telepítése, eltávolítása és frissítése alkalmával.

Rendszerelem leltár – Automatizált karbantartás

A szervezet szükség szerint automatizált mechanizmusokat alkalmaz a rendszerelem leltár naprakészségének, teljességének, pontosságának és hozzáférhetőségének a fenntartására.

Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése

A Rendszergazda meghatározott gyakorisággal, automatizált mechanizmusok segítségével vizsgálja a rendszerben található jogosulatlan hardver-, szoftver-, és firmware-elemek jelenlétét. A jogosulatlan elemek észlelése esetén letiltja az ilyen elemek hálózati hozzáférését, izolálja a rendszerelemeket és értesíti a szervezet által meghatározott személyeket vagy szerepköröket.

Rendszerelem leltár – Elszámoltathatósággal kapcsolatos információk

A Rendszergazda a rendszerelem leltárt olyan módon alakítja ki, amely lehetővé teszi a rendszerelemek kezeléséért felelős és számonkérhető személyek azonosítását név, munkakör és szerepkör alapján.

Konfigurációkezelési terv

A Szervezet kialakít egy konfigurációkezelési tervet az EIR-re vonatkozóan, amely figyelembe veszi a szerepköröket, a felelősségeket, és a konfigurációkezelési folyamatokat és eljárásokat. Ez a terv a fejlesztési és beszerzési szakaszban készül el, és leírja, hogyan

lehet változtatásokat végrehajtani a változáskezelési folyamatokon keresztül, frissíteni a konfigurációs beállításokat és az alapkonfigurációkat, fenntartani az elemleltárakat, ellenőrizni a fejlesztési, tesztelési és működési környezeteket, valamint kidolgozni, kiadni és frissíteni a kulcsdokumentumokat. A Szervezet bevezet egy folyamatot a rendszerfejlesztési életciklus folyamán a konfigurációs elemek azonosítására a konfigurációs elemek konfigurációjának kezelése céljából. Ez magába foglalja olyan hardver, szoftver, firmware és dokumentáció azonosítását, amelyeket konfigurációs szempontból kezelni kell.

A Szervezet meghatározza az EIR konfigurációs elemeit, és a konfigurációs elemeket a konfigurációkezelés hatálya alá helyezi. Ahogy az EIR halad előre a fejlesztési életciklusban, új konfigurációs elemek kerülhetnek azonosításra, illetve kiderülhet, hogy néhány meglévő konfigurációs elemet már nem szükséges konfigurációs szempontból tovább kezelni.

A szoftverhasználat korlátozásai

A Szervezet vezetője

a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt engedélyez, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak;

b) a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;

c) ellenőrzi és dokumentálja az állomány megosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására;

d) ellenőrzi, hogy a Szervezet eszközein szoftvereket (beleértve a hozzájuk tartozó dokumentációt) csak a felhasználási jog keretei szerint telepítik, másolják, futtatják, kivéve a törvény adta szabad felhasználás körében (így különösen biztonsági másolat készítése céljából). Egyetlen termék többszörös használata esetén a szoftver csak a licenc megállapodásnak megfelelően használható. A Szervezet informatikai eszközeire TILOS illegális és/vagy nem jogtiszta szoftvert telepíteni!;

e) engedélyével a Szervezet informatikai eszközeire szoftvereket a felhasználó is telepíthet, de tudatában kell lennie annak a Információbiztonsági kockázataival;

f) által átruházott az informatikai rendszerek üzemeltetési feladataival megbízottak felelőssége, hogy csak akkor telepítsenek licencköteles programot informatikai rendszerre, ha előzetesen meggyőződtek róla, hogy azzal szerzői jogot, licenc megállapodást nem sértenek, a program jogszerű használatát igazoló bizonylatok, okiratok rendelkezésre állnak;

g) által megbízott rendszergazda feladata rendszeres időközönként (legalább kétévente) ellenőrizni automatikus, vagy manuális módszerekkel a Szervezeti szoftverhasználat jogtisztaságát, illetve szerzői jogvédett tartalmak (pl. zene, film, dokumentumok) jogosulatlan megosztását a Szervezet informatikai rendszerein;

h) illegális szoftverek használata, illetve a Szervezet által nem engedélyezett szerzői jogvédett tartalmak tárolása esetén a használatban és megosztásban érintett felhasználóval szemben felelősségének megállapítása érdekében fegyelmi,

kártérítési, illetve egyéb eljárás indulhat, mely eljárást az informatikai feladatokért felelős vezető kezdeményezheti.

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem

- a rendszerszoftver módosításához az illetékes engedélye szükséges;
- a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
- a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni
- (eseménynapló)

Programhoz való hozzáférés, programvédelem

- A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
- Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
- A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartania a program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója;
- a program készítőjének neve;
- a feldolgozási rendszer megnevezése.

Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni;
- a nyilvántartásból egyértelműen megállapíthatónak kell lennie a program azonosítására és kezelésére vonatkozó adatok.

Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni.

Rendszerszoftver

Az üzemeltetésért felelős informatikusnak biztosítani kell, hogy a rendszerszoftver napra-kész állapotban legyen és a segédprogramok programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Felhasználói programok

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Bejelentkezési biztonság (LOGIN SECURITY)

A Szervezetben dolgozók felhasználói jogosultságát és annak körét a rendszergazda a *felhasználó nyilvántartásban* vezeti. A nyilvántartás vezetése és folyamatos aktualizálása a rendszergazda feladata.

A Szervezet az elektronikus információbiztonsággal, rendszer- és szoftverhasználattal kapcsolatos szabályait egy külön dokumentumban *(Engedélyezési és jogosultsági Szabályzat)* kezeli.

Felhasználó által telepített szoftver

A Szervezet vezetője a dolgozóinak, felhasználóinak sem hardveresen, sem szoftveresen nem korlátozza a telepítési és módosítási jogosultságokat. A Szervezet vezetője a Szervezet által használt EIR-ek felhasználói számára az informatikai eszközöket és erőforrásokat a Szervezeti munkavégzés céljára biztosítja. Így a rendszereire, valamint azok számítógépeire és egyéb komponenseire nem csak a rendszergazdák, vagy megbízottak telepíthetnek szoftvereket, de annak informatikai, információbiztonsági kockázataival tisztában kell lenniük.

Amennyiben technikai okok miatt rendszergazdai jogokkal rendelkezik a felhasználó akkor sem jogosult munkahelyi vezetője vagy a rendszergazda engedélye nélkül hardver vagy szoftver telepítése, módosítása.

Információ helyének azonosítása és dokumentálása

A Szervezet azonosítja és dokumentálja az információk helyét, valamint azon konkrét rendszerelemek helyét, ahol az információfeldolgozás és tárolás történik. Ez magába foglalja a specifikus információ típusok és az információ helyének azonosítását a rendszerelemekben, valamint azt, hogy hogyan történik az információfeldolgozás.

A Szervezet azonosítja és dokumentálja azokat a felhasználókat, akik hozzáféréssel rendelkeznek az EIR-hez és a rendszerelemekhez, ahol az információfeldolgozásra és tárolásra kerül.

A Szervezet dokumentálja azokat a változásokat, amelyek az információ feldolgozásának és tárolásának helyét érintik.

3.7 Készenléti tervezés

A Szervezet vezetője megfogalmazza, és az érintett Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a készenléti tervezésre vonatkozó eljárásrendet. A szervezet vezetője kinyilvánítja, hogy az üzletmenetfolytonossági tervek az incidensek és ezáltal a szervezettel kapcsolatos támadásokat követően egy létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére. A szervezet vezetője, az üzletmenetfolytonosság kritériumainak megállapítására egy célt tűzött ki. A tervezett mentések próbáinak sikeres végrehajtása (mérőszám 100%).

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb szabályokat egy külön dokumentumban *(Üzletmentfolytonosság Szabályzat)* kezeli

Üzletmenet-folytonossági Szabályzat és eljárásrendek

Az információk védelmének és a megfelelő rendelkezésre állásának biztosítása érdekében a Szervezet vezetője az alábbi módon teljesíti az üzletmenet-folytonossági elvárásokat:

a) biztosítja, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezetnél (ne sérüljön az SLA);

b) megfelelő alapot ad a kockázatok csökkentésére irányuló hatékony intézkedések végrehajtásához és eredményességük nyomon követéséhez;

c) szerepkörük szerint meghatározza azokat az intézkedéseket, amelyek ahhoz szükségesek, hogy a Szervezet folyamatos működése biztosítva legyen;

d) szerepkörük szerint meghatározza azokat az intézkedéseket, feladatokat, melyeket az esetleges folytonosság megszakadásra felkészülésként, illetve bekövetkezésekor a kár enyhítéseként, illetve a helyreállításért kell tenni;

e) biztosítja, hogy az üzletmenet-folytonosság és a szolgáltatások rendelkezésre állása személyes felelősséghez köthető legyen.

Üzletmenet-folytonossági terv

A Szervezet vezetője: az EIR-re vonatkozó *üzletmenet folytonossági tervben* meghatározza

- az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;
- a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;
- a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket és azok elérhetőségeit;
- az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat;
- az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek;

Az üzletmenet-folytonossági terv jogosulatlanok számára nem megismerhető és módosítható.

A Szervezet működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a Szervezet vezetője feladata. A feladat keretében a Szervezet vezetője alapvetően biztosítja, hogy informatikai szolgáltatás kiesésével járó rendkívüli esemény esetén

- az informatikai szolgáltatás elfogadható időn belül és elfogadható adatveszteség mellett újraindítható legyen;
- az informatikai szolgáltatás kiesésének idejére azon kritikus fontosságú folyamatoknál, ahol ez indokolt a kieső informatikai szolgáltatás használata nélkül működtethető alternatív folyamat biztosítsa a szükséges minimális szinten a működést;
- a Szervezet működését érintő rendkívüli esemény esetén a Szervezet a szükséges tájékoztatási feladatokat Szervezett módon végrehajtsa;
- az informatikai szolgáltatás újraindítását követően az ügyviteli folyamatok a normál működési szintnek megfelelően, a normál ügyviteli rend szerint folytathatóak legyenek.

A fentieket figyelembe véve a vonatkozó kockázatokat szem előtt tartva a Szervezet az informatikai rendszereit úgy alakítja ki, illetve tartalékolja, valamint a külső szolgáltató

által nyújtott informatikai szolgáltatásokra olyan rendelkezésre állási követelményeket köt ki, hogy azok költséghatékonyan támogassák a Szervezet feladatait, illetve az azok alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket.

A fenti követelmények érdekében számba veszi a Szervezet működését támogató informatikai szolgáltatásokat, a szolgáltatások rendelkezésre állását veszélyeztető lehetséges rendkívüli eseményeket és meghatározza, hogy milyen preventív, detektív, illetve korrektív intézkedések bevezetésével csökkenthetőek az informatikai szolgáltatások kieséséből származó kockázatok elfogadható szintre.

A meghatározott – informatikai szolgáltatás kiesésével járó – rendkívüli esemény bekövetkezése esetén végrehajtandó alternatív folyamat szükségességének meghatározásakor az érintett ügyviteli folyamatok rendelkezésre állási követelményei mellett figyelembe veszi a Szervezet által használt informatikai rendszerek rendelkezésre állási képességeit (hogyan és mennyi idő alatt lehet a rendszert újraindítani egy esetleges meghibásodást követően és az újraindítás során mikori adatokat lehet a rendszerbe visszatölteni), illetve a külső féltől igénybe vett informatikai szolgáltatások esetén az azokra vállalt rendelkezésre állási paramétereket.

A fenti szempontok figyelembe vételével a Szervezet vezetője felelőssége meghatározni a Szervezet által alkalmazott kockázatkezelő intézkedéseket; valamint a bevezetett intézkedések működésének biztosítása és felügyelete (pl. az esetlegesen szükségesnek ítélt folytonossági tervek oktatása, tesztelése, rendszeres felülvizsgálata; az informatikai rendszerekre meghatározott rendelkezésre állási képességeket biztosító intézkedések működtetése).

Üzletmenet-folytonossági terv – Összehangolás a kapcsolódó tervekkel

A Szervezet vezetőjének felelőssége, hogy egyeztesse az üzletmenet-folytonossági tervet a kapcsolódó tervekért felelős Szervezeti egységekkel.

Üzletmenet-folytonossági terv – Kapacitás tervezése

A szervezet vezetője megtervezteti a folyamatos működéshez szükséges információfeldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.

- Az EIR-ek kapacitásának tervezését,
- a normál és vészhelyzeti terhelést,
- a környezeti támogatás megtervezését.

Üzletmenet-folytonossági terv – Üzleti (ügymeneti) funkciók visszaállítása

A Szervezet vezetője meghatározza az alapfunkciók újrakezdésének időpontját (azonnali, rövid távú, középtávú vagy hosszú távú) az üzletmenet-folytonossági terv aktiválását követően.

Üzletmenet-folytonossági terv – Alapfeladatok és alapfunkciók folyamatossága

A szervezet vezetése az alapfeladatok és alapfunkciók folyamatosságát úgy tervezi meg, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő. Fenntartható legyen a folyamatosság az EIR elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

Üzletmenet-folytonossági terv – Kritikus erőforrások meghatározása

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerekkel kapcsolatban meghatározza és dokumentálja az elektronikus információs rendszerek alapfunkcióit támogató kritikus rendszerelemeket az üzletmenet folytonossági tervben.

A folyamatos működésre felkészítő képzés

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerek folyamatos működésére, felkészítő képzést tartat az Információbiztonsági felelős révén a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő meghatározott (az Információbiztonsági vezető ajánlása, de legkésőbb az éves oktatás során) időn belül;
- legalább évente egyszer, vagy amikor az elektronikus információs rendszer változásai ezt szükségessé teszik.
- Szükséges gyakorisággal vagy meghatározott eseményeket követően felülvizsgálja és frissíti a folyamatos működésre felkészítő képzés tartalmát.
- Az oktatásról szóló jegyzőkönyvet, dokumentált formában megőrzi.

A folyamatos működésre felkészítő képzés - Szimulált események

A szervezet vezetése megköveteli, hogy a folyamatos működésre felkészítő képzés során, ahol ez alkalmazható szimulált eseményeket alkalmazásával segítse elő a személyzet hatékony reagálását a szervezet működése szempontjából kritikus helyzetekben.

Üzletmenet-folytonossági terv tesztelése

A Szervezet vezetője értékeli az üzletmenet-folytonossági terv tesztelési eredményeit és a felülvizsgálat eredményei alapján, szükség esetén javíttatja a tervet.

Üzletmenet-folytonossági terv tesztelése – Összehangolás a kapcsolódó tervekkel

A Szervezet vezetője egyezteti az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős Szervezeti egységekkel.

Üzletmenet-folytonossági terv tesztelése - Alternatív feldolgozási helyszín

A szervezet vezetése megköveteli, hogy amennyiben ez releváns a szervezetre tesztelve legyenek az üzletmenet folytonossági tervek az alternatív feldolgozási helyszínen is:

- a vészhelyzeti személyzetnek a létesítménnyel és az elérhető erőforrásokkal való megismertetése érdekében; és
- az alternatív feldolgozási helyszín képességeinek értékelése és a vészhelyzeti műveletek támogatása céljából.

Biztonsági tárolási helyszín

A Szervezet vezetője létrehoz egy az elsődleges tárolási helyszíntől földrajzilag elkülönülő biztonsági tárolási helyszínt, beleértve a szükséges megállapodásokat, a

rendszer biztonsági mentési információinak tárolásához és visszakereséséhez, amely biztosítja, hogy a biztonsági tárolási helyszín ugyanolyan szintű védelmi intézkedéseket biztosítson, mint az elsődleges helyszín. Célja, hogy a Szervezetek a Szervezeti rendszerek kompromittálódása, meghibásodása vagy megszakadása ellenére is fenn tudják tartani az alapvető ügymeneti és üzleti funkciókat.

Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől

A Szervezet megfelelően elkülöníti a biztonsági tárolási helyszínt az elsődleges tárolási helyszíntől, az azonos veszélyeknek való kitettségük csökkentése érdekében.

Biztonsági tárolási helyszín – Helyreállítási idő és helyreállítási pont céljai

A szervezet vezetése megköveteli, hogy amennyiben alkalmazható a biztonsági tárolási helyszínt úgy konfigurálják, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

Biztonsági tárolási helyszín – Hozzáférhetőség

A Szervezet vezetője felelős, hogy azonosítsák a potenciális hozzáférési problémákat a biztonsági tárolási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határozzanak meg.

Alternatív feldolgozási helyszín

A Szervezet vezetője kritikus események bekövetkeztének esetére, kijelöl egy alternatív feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésre, az EIR előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - az alternatív helyszínen újrakezdhesse, vagy folytathassa. Gondoskodik arról, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek az alternatív feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak, akár külső Szervezettel kötött szerződések által biztosítva. Biztosítja, hogy az alternatív feldolgozási helyszín védelmi intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal

Alternatív feldolgozási helyszín – Elkülönítés az elsődleges helyszíntől

A Szervezet vezetője olyan alternatív feldolgozási helyszínt jelöl ki, amely megfelelően elkülönül az elsődleges feldolgozási helyszíntől, az azonos fenyegetésekkel szembeni kitettség csökkentése érdekében.

Alternatív feldolgozási helyszín – Hozzáférhetőség

A Szervezet vezetője felelős, hogy azonosítsák azokat a potenciális hozzáférési problémákat az alternatív feldolgozási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határoz meg.

Alternatív feldolgozási helyszín – Szolgálatás prioritása

A Szervezet vezetője az alternatív feldolgozási helyszínre vonatkozóan szükségszerűen olyan megállapodásokat köt, és olyan intézkedéseket vezet be, amelyek a Szervezet

rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal) összhangban álló szolgáltatásprioritási rendelkezéseket tartalmaznak.

Alternatív feldolgozási helyszín - Használatra való felkészítés

A szervezetben amennyiben ez értelmezhető, úgy kell felkészíti az alternatív feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására. Ez magában foglalja az EIR konfigurációjának beállítását, a szükséges hardverek és szoftverek telepítését, valamint a hálózati kapcsolatok és a biztonsági intézkedések meglétét. A szervezetnek biztosítania kell, hogy az alternatív feldolgozási helyszín rendelkezzen a szükséges erőforrásokkal és képességekkel az alapvető funkciók zavartalan működéséhez. A szervezetnek dokumentációt kell vezetnie az alternatív helyszín előkészítéséről

Telekommunikációs szolgáltatások

A szervezetben tartalék infokommunikációs szolgáltatásokat kell létesíteni. Erre vonatkozóan olyan megállapodásokat kell kötni, amelyek lehetővé teszik az EIR alapfunkcióinak, vagy meghatározott műveleteinek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

Telekommunikációs szolgáltatások - Szolgáltatásprioritási rendelkezések

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerei mellett, tartalék infokommunikációs szolgáltatásokkal létesíti és üzemeltet. Erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem az esetleges tartalék feldolgozási vagy tárolási helyszínen.

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor a Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerekkel kapcsolatos üzemeltetőktől megköveteli, hogy az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a Szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

Amennyiben A Szervezet által igénybe vett elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor annak tartalmaznia kell a szolgáltatásprioritási rendelkezéseket, összhangban a Szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal).

Telekommunikációs szolgáltatások - Kritikus meghibásodási pont

A Szervezet olyan tartalék infokommunikációs szolgáltatásokat vesz igénybe, amelyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét.

Telekommunikációs szolgáltatások - Elsődleges és másodlagos szolgáltatók különválasztása

A szervezetnek szükség szerint tartalék infokommunikációs szolgáltatásokat kell beszerezni, nem csak az elsődleges szolgáltatóktól, hanem a tőlük elkülönült független szolgáltatóktól is, hogy csökkentse a szervezet azonos fenyegetéseknek való kitettségét.

Telekommunikációs szolgáltatások – Szolgáltatói üzletmenet-folytonossági terv

A Szervezet vezetése megköveteli, hogy az elsődleges és a tartalék infokommunikációs szolgáltatóknak rendelkezniük kell üzletmenet-folytonossági tervvel.

Felülvizsgálja a szolgáltatók üzletmenet-folytonossági terveit annak érdekében, hogy megfelelnek-e az általa meghatározott üzletmenet-folytonossági követelményeknek.

Meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját.

Az elektronikus információs rendszer mentései

Általános követelmények

- Az adatok mentése azt a célt szolgálja, hogy üzemzavar esetén az aktuális vagy ahhoz közelálló állapot visszaállítható legyen.
- A munkaállomáson tárolt adatok mentését a rendszergazda végzi.
- Archiválandó felhasználói dokumentumok mentése a mentési Szabályzat alapján történik.
- Szervizelés megkezdése előtt a rendszergazda feladata a számítógépek teljes adatmentését elvégezni (amennyiben lehetséges).
- Az adatok archiválásnak célja, hogy az adatok valamely állapotának hosszabb távú megőrzését biztosítsa.
- Az adatok archiválását a rendszergazda végzi.

Az adatok visszaállítása, katasztrófaelhárítás

A vészhelyzetekből eredő veszteségek csökkentéséhez szükséges, hogy a számítógépes infrastruktúra bármely elemének károsodása esetére "készenlétben álljon" az alkalmazandó megoldás.

Az adatok visszaállítása történhet valamely vészhelyzetben, a számítógép olyan szintű meghibásodásakor, hogy a rajta tárolt információk már nem másolhatóak új gépre, továbbá az adatrendszer sérülése vagy egyéni igény alapján (pl. visszavonhatatlan hibás rögzítés).

Az adatrendszer sérülése esetén a rendszergazda a legfrissebb mentés vagy archiválás alapján elvégzi az adatok visszatöltését és az érintett irodák dolgozóit felkéri a mentés utáni adatváltozások rögzítésére.

Munkaállomás meghibásodása esetén a javítás megkezdése előtt, amennyiben lehetséges, teljes adatmentést kell végezni, ezt követi a felhasználóhoz rendelt operációs rendszer és a felhasználói programok telepítése, konfigurálása.

A Szervezet vezetője feladata biztosíttatni a Szervezet működése szempontjából kritikus adatok, szoftverek, konfigurációs beállítások megfelelő tartalékolását. A Szervezet informatikai rendszereinek, illetve az informatikai rendszereken kezelt adatoknak a mentését, megőrzését, tárolását úgy oldja meg hogy a mentések típusa, gyakorisága és példányszáma elfogadható adatvesztési kockázatot eredményezzen, valamint az archiválásra vonatkozó jogszabályi követelményeket teljesíthesse.

A Szervezet vezetője olyan mentési megoldásokat alkalmaz, illetve olyan mentési eljárást működtet, ami biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, illetve a tárolt adatok sérülése használhatatlanná válása esetén rendelkezésre álljon olyan mentés, amely segítségével a kiesett informatikai szolgáltatás elfogadható időn belül újraindítható, illetve amelynek visszaállításával az elvesztett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzését a Szervezet elektronikus formában biztosítjuk, hogy a mentések alkalmasnak az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A Szervezetben hálózati meghajtóra szabad dolgozni (ennek hiányában, a saját gép osztott könyvtárát kell használni) amelyről naponta mentés készül. A kijelölt adatok mentései automatizált módon, fizikailag elkülönített gépre történnek. Napi rendszerességgel cobian backup segítségével. Ezt csak indokolt esetben lehet mellőzni (pl. hálózat nem elérhető, program mappa helyi gépen van) a rendszer üzemeltetőjének tájékoztatásával. Ebben az esetben is gondoskodni kell az adatok mentéséről.

A fentieknek megfelelően a Szervezet vezetőjenek az alábbi irányelveket javasolt figyelembe vennie:

- az adatok mentése illetve archiválása mellett az adatok visszaállításához szükséges valamennyi egyéb adat és szoftver komponens is visszaállíthatóan mentésre, illetve archiválásra kerüljön, vagy mentésük illetve archivált állományuk létezzen,
- a mentésre, illetve archiválásra alkalmazott adathordozó megválasztása az adathordozó felhasználhatóságának gyártói korlátozásai – pl. adatmegőrzési idő, újraírhatóság száma, tárolási előírások stb. - figyelembe vételével történjen,
- a mentéseket tartalmazó adathordozók kezelése a rajtuk tárolt adatok érzékenységének megfelelően történjen, valamint a forrásrendszerrel azonos szintű biztonságos fizikai hozzáférés védelem mellett kerüljenek megőrzésre,
- a mentett és az archív állományok adatainak a visszatöltéséhez szükséges berendezés mindenkor a rendelkezésre álljon.

Egyes rendszerek a programfrissítésük során egy biztonsági mentést végeznek, hogy a sikertelen frissítés esetén vissza lehessen állítani a korábbi állapotot. Ezeket a funkciókat nem tekintjük a Szervezet időszakos mentési politákája részének.

A rendszerek nyilvántartásának részét képezi, hogy milyen időközönként, milyen módon történik mentés az adott rendszerben.

A szerverszobában elhelyezett adattároló eszközre történik a mentés az alábbi eljárás szerint:

Image lemezkép alapu mentés a szerverekről és a kliensgépekről is az elsődleges meghajtókról. Naponta (munkaidőben egyszer) a mentési ügynök elosztja, hogy folyamatosan mikor melyiket menti. Csak a változásokat menti. Kb. 7 -10 napi állapotot lehet visszaállítani.

Az elektronikus információs rendszer archíválása

A Szervezet tevékenységéből adódóan, ha saját rendszerein személyes, Szervezeti védendő adatokat kezel és dolgoz fel és ebből következően archiválási folyamatot tart fent az elektronikus dokumentumok hosszú távú, biztonságos megőrzése, archiválása céljából, akkor a Szervezet az archíválási tevékenységét a rendeletnek megfelleő *Archíválási Szabályzata* szerint hajtja végre.

Egyéb esetben a Szervezet maga határozza meg az archíválandó adatok körét és módját.

Az elektronikus információs rendszer mentései - Megbízhatóság és sértetlenség tesztelése

A Szervezet meghatározott gyakorisággal, de legalább évente egyszer teszteli a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.

Az elektronikus információs rendszer mentései - Visszaállítás tesztelése mintavétellel

A Rendszergazda a helyreállítási terv tesztelésének részeként egy kiválasztott mintát használ a mentett információkból az EIR kiválasztott funkcióinak helyreállítása során.

Az elektronikus információs rendszer mentései - Kritikus információk elkülönített tárhelye

A mentésért felelős Rendszergazda feladata, hogy az EIR szervezet működése szempontjából kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak mentéseit az elsődleges feldolgozási helyszíntől elkülönített létesítményben vagy egy tűzbiztos tárolóban tárolja.

Az elektronikus információs rendszer mentései - Átvitel másodlagos tárolási helyszínre

A szervezet amennyiben ez értelmezhető, meghatározott adatátviteli sebességgel vagy meghatározott idő alatt, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal, átmásolja az EIR mentésének információit az alternatív tárolási helyszínre.

Az elektronikus információs rendszer mentései - Kriptográfiai védelem

A Szervezet megköveteli, hogy kriptográfiai mechanizmusokat alkalmazzanak a mentéstért felelős munkatársak, hogy megakadályozza a meghatározott biztonsági mentési információk jogosulatlan felfedését és módosítását.

Az elektronikus információs rendszer helyreállítása és újraindítása

A Szervezet vezetője által megbízott személy, évente legalább egyszer a felülvizsgálat alkalmával gondoskodik az elektronikus információs rendszer(ek) utolsó ismert állapotba történő helyreállításának próbájáról és újraindításáról, hogy folyamatossá tegye az ügymenetet egy összeomlást, kompromittálódást vagy hibát követően.

A Szervezet az elektronikus információbiztonsággal kapcsolatos helyreállítási szabályokat, valamint az elektronikus információs rendszer helyreállításának, újraindításának menetét az érintett dokumentumban *(Üzletmentfolytonossági Szabályzata)* kezeli. A mentett állományok ad-hoc visszaírása is helyreállítási tesztnek minősül.

Az elektronikus információs rendszer helyreállítása és újraindítása – Tranzakciók helyreállítása

A Szervezet tranzakció alapú EIR-ek esetén tranzakció-helyreállítást hajt végre. A tranzakció naplózása során a Szervezet naplózza a tranzakció összes lépését. Ha a tranzakció nem sikerül, a napló segítségével a Szervezet képes visszaállítani az EIR állapotát a tranzakció kezdete előtti állapotra.

Az elektronikus információs rendszer helyreállítása és újraindítása – Meghatározott időn belüli visszaállítás

A szervezet vezetése, biztosítja, hogy a rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani, olyan a mentésért felelős Rendszergazda által ellenőrzött konfigurációból és sértetlenségvédett információkból, amelyek a rendszerelem ismert működési állapotát reprezentálják.

3.8 Azonosítás és hitelesítés

Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza, és az érintett Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti az azonosítási és hitelesítésre vonatkozó eljárásrendet, mely az azonosítási és hitelesítési Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb azonosítási és hitelesítési szabályokat egy külön dokumentumban *(Azonosítási hitelesítési eljárásrend)* kezeli.

Ebben dokumentálja, kiadja és megismerteti a Szervezet által meghatározott személyekkel szerepkörük szerint a Szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési Szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a Szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a Szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal.

A biztonsági eseményekből és az auditokon levont tanulságokat, be kell építeni az azonosítási és hitelesítési folyamatokba. Ezeknek a megtétele az IBF feladata.

A szervezet vezetője, az azonosítás és hitelesítés megfelelőségi kritériumainak megállapítására egy célt tűzött ki. A tervezett azonosítási, hitelesítési sikeres nem felderített incidensek száma nulla.

Azonosítás és hitelesítés

Fő szabály szerint a Szervezet egyedileg azonosítja és hitelesíti a felhasználókat, és egyedi azonosítóhoz kapcsolja a felhasználók által végzett tevékenységeket.

Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése

Amennyiben alkalmaz ilyet, akkor a Szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.

Azonosítás és hitelesítés (felhasználók) - Nem-privilegizált fiókok többtényezős hitelesítése

Amennyiben alkalmaz ilyet, akkor a Szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.

Azonosítás és hitelesítés (felhasználók) - Egyéni azonosítás csoportos hitelesítéssel

Amikor a szervezet közös használatú fiókokat vagy hitelesítő eszközöket alkalmaz, akkor a felhasználókat egyénileg azonosítja, mielőtt hozzáférést biztosítana a közös használatú fiókokhoz vagy erőforrásokhoz.

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

A Szervezet szükség szerint alkalmaz visszajátszás elleni védelmet (A visszajátszásos támadás (replay támadás, más néven playback támadás) olyan kibertámadás, melynek során a rosszindulatú entitás befogja, majd visszajátssza a hálózaton keresztülhaladó érvényes adatátvitelt.) biztosító hitelesítési mechanizmusokat a privilegizált és a nem privilegizált fiókokhoz való hozzáféréshez.

Eszközök azonosítása és hitelesítése

A Szervezet vezetője megköveteli, hogy egyedileg azonosítsák és hitelesítsék a meghatározott eszközöket, vagy eszköztípusokat, mielőtt helyi, távoli, hálózati vagy egyéb kapcsolatot létesítene velük.

Azonosító kezelés

A Szervezet vezetője megköveteli, hogy az egyéni-, csoport-, szerepkör- vagy eszközazonosítók kijelölését a Szervezet által meghatározott személyek vagy szerepkörök jogosultságához köti. Az így kisztott jogokat a felhasználók kötelesek használni attól nem térjhetnek el. Ez az azonosító lehet például MAC cím, IP cím, vagy eszköz-specifikus token. Ezt, hozzá kell rendelnie az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz. Ez általában az EIR felhasználói fiókok felhasználóneveinek hozzárendelését jelenti az adott személyekhez. A korábban használt egyéni, csoport, szerepkör, szolgáltatás, vagy eszköz azonosítókat más személyekhez, csoportokhoz, szerepkörökhöz, szolgáltatásokhoz vagy eszközökhöz nem rendelhetőek.

Azonosító kezelés - Felhasználói státusz azonosítása

A Szervezet vezetője megköveteli, hogy a felhasználói azonosítókhoz státuszjelölést (szerződéses munkavállalók, külföldi állampolgárok és a Szervezeten kívüli felhasználók) rendeljenek.

A hitelesítésre szolgáló eszközök kezelése

A Szervezet vezetője által kijelölt személy

a) ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;

b) meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

c) biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

d) dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

e) megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;

f) meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;

g) a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;

h) megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

i) megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;

j) lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hasító érték tárolást), és nem továbbítja.

A jelszavas hitelesítést alkalmazó rendszerelemeken kötelező a jelszavas védelem beállítása és alkalmazása.

A felhasználói jelszavakra vonatkozó a mindig a technikailag elvárt, de minimálisan alkalmazandó általános jelszó követelmények:

- a jelszó minimális hossza (legrövidebb jelszó): 8 karakter;
- a jelszó bonyolultsága (komplexitás): tartalmaz legalább egy kis- és nagybetűs, speciális karaktert, valamint számjegyet;
- előző jelszavak megőrzése: legutolsó 5 jelszó tárolása;
- a jelszavak minimális és maximális élettartama: 0 és 90 nap.

A meghatározott jelszóképzési szabálytól eltérni a jelszó hosszát, bonyolultságát illetően a magasabb védelmi szintet jelentő irányba, felfelé lehet (pl.: „jelszó helyett jelmondat" -elv alkalmazásával).

A központi üzemeltetésű, illetve központi szolgáltatótól igénybe vett EIR-ek esetében a Szervezet a rendszer tulajdonosa által meghatározott jelszóképzési szabályokat alkalmazza.

A felhasználói jelszavakat tilos papír alapon, felírva tárolni! Kivételt képeznek ez alól a privilegizált hozzáférésekhez tartozó azonosítók és jelszavak, melyeket rendelkezésre állásuk folyamatos biztosítása érdekében a Szervezet vezetője gondoskodik azok biztonságos megőrzéséről és kezeléséről (lezárt borítékban, páncélszekrényben).

A felhasználói azonosítók és jelszavak elektronikus tárolása, nyilvántartása kizárólag önálló és biztonságos hitelesítési megoldással rendelkező vagy egyéb kriptográfiai védelemmel ellátott módon, offline tárolással engedélyezett; nyílt formában vagy mobil infokommunikációs eszközön, valamint online jelszótároló rendszerben tilos!

Az internetkapcsolaton keresztül elérhető EIR-ek, illetve rendszerelemeik esetében az internet böngészőprogramok beépített kényelmi funkciójának, a bejelentkezési adatok tárolásának (pl.: automatikus kiegészítés, felhasználói jelszavak megjegyzése) a használata tilos, a funkciót kikapcsoljuk!

A gyakran használt/könnyen kitalálható jelszavak listáját minimum évente, de kritikus rendszerek esetében inkább 3-6 havonta kell frissíteni, és minden jelentős jelszószivárgás után azonnal aktualizálni.

Egy kompromittálódott jelszó miatti fiók újra visszaállításakor azonnal új jelszót kell alkalmazni. A régi kompromittálódott jelszó továbbiakban használni tilos.

A hitelesítésre szolgáló eszközök kezelése – Nyilvános kulcs alapú hitelesítés

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél

- hardver token alapú hitelesítése esetén, olyan mechanizmusokat alkalmaz, amely megfelel a Szervezet vezetője által meghatározott minőségi követelményeknek, vagy
- az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal.

Ha a Szervezet hatáskörébe tartozik, akkor azt minden esetben átadás-átvételi bizonylattal dokumentálja. Az átadás-átvétel dokumentumainak megőrzéséről a Szervezet a hatályos iratkezelési szabályainak megfelelően gondoskodik.

A Szervezet vezetője a birtoklásalapú hitelesítésre szolgáló eszközök használati idejét, továbbá ismételt felhasználhatóságának feltételeit az érintett EIR igénybevételére vonatkozó szabályok, valamint a kibocsátó, illetve a gyártó ajánlásainak megfelelően alakítja ki, illetve alkalmazza.

A hitelesítésre szolgáló eszközök kezelése – A hitelesítő eszközök védelme

A Szervezet vezetője meghatározott hitelesítő eszköz átvételéhez megkövetel egy olyan regisztrációs eljárást, melyet meghatározott regisztrációs Szervezet folytat le a Szervezet vezetője által meghatározott személyek vagy szerepkörök jóváhagyása mellett. A hitelesítő eszközöket az információk biztonsági besorolásának megfelelő védelemmel látja el, amelyekhez a hitelesítő eszköz a hozzáférést biztosítja.

Hitelesítési információk visszajelzésének elrejtése

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

Hitelesítés kriptográfiai modul esetén

Amennyiben szükséges, az EIR olyan mechanizmusokat alkalmaz a kriptográfiai modul hitelesítéséhez, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, Szabályzatoknak, szabványoknak.

Azonosítás és hitelesítés (Szervezeten kívüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett Szervezeton kívüli felhasználókat és tevékenységüket. A Szervezet vezetője az

Engedélyezési és jogosultsági Szabályzatba leírtak szerint biztosíthat távoli hozzáférést a rendszereihez, melyről külön nyilvántartást kell vezetni. A Szervezet jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára, csak a hálózatának elemeihez.

A Szervezet hálózatának távoli elérésére az egyes munkaállomások távoli elérésének keretében van lehetőség (titkosított terminál kapcsolat).

A távoli elérések szabályai

- A bejelentkezés időtartamára a felhasználóra kötelezőek a jelen Szabályzatban foglaltak
- A távoli elérésnek biztonságos titkosított terminál kapcsolaton keresztül kell megvalósulnia
- A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító/jelszó megadása)
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni tilos
- 5 egymás utáni sikertelen bejelentkezési kísérlet után a hozzáférést le kell tiltani a bejelentkezéseket naplózni kell a tűzfalon.

A naplózás beállításáért a hálózatért felelős rendszergazda felel.

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

A Szervezet szükség szerint azonosítási profilokat vezet be, amelyeket az azonosítási folyamat során alkalmazni kíván. Így biztosítja, hogy választott és használt nyílt személyazonosság-kezelési szabvány életképes, megbízható, fenntartható és interoperábilis más rendszerekkel, rendszerelemekkel. meghatározott profilokat alkalmaz az azonosítási folyamat során.

Újrahitelesítés

A Szervezet meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az újra hitelesítést.

Személyazonosság igazolása

A Szervezet vezetője megköveteli, hogy amennyiben szükséges, akkor azonosítja azokat a felhasználókat, akiknek a rendszerekhez való logikai szintű hozzáféréshez olyan felhasználói fiókra van szükségük, ami teljesíti a vonatkozó szabványokban vagy irányelvekben meghatározott szintű, a személyazonosság bizonyítására vonatkozó követelményeket. A felhasználói azonosítókat hozzárendeli egy egyedi személyhez és összegyűjti, hitelesíti és ellenőrzi a személyazonosságot igazoló bizonyítékokat.

Személyazonosság igazolása – Személyazonosság bizonyítéka

A Szervezet vezetője - amennyiben szükséges - megköveteli a személyazonosságot igazoló bizonyíték bemutatását a fiókok regisztrációját végző szervnél.

Személyazonosság igazolása – Személyazonossági bizonyítékok hitelesítése és ellenőrzése

A Szervezet vezetője - amennyiben szükséges - megköveteli a bemutatott személyazonosságot igazoló bizonyíték meghatározott módszerekkel történő hitelesítését és ellenőrzését.

Személyazonosság igazolása – Személyes jelenlét melletti hitelesítés és ellenőrzés

A szervezet vezetője, megköveteli, hogy a személyazonosságot igazoló bizonyítékok hitelesítését és ellenőrzését személyes jelenlét mellett a fiókok regisztrációját végző szerv helyett a jogosultságot igénylő személy előtt kell elvégezni.

Személyazonosság igazolása – Cím megerősítése

A Szervezet vezetője - amennyiben szükséges - megköveteli, hogy egy regisztrációs kód vagy megerősítő értesítés egy másodlagos csatornán keresztül kerüljön kézbesítésre, hogy a felhasználók nyilvántartásba vett (fizikai vagy elektronikus) címe ellenőrzésre kerüljön.

3.9 Biztonsági események kezelése

Hitelesítésszolgáltatók tanúsítványának elfogadása

A Szervezet vezetője – szükség szerint az IT üzemeltetővel, és az információbiztonsági felelőssel konzultálva – a bekövetkezett kieséses, állapot körülményeiről és hatásairól, becsült időtartamáról (helyreállítási idő) rendelkezésre álló információk mérlegelését követően dönt az esemény kezelési módjáról, amely lehet:

- kisebb hatású, az informatikai erőforrások szűk körét érintő vagy várhatóan rövid idejű erőforrás kiesés esetén (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybevételével – kezelhető, mint például egy eszköz újraindítása) a szükséges intézkedés megtételének;
- az informatikai erőforrások széles körét vagy egészét érintő (vészhelyzet) esetén a rendeletben előírt működés, nem teljesülését okozó esemény, amely a tartalék intézkedések, illetve helyreállító tevékenységek végrehajtásának elrendelését indokolja.

A biztonsági eseménykezelési szabályokat minden rendkívüli esemény, incidens, auditok alakalmával, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást az IBF végzi a rendszergazdával a management döntései alapján

Biztonsági esemény kezelése Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza, és az érintett Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti az biztonsági események kezelésével kapcsolatos szabályokat.

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb biztonsági események kezelése szabályokat egy külön dokumentumban *(Biztonsági eseménykezelési Szabályzat)* kezeli.

Ebben dokumentálja, kiadja és megismerteti a Szervezet által meghatározott személyekkel szerepkörük szerint a Szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési Szabályzatot, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a Szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá összhangban van a Szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal.

A biztonsági események kezelésének előfeltétele azok felismerése, amelynek érdekében a Szervezet minden munkavállalója, illetve az általa használt EIR-ekhez hozzáféréssel rendelkező, a Szervezettel egyéb munkavégzésre irányuló jogviszonyban álló személy köteles a tapasztalt rendellenességeket a jelezni.

Amennyiben a bekövetkezett esemény hatására a Szervezet által használt EIR-ek, illetve a bennük kezelt adatok, továbbá azok helyben tárolt bemeneti vagy kimeneti információinak bizalmassága, sértetlensége vagy rendelkezésre állása sérül vagy sérülhetett, akkor azt minden esetben biztonsági eseményként kell kezelni.

Az adott esemény biztonsági eseménnyé minősítését kérdéses esetben, illetve annak kiértékelése során az információbiztonsági felelős támogatja, illetve végzi el az eset összes körülményéről rendelkezésre álló információk alapján.

A biztonsági esemény értékeléséhez, kivizsgálásához, illetve bejelentéséhez esetlegesen szükséges további információk (pl.: log fájlok) begyűjtésében az IT üzemeltető köteles közreműködni.

A Szervezet által használt EIR-ek bizalmasságát, sértetlenségét, illetve rendelkezésre állását közvetlenül veszélyeztető biztonsági eseményt az információbiztonsági felelős köteles a jogszabályban meghatározott eseménykezelő felé bejelenteni.

A biztonsági esemény jellegétől és várható hatásaitól függően a bekövetkezett vagy okozható kár, kockázat mérséklése, illetve a fenyegetettség vagy veszélyhelyzet elhárítása, megszüntetése érdekében az információbiztonsági felelős által javasolt és szükséges, illetve a Szervezet vezetője által meghatározott intézkedések végrehajtásában minden érintett köteles együttműködni.

A biztonsági esemény kezelésének lezárását követően szükség esetén új megelőző védelmi intézkedések bevezetésével kell a hasonló incidensek jövőbeni előfordulásának kockázatát csökkenteni. A biztonsági eseményről rendelkezésre álló információk vizsgálata alapján az információbiztonsági felelős jogosult az indokolt új, illetve meglévő védelmi intézkedések módosítására vonatkozó javaslat elkészítése, s a Szervezet vezetője számára történő megküldése.

Képzés a biztonsági események kezelésére

A Szervezet által használt EIR-ekhez, illetve a Szervezet által kezelt adatokhoz hozzáféréssel rendelkező személyek biztonsági események kezelésével kapcsolatos képzése a rendszeres éves biztonsági képzés részeként, történik.

Képzés a biztonsági események kezelésére - Szimulált események

A szervezet vezetője, az információs rendszereket működtető személyzetnek szimulált eseményeket épít be a biztonsági események kezelésére vonatkozó képzésbe, hogy elősegítse a személyzet számára a válsághelyzetekben szükséges reagálást.

Képzés a biztonsági események kezelésére - Automatizált képzési környezet

A szervezet vezetője, amennyiben ez lehetséges automatizált mechanizmusokat alkalmaz, hogy a biztonsági eseménykezelési képzéséhez valósághű környezetet biztosítson.

Biztonsági események kezelésének tesztelése

A Szervezet vezetője, szükség szerint és meghatározott módon és gyakorisággal teszteli a rendszerre vonatkozó biztonsági eseménykezelési képességek hatékonyságát.

Biztonsági események kezelésének tesztelése – Összehangolás a kapcsolódó tervekkel

A Szervezet vezetője, amennyiben releváns, egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért felelős Szervezeti egységekkel.

Biztonsági események kezelése

A biztonsági eseménykezelési tevékenységek megfelelő működése érdekében amennyiben szükséges mérőszámokat és értékelési kritériumokat lehet bevezetni a biztonsági eseménykezelési programok értékelésére, annak érdekében, hogy folyamatosan javítsák az eseménykezelés teljesítményét.

Ekkor a Szervezet összehangolja a biztonsági eseménykezelési tevékenységeket az üzletmenet folytonossági tervezési tevékenységekkel, beépíti a folyamatos biztonsági eseménykezelési tevékenységekből származó tanulságokat a biztonsági eseménykezelési eljárásokba, képzésbe és tesztelésbe.

Biztonsági események kezelése – Automatizált eseménykezelő folyamatok

A Szervezet vezetője - amennyiben releváns - megköveteli, hogy meghatározott automatizált mechanizmusok segítségével támogassa a biztonsági eseménykezelési folyamatot. Ezek az eszközök magukban foglalják az online eseménykezelő rendszereket és azokat az eszközöket, amelyek támogatják a biztonsági események kezeléséhez szükséges adatok gyűjtését, a teljes hálózati csomagok rögzítését és a forensics elemzést.

Biztonsági események kezelése – Információk korrelációja

A szervezet korrelálja a biztonsági eseményekre vonatkozó információkat a szervezet egyéb releváns információival az átfogóbb helyzetfelismerés és -értékelés érdekében. Egy fenyegető eseményt sohasem egymagában kezeli a rendszergazda és az IBF, hanem további információt gyűjt a többi szervezeti egységtől, esetleg eseménykezelő központtól.

Biztonsági események kezelése – Integrált eseménykezelő csoport

A szervezet vezetője az informatikai szervezet teljes állományát kijelöli, mint egy egy integrált biztonsági eseménykezelő csoportot, amely a szervezet által meghatározott időn belül bármely kijelölt helyszínen bevethető.

A biztonsági események nyomon követése

A Szervezet által használt EIR-ekhez hozzáféréssel rendelkező munkatársak és a Szervezet által egyéb munkavégzésre irányuló jogviszonyban álló személyek egyaránt kötelesek hibás működés vagy rendellenes esemény észlelése esetén jelezni. A jelzés

formájától és tartalmától függően az esemény a kezelése során különböző eszkalációs szinteken kerülhet dokumentálásra. Elektronikus (pl.: email) jelzés esetén az észlelő, egyéb esetekben az IT üzemeltető, hatósági bejelentést igénylő biztonsági esemény kapcsán az információbiztonsági felelős által. A biztonsági eseményeket kezelő automatizált rendszerek, melyek az események begyűjtését és elemzését végzik, a CSIRT-ek és egyéb rendelkezésre álló elektronikus adatbázisok és hálózati monitorozó eszközök adatait használják fel.

A biztonsági események nyomon követése - Automatizált nyomon követés, adatgyűjtés és elemzés

A szervezet vezetője, az IBF által küldött riasztásokon keresztül automatizált mechanizmusokat alkalmaz a biztonsági események nyomon követésére, a biztonsági eseményekre vonatkozó információk gyűjtésére és vizsgálatára.

A biztonsági események jelentése

A Szervezet vezetője megköveteli, hogy a használt EIR-ek bármely rendszerelemének, hardver- illetve szoftver komponenseinek rendellenes vagy hibás működéséről, működési zavarairól vagy hibajelzéseiről lehetőség szerint elektronikus formában (email) – vagy ha az nem működik, akkor telefonon keresztül – minden munkavállaló köteles tájékoztatni az IT üzemeltetőt, aki biztonsági incidens gyanújának felmerülésekor köteles haladéktalanul tájékoztatni az információbiztonsági felelőst és a Szervezet vezetőjét.

Ha az a bejelentési kötelezettség körébe tartozó biztonsági esemény, akkor jelenti az tv.-ben meghatározott eseménykezelő felé.

A biztonsági események jelentése – Automatizált jelentés

A Szervezet vezetője - amennyiben alkalmazható - automatizált mechanizmusokat alkalmaz a biztonsági események bejelentésének támogatására.

A biztonsági események jelentése – Ellátási lánc koordinációja

A Szervezet vezetőjének feladata, hogy megossza a biztonsági eseményekkel kapcsolatos információkat az érintett termék vagy szolgáltatás szállítójával (Az ellátási lánc tevékenységekben érintett Szervezetek közé tartoznak a termékfejlesztők, az rendszerintegrátorok, a gyártók, a csomagolók, az összeszerelők, az elosztók, az értékesítők és a viszonteladók), valamint más Szervezetekkel, amelyek részt vesznek az érintett rendszerek vagy rendszerelemek ellátási láncában, vagy annak irányításában.

Segítségnyújtás a biztonsági események kezeléséhez

A Szervezet támogatást biztosít (helpdesk, oktatás) a biztonsági események kezeléséhez és jelentéséhez az EIR felhasználói számára. A biztonsági incidens kezelésének támogatását a feladat- illetve felelősségi körének megfelelően az IT üzemeltető, illetve az információbiztonsági felelős végzi.

Segítségnyújtás biztonsági események kezeléséhez – Automatizált támogatás az információk és a támogatás elérhetőségéhez

A Szervezet vezetője - amennyiben releváns - automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségét és a támogatást.

Biztonsági eseménykezelési terv

A biztonsági eseménykezelési terv (mely része a BCP tervnek), tartalmazza:

- a terv struktúráját és Szervezetet,
- a bejelentésköteles biztonsági eseményeket,
- szükség szerint a metrikákat a belső mérésre,
- az erőforrásokat
- az információmegosztás módját
- a szerepköröket, felelősöket.

A biztonsági események terveit, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást az IBF végzi a rendszergazdával a management döntései alapján. A biztonsági eseményeket az abban résztvevőkkel (Rendszergazda) meg kell ismertetni.

3.10 Karbantartás

Karbantartási Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a rendszer karbantartási eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A karbantartási szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda végzi a management döntései alapján. A karbantartási szabályoakt az abban résztvevőkkel (Rendszergazda) meg kell ismertetni.

A szervezet vezetője, a karbantartási kritériumainak megállapítására egy célt tűzött ki. A tervezett karbantartások sikeres végrehajtása (mérőszám 100%).

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb karbantartások kezelése szabályokat egy külön dokumentumban *(Karbantartási Szabályzat)* kezeli.

Szabályozott karbantartás

A Szervezet vezetője által megbízott személyek vagy vállalkozók

a) a karbantartásokat és javításokat ütemezetten hajtatja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Szervezet követelményeinek megfelelően;

b) jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban;

c) az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a Szervezeti létesítményből;

d) az elszállítás előtt minden adatot és információt – mentést követően – töröl a berendezésről;

e) ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;

f) csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási a számítástechnikai eszközökön javítást, módosítást, illetve új eszközök telepítését csak a rendszergazdák, vagy az általuk megbízott és ellenőrzött külső vállalkozó végezhet;

g) számítógépek esetében, ha a javítás külső helyszínen történik, az esetleges adattartalmat töröljük, az el- és visszaszállítást pedig dokumentáljuk

h) a nem javítható eszközöket a leírtaknak megfelelően selejtezzük, esetleges adattartalmukat pedig – szükség esetén véglegesen és helyreállíthatatlanul – töröljük

i) a tervezett karbantartások mértéke és gyakorisága megfelel a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer elvégzésre kerül;

j) minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával) csökkentéséhez, a helyes és rendszeres karbantartottság révén;

Rendszeres karbantartás – Automatizált karbantartási tevékenységek

A szervezet vezetője megköveteli a karbantartásokat végző informatikai osztály vezetőjétől, hogy automatizáltan, ütemezetten szervezze meg a karbantartásokat és javításokat, és azok dokumentálását. Továbbá a megrendelt, ütemezett, folyamatban lévő és befejezett valamennyi karbantartásról és javításról naprakész, pontos és teljes nyilvántartást vezessen.

Tervezett karbantartások

A Szervezet vezetője az eszközparkot az alábbi gyakorisággal tartja (vagy tartatja) karban, melyek elvégezését és eredményét dokumentálja:

- Számítógépek és szerverek: évenkénti karbantartás
- Számítástechnikai hálózat: évenkénti karbantartás és tesztelés
- Nyomtatók és egy eszközök: igény szerinti, de legalább évente

Hardver védelem

- A számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigény bevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a szerverszobában klímaberendezés használata ajánlott; szervereknél biztosítani kell a szünetmentes feszültségforrást és rack szekrényben vagy szerverszobában kell elhelyezni;
- a számítógép-hálózat csatornáit lehetőség szerint külön kábelcsatornában kell vezetni, melyre jól látható helyekre rá kell írni a hálózat típusát;
- a fali csatlakozók megbontása szigorúan tilos;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez;
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni;
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (Szervezeti informatikus), illetve a szervizek szakemberei nyúlhatnak bele;
- havi rendszerességgel a számítógépeken hardver teszteket kell lefuttatni.
- számítógépek, perifériák, nyomtatók meghibásodása vagy felhasználó váltása estén, illetve 1 év folyamatos üzemelés után az alapvető karbantartást el kell

végezni (felü-let tisztítása, az eszköz belsejéből a por eltávolítása, érintkezők tisztítása),
- az informatikai rendszereket kiszolgáló szerverek karbantartását évente el kell végezni (tisztítás, portalanítás stb.),
- a működéshez szükséges hálózati kiszolgáló eszközök (switch, router) meghibásodása esetén azokat a tartalék készletből azonnal pótolni kell.

Szoftverek karbantartása

- a rendszergazda köteles a használt szoftverek frissítéseit figyelemmel kísérni, a kri-tikus frissítéseket haladéktalanul telepíteni,
- az üzemeltetett informatikai rendszerek verzióváltásait annak rendelkezésre állása után azonnal telepíteni kell,
- rendszergazda folyamatosan ellenőrzi, hogy minden használt szoftver üzemeltetési feltételei biztosítottak-e (szükséges memória mennyiség, tárterület).

Az elvégzett karbantartási munkákat a karbantartási naplóban rögzíteni kell.

Karbantartási eszközök

A Szervezetben - amennyiben ez releváns - az EIR-hez kapcsolódó karbantartási eszközöket csak jóváhagyva, nyilvántartottan és ellenőrzött lehet használni. A nyilvántartásokat a Szervezet az általa meghatározott időközönként felülvizsgálja.

Karbantartási eszközök – Eszközök vizsgálata

A Szervezet vezetője - amennyiben ez releváns - ellenőrizteti a karbantartó személyzet által használt eszközöket, a nem megfelelő, vagy nem engedélyezett módosítások észlelése érdekében.

Karbantartási eszközök – Adathordozók vizsgálata

A Szervezet vezetője ellenőrizteti a diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák, azért, hogy kiderüljön, hogy a diagnosztikai és tesztprogramok adathordozói tartalmaznak-e kártékony kódot.

Karbantartási eszközök – Jogosulatlan elszállítás megakadályozása

A Szervezet (ha a Szervezet által meghatározott személyek vagy szerepkörök egyike kifejezetten engedélyezi a berendezésnek a létesítményből történő elszállítását) megakadályozza a Szervezeti információkat tartalmazó karbantartó eszközök elszállítását az alábbiak szerint:

- Kiszállítás előtt ellenőrzi, hogy a berendezésen van-e Szervezeti információ.
- Szükség szerint, megsemmisíti a berendezést vagy biztonságosan törli annak tartalmát.

Távoli karbantartás

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél

- jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket;

- csak akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az Információbiztonsági Szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében;
- hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál;
- nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről;
- kötelezi a felhasználókat, hogy lezárják, a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

Távoli karbantartás - Azonos szintű biztonság és adattörlés

A szervezet vezetője:

- megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan EIR-ből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a karbantartott rendszer biztonsági képességeivel, vagy amennyiben ez nem biztosított,
- akkor a karbantartandó elemet az EIR-ből eltávolítsák, a karbantartást megelőzően minden szervezeti információt biztonságosan töröljenek az érintett rendszerelemről. A karbantartási folyamat végrehajtását követően az érintett elemet átvizsgálják a potenciálisan kártékony szoftverek észlelése érdekében, mielőtt az EIR-hez csatlakoztatnák.

Karbantartó személyek

A Szervezet vezetője kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére, és nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó Szervezetekről vagy személyekről. Ellenőrizteti az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait, szükség szerint kíséretet rendel a karbantartók mellé. Kijelöli a Szervezethez tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyeket arra, hogy felügyeljék a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

Karbantartó személyek - Nem megfelelő ellenőrzöttségű személyek

A szervezet vezetője eljárásokat dolgoztat ki a nem megfelelő biztonsági ellenőrzöttségű karbantartó személyzet tevékenységének szabályozására. Így:

- Azokat a karbantartó személyeket, akik nem rendelkeznek a szükséges hozzáférési jogosultságokkal, a szervezet által jóváhagyott, megfelelő hozzáférési jogosultsággal és szaktudással rendelkező személyek kísérik és felügyelik őket a karbantartási és diagnosztikai tevékenységek során.
- A karbantartási és diagnosztikai tevékenységek megkezdése előtt minden volatilis adattároló eszközt biztonságosan töröl, a nem volatilis eszközök esetében gondoskodik az adattároló eltávolításáról vagy fizikailag leválasztja a rendszerről.
- Alternatív biztonsági folyamatot alakít ki arra az esetre, ha egy rendszerelemet nem lehet törölni, eltávolítani vagy a rendszerről leválasztani.

Kellő időben történő karbantartás

A Szervezet EIR-t felügyelő működtető feladata, hogy meghatározza, hogy mely rendszerelemek esetén, milyen időtartamon belül szükséges karbantartási támogatást vagy pótalkatrészt biztosítani, (figyelembe véve a BCP és jogi kötelezettségeket) egy hiba esetén.

3.11 Adathordozók védelme

Adathordozók védelme Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza, és az érintett Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti az adathordozók védelmével kapcsolatos szabályokat. Az adathordozók védelme szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda végzi a management döntései alapján. Az adathordozók védelme szabályokat az abban résztvevőkkel (Felhasználók, Rendszergazda) meg kell ismertetni.

A szervezet vezetője, az adathordozók védelme szabályok kritériumainak megállapítására egy célt tűzött ki. A sikeres nem felderített incidensek száma, ami az adathordozók helytelen használatára vezethető vissza (0%).

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb adathordozók kezelése szabályokat egy külön dokumentumban *(Adathordozók védelme Szabályzat)* kezeli.

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti az adathordozók védelmétvel kapcsolatos szabályokat, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Az adathordózónak minősülő eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, stb.) kezelésének a Szervezetben használatos irányelvei:

a) hozzájárul az adathordozók kezeléséből eredő kockázatok csökkentéséhez;

b) lehetővé teszi valamennyi, a tevékenységet érintő adathordozók kezelésével kapcsolatos fenyegető esemény azonosítását;

c) könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak, illetve rendelkezésre álljanak,

d) a jogosultság és a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,

e) a használt adathozdozókat a használat után a tárolási helyre kell visszatenni,

f) munkaidőben a munkaasztalon, csak az aktuális adatfeldolgozáshoz szükséges adathordozók lehetnek

g) adathordozót nem jogosultnak, csak a Szervezet vezetője utasítására lehet átadni,

Vagyontárgyakért viselt felelősség

- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- az adathordozók nyilvántartásában az azonosító adaton kívül a felírás és megőrzés dátumát, a védettség tényét, a jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- adathordozót más intézménynek átadni csak az rendszergazda engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg;
- az adathordozókat félévenként ellenőrizni és tisztítani kell;
- épületen kívülre vitt adathordozót (laptop is) titkosítani kell.
- csak a Szervezet által biztosított adathordozót lehet használni a Szervezeti munka során.

Az olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő:

a) a fizikailag sérült, javíthatatlan;
b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformá-lódott);
c) ha a kapacitás a névleges érték 75%-ánál kevesebb;
d) véglegesen elhasználódott adathordozót.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a *Selejtezési Szabályzatnak* és a *Szervezeti Iratkezelési Szabályzatának* megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

A Szervezet vezetőjének felelőssége, hogy a Szervezet informatikai rendszerein kezelt adatok, az azokat tároló adathordozók, illetve az azokat kezelő informatikai eszközök védelme a kezelt, illetve feldolgozott adatok érzékenységének és a kapcsolódó jogszabályi követelményeknek megfelelő módon valósuljon meg, értékelje az adatok informatikai eszközökön történő feldolgozásának kockázatait és a kockázatok elfogadható szinten tartásának figyelembe vételével alakítsa ki az ügyviteli, adatvédelmi, illetve Információbiztonsági szabályokat. A Szervezet vezetője felelőssége, hogy a selejtezés a rendszergazda bevonásával történjen és minden leselejtezett, de nem megsemmisített adathordozót a Szervezet elzártan tároljon. Az adathordozók megsemmisítése során olyan eljárást alkalmazunk, mely biztosítja az adattartalmuk visszaállíthatatlanságát.

A Szervezet ügyviteli folyamataihoz, valamint a rendszergazda által használt külső adattárolóiról (pl. flash disk, USB pendrive, memóriakártya, hordozható HDD és SSD) nyilvántartást vezet

Hozzáférés adathordozókhoz

Az adathordozókat alapértelmezetten a rendszergazda tárolja és tartja nyilván. A rendszergazda bocsájtja rendelkezésre az adathordozókat igény esetén meghatározott időre. Ettől az eljárástól eltérni csak a Szervezet vezetője engedélyével lehet.

A használni kívánt adattárolót a tárolásra kijelölt helyről vesszük ki és használatot követően oda is helyezzük vissza. A munkaasztalokon csak a munkavégzéshez használatos adathordozók lehetnek.

Az adattárolóknak minden felhasználónak rendeltetésszerűen használja. A Szervezet adathordozóin csak munkavégzéshez szükséges adatokat tároljuk.

A felhasználók saját tulajdonú adathordozóit az informatikai hálózatra csak vírusszűrés után csatlakoztathatják.

Adathordozók címkézése

A Szervezet vezetője - amennyiben ez releváns - megkövetelheti, hogy a Szervezetben jelöljék meg az EIR adathordozóit, jelezve az információra vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és a megfelelő biztonsági jelzéseket a hatályos jogszabályoknak, irányelveknek megfelelően. Mentesíthet meghatározott adathordozótípusokat a jelölési kötelezettség alól, ha az adathordozók a Szervezet által meghatározott ellenőrzött területeken belül maradnak.

Adathordozók tárolása

A Szervezet vezetője megköveteli, hogy az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél:

- fizikailag egyedileg azonosítsák, ellenőrizzék és biztonságosan tárolják az adathordozókat az arra engedélyezett vagy kijelölt (elzárt) helyen;
- védi (és ezt a munkatársaitól is megköveteli) az elektronikus információs rendszer adathordozóit mindaddig, amíg az adathordozókat jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik.

A Szervezeti munkavégzéshez a Szervezet által biztosított, beépített adathordozót tartalmazó mobil eszközök (pl.: laptop, tablet, okostelefon) és mobil adattároló eszközök (pl.: memóriakártya, külső háttértároló eszköz vagy merevlemez, optikai adathordozó lemez stb.) fizikai védelméről és biztonságos tárolásáról és kezeléséről a használatára jogosult személy, munkavállaló köteles gondoskodni. Használaton kívül az eszközt, adattárolót elzárjuk, illetve illetéktelenek számára hozzáférhető helyen folyamatos felügyelet nélkül, őrizetlenül hagyni (pl.: közterületen parkoló zárt gépjárműben is) nem szabad!

Adathordozók szállítása

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél

- megköveteli, hogy az IBSZ-ben leírt biztonsági óvintézkedésekkel védjék és ellenőrizzék az elektronikus információs rendszer adathordozóit az ellenőrzött területeken kívüli szállítás folyamán;
- biztosítja az adathordozók elszámoltathatóságát az ellenőrzött területeken kívüli szállítás folyamán;

- feljegyzésben dokumentálja az adathordozók szállításával kapcsolatos tevékenységeket;
- korlátozza az adathordozók szállításával kapcsolatos tevékenységeket az arra jogosult személyekre.

Adathordozók törlése

A meghibásodott, további felhasználásra alkalmatlan adathordozókat a rendszergazdának fizikai roncsolással kell megsemmisíteni.

Az adathordozókat selejtezés vagy az újrafelhasználásra való kibocsátás előtt a rendszergazdának helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törli, így védve az adatok bizalmasságát. A biztonságos törlés eredményességét a rendszergazdának minden esetben ellenőrzi. Azokat az adathordozókat, amelyeket nem lehet biztonságosan törölni, tilos újrafelhasználni, azokat meg kell semmisíteni.

Adathordozók törlése - Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés

A szervezet informatikai osztályának vezetője, felülvizsgálja, jóváhagyja, nyomonköveti, dokumentálja és ellenőrzi az adathordozók biztonságos törlésével és megsemmisítésével kapcsolatos tevékenységeket. A nyilvántartás tartalmazza, hogy kik vizsgálták felül és hagyták jóvá a biztonságos törlési vagy megsemmisítési intézkedéseket, a megsemmisített adathordozók típusait az adathordozón tárolt adatok, az alkalmazott törlési eljárások, a törlési vagy megsemmisítési intézkedések dátumát és időpontját, a törlést vagy megsemmisítést végző személyek, a végrehajtott ellenőrzési műveletek, az ellenőrzést végző személyek és a biztonságos törlésre vagy megsemmisítésre vonatkozó intézkedésekrt.

Adathordozók törlése - Berendezés tesztelése

A szervezet informatikai osztályának vezetője a biztonságos törléshez alkalmazott eszközöket és eljárásokat vonatkozó inciden esetén, de egalább évente egyszer teszteli.

Adathordozók törlése - Roncsolásmentes technikák

A szervezet informatikai osztályának vezetője roncsolásmentes adattörlési technikákat alkalmaz a frissen vásárolt, vagy az ellenőrzésük alól kikerülő adathordozókon, mielőtt azokat a szervezet által meghatározott körülmények között csatlakoztatná a rendszerhez.

Adathordozók használata

A Szervezet vezetője engedélyezi az adathordozók használatát, és dokumentálja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint jogosítványuk tartalmát, időtartamát. Alapesetben, megtiltja a hordozható adattároló eszközök használatát a Szervezeti EIR-ekben, ha azoknak nincs azonosítható, vagy engedélyezett tulajdonosa.

3.12 Fizikai és környezeti védelem

Fizikai környezet védelme Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a fizikai védelemmel kapcsolatos szabályokat, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A fizikai védelmi szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A fizikai védelmi szabályokat az abban résztvevőkkel (A teljes személyzet és külső megbízottak, alvállalkozók) meg kell ismertetni.

A szervezet vezetője, a fizikai védelmi szabályok kritériumainak megállapítására egy célt tűzött ki. A sikeres nem felderített incidensek száma, ami a fizikai védelmi szabályok helytelen használatára vezethető vissza (0%).

A Szervezet az elektronikus információbiztonsággal kapcsolatos egyéb fizikai biztonsági szabályokat egy külön dokumentumban *(Fizikai védelem Szabályzat)* kezeli.

Alapvető normák, üzemeltetési szabályok

A felhasználók kötelesek betartani a Szervezet vezetője által meghatározott fizikai védelmi intézkedéseket, önhatalmúlag nem változtathatják meg az eszközök elhelyezését, valamint kötelesek a napi munkavégzés során az alábbi alapvető viselkedési normákkal összhangban kezelni az informatikai eszközöket, illetve adathordozókat.

A Szervezet épületeinek minden oldalról zárható határfelülettel kell rendelkeznie. Minden munkatárs köteles ellenőrizni a felügyelete alatt álló Szervezeti helyiség nyílászáróinak megfelelő működését, zárhatóságát. Rendellenesen működő, nem zárható nyílászáró javításáról haladéktalanul intézkedni kell, emiatt azt soron kívül jelezni köteles a hibát észlelő vagy arról értesülő munkatárs a Szervezet vezetője felé.

A Szervezet épületeinek ügyfelek, illetve látogatók számára biztosított bejáratain, valamint az ügyfelek és látogatók számára nyitott területein és az ügyintézésre használt, az ügyintéző munkatárs által felügyelt helyiségein kívül minden más be- és kilépésre alkalmas nyílászárót használaton kívül nyitvatartási időben is zárt állapotban kell tartani.

A belépésre jogosultak által elérhető helyiségek folyamatos ellenőrzésének biztosítása érdekében a Szervezet ügyintézésre használt helyiségeiben ügyfelek, továbbá a Szervezet egyéb, ügyfelek elől elzárt területeire, köztük a Szervezet által használt információs rendszerek elemeinek helyt adó helyiségeiben a látogatók és munkavégzés céljából a Szervezettel munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó stb.) kizárólag felügyelet mellett tartózkodhatnak. A felügyelet biztosítása ügyfél esetében az ügyében eljáró ügyintéző, látogató és szerződéses partner esetében a Szervezet vezetője által ezzel megbízott munkavállaló feladata.

Amennyiben a Szervezet adott telephelyén, épületében a beléptetés nem lehetséges a látogatók számára, akkor annak nyilvántartását egy feljegyzésben (napló) kell rögzíteni. A belépési napló vezetésére vonatkozó kötelezettség betartását a Szervezet vezetője jogosult ellenőrizni.

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent. A

szerverszobára vonatkozó tűzvédelem feladatait, sajátos előírásait *„A Szervezet tűzvédelmi Szabályzata"* tartalmazza.

Vagyonvédelem, fizikai biztonság

- a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;
- a szerverszoba kulcsát a Szervezeti informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel;
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- a szerverszobába történő illetéktelen behatolás tényét a Szervezet vezetőjenek azonnal jelenteni kell;
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők, illetve alkalmazottak használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Általános informatikai védelem

- A szerverszobában a Szervezeti informatikuson, valamint az informatikai rendszer üzemeltetését végző gazdálkodó Szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a Szervezeti egység vezető engedélyezheti.
- Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát a Szervezeti informatikus tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben. A szerverszoba áramtalanításáért a Szervezeti informatikus a felelős.
- Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért a Szervezeti informatikus a felelős.
- A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!
- A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!
- A szerverszoba takarítását csak a Szervezeti informatikus felügyelet mellett, legalább havonta egyszer, a kijelölt személyek végezhetik.
- A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a Szervezeti informatikus és a szervizek szakemberei végezhetnek.
- A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.
- Adathordozókat csak a Szervezeti informatikus engedélyével lehet be- és kivinni a szerverszobából.
- Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet.

- A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket.
- Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben a rendszergazda fegyelmi felelősségre vonást kezdeményezhet

Védelmi előírások

- A számítógépeket csak indítójelszóval lehessen elindítani, az indító jelszót 30 naponta meg kell változtatni; induláskor minden esetben vírus-ellenőrző programot kell elindítani;
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- Az egyes szakági rendszerek felhasználói csak jelszavas azonosítást követően léphetnek be a rendszerbe. A felhasználói névnek és a jelszónak minden esetben egyedinek kell lennie.
- Minden esetben a jelszavaknak különbözniük kell.
- A bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel vagy külső programmal is.
- A módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni;
- A teljes anyagról heti mentéseket kell készíteni;
- A teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni és azt meg kell őrizni. Ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény).
- A felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól az épületen kívül, egy tűzbiztos helyen kell tárolni.

Felhasználókra vonatkozó szabályok

Felhasználó lehet, a Szervezet képviselője, a Szervezet dolgozója (egyéb jogviszony keretében foglalkoztatott), illetve egyéb személy, aki felhasználói jogot kért és kapott. A felhasználói jogosultság teljes egészében csak a Szabályzatban meghatározott esetekben vonható meg, az alapszolgáltatásokon túl igénybe venni kívánt egyéb szolgáltatásokhoz felhasználói jogot kell kérniük a rendszergazdától, a Szervezet vezetője engedélyével. Egyéb személy felhasználói jogot csak Szervezet vezetőjének engedélyével szerezhet.

A felhasználók az épületbe személyes, egyedi azonosítóval ellátott, elektronikus beléptető rendszer ellenőrzésen keresztül léphetnek be. A belépési jogot és az eszközt, a munkába lépéskor kapják meg és a jogviszony napjának lejártakor vissza kell vonni. Elvesztés esetén, egyedi ideiglenes belépőt kell kiosztani és dokumentálni az elveszett elektronikus azonosító egyidejű visszavonásával. Az így kiosztott elektronikus eszközök érvényes jogosultságát rendkívüli esetben, incidens alkalmával, de legalább évente egyszer, felül kell vizsgálni. A vendégek belépését külön látogatói naplóban kell rögzíteni. A napló felülvizsgálatára hasonló szabályok vonatkoznak, mint az elektronikus beléptető rendszerre. A naplókat tilos módosítani. A naplóban tett utolsó bejegyzéstől számított 5 évig meg kell őrizni.

Általános felhasználói szabályok

- A Szervezet tulajdonában vagy használatában levő számítógépes infrastruktúra felhasználója köteles munkáját a Szabályzat szerint végezni.
- A felhasználó a számítógépes infrastruktúrát köteles rendeltetésének megfelelően használni. Így tilos különösen: más felhasználók tevékenységének zavarása, illetéktelen jogosultságok és adatok megszerzése, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése.
- A felhasználó köteles együttműködni a rendszergazdával, köteles figyelembe venni a megfelelő üzemelés érdekében tett javaslatokat.
- A Szabályzat előírásainak az egyéb, a felhasználó általi vétkes megszegése esetén a szabályszegés – egyéb szankciók mellett – a felhasználásból történő kizárást vonhatja maga után.

A Szervezet épületén kívül

Az alábbi szabályok érvényesek minden olyan helyiségre, ami nem Szervezet használatában, felügyeletében van. Így tipikusan ilyenek például az alábbiak:

- felhasználó lakása;
- közösségi közlekedés;
- közösségi helyek (pl. étterem, kávézó)
- egyéb közterület (pl. utca).

Az ilyen jellegű környezetben az alábbi szabályok betartásával lehet Szervezet tulajdonú informatikai eszközt tárolni, használni:

- Utcán, tömegközlekedési eszközön és egyéb nyilvános helyen a Szervezet tulajdonát képező informatikai eszközt – különös tekintettel az adathordozókra – nem szabad felügyelet nélkül hagyni.
- Tilos bekapcsolt és bejelentkezett, de nem zárolt laptopot, vagy egyéb hordozható eszközt felügyelet nélkül hagyni.
- Laptopon, hordozható eszközökön, hordozható adathordozón a feltétlen szükséges minimumra korlátozzuk az érzékeny adatok tárolását, ahol adottak ennek a technikai feltételei az érzékeny adatokat titkosítva tároljuk (ennek egy tipikus módja, ha a laptopokon ki alakításra kerül egy titkosított partíció az érzékeny adatok tárolására)
- Nem szabad nyilvános helyen őrizetlenül hagyni.

Tiszta asztal, tiszta politika

Az irodahelyiségekben tárolt és kezelt adatok jogosulatlan felhasználása ellen minden belépésre jogosultnak fel kell lépnie. Így,

- kötelesek az általuk kezelt adathordozókat csak a használat ideje alatt maguknál tartani;
- kötelesek a papír alapú adathordozók kezelése során az iratkezelési Szabályzat előírásait betartani;
- a részükre kiadott biztonsági eszközöket a hatályos szabályozások szellemében, más személyek részére nem adhatják át;

- kötelesek az informatika eszközről kijelentkezni vagy azt zárolni minden esetben, ha a tevékenységet befejezte vagy megszakítja oly módon, hogy az informatikai eszköz felügyelet nélkül marad;
- kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekben, hogy az ellenőrizetlenül ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz;
- kötelesek a munkanap végén a rendelkezésére bocsátott informatikai eszközt kikapcsolni. Ez alól a szabály alól a Szervezet vezetője személyre, eszközre, munkafolyamatra vonatkozó felmentést adhat, ha ez szakmailag indokolt.
- a Szervezet épületén belül, Szervezeti informatikai eszközt harmadik személynek csak indokolt esetben lehet átadni (pl. laptop, előadás céljára), de ebben az esetben is gondoskodni kell róla, hogy illetéktelen ne jutthasson érzékeny adatokhoz.
- Az ügyfelek, illetve látogatók által látható területen az ügyintézés időtartama alatt a papír alapú adathordozók kezelése során kizárólag az aktuális ügyhöz szükséges iratok lehetnek elő
- kizárólag az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva, (amennyiben az ügyfél rálát a képernyőre) a képernyőn.

Számítógépek, szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen és maradéktalanul elvégezni:

- menteni a még használható fizikai és logikai eszközöket
- biztonsági mentésekből, háttértárakról a megsérült adatok visszaállítása
- archivált anyagok (ill. tartalék eszközök) használatával folytatni kell a feldolgozást

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése, tartalékolása. Az üzemeltetést, karbantartást és szervízelést a rendszergazda végzi. Információs eszköz megbontását (kivéve garancia) csak a rendszergazda végezheti el. A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlásait,
- mások és a saját tapasztalatot

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót. A selejtezést a Selejtezési Szabályzatnak és a Szervezeti Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

Informatikai feldolgozás folyamatának védelme

Az adatrögzítés védelme:

- adatbevitel hibátlan állapotú eszközön történhet
- csak tesztelt, leltárban lévő adathordozóra lehet adatokat másolni, rögzíteni
- a jogosultságok használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz,
- az adatzok bevitelénél elv, hogy azonos állomány rögzítését és ellenőrzését uygan az a személy nem végezheti,
- az adatrögzítési dokumentumok:
    - adatrögzítési utaístások
    - ellenőrzési utasítások
    - programok kezelési utasításai
    - megőrzési és archíválási utasítéás
    - kezelési és karbantartási utasítások.

Központi gépek védelme

Szünetmentes áramforrást kell használni, amely megvédi az információs eszközt a feszültségingadozásoktól, adatvesztéstől, egy áramkimaradás esetén. A központi gépek háttértárairól folyamatosan biztonsági mentést kell végezni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

Munkaállomások gépeinek védelme

Külső helyről hozott, kapott adatokat a használat előtt, egy arra alkalmas (hálózatról leválasztott) gépen, a rendszergazda által, vírusellenőrző programmal kell ellenőrizni. Új rendszerek használata előtt, szükség szerint adaptálni kell és tesztadatokkal ellenőrizni kell a működésüket.

A hálózati elemek és vezetékek, csatlakozók és egyéb átviteli elemeket mindennemű sérüléstől óvni kell. Ezek illetéktelen megbontása tilos.

A Szervezet azon helyiségeibe, ahol információs rendszerek (pl. szerverek, adatmentések, telefonközpontok, stb.) vagy rendszerelemek (pl. számítógépek) találhatóak, vagy ahonnan bármilyen jellegű hozzáférés lehetséges a rendszerekhez vagy rendszerelemekhez, ellenőrizetlenül csak az arra jogosultak léphetnek be, meghatározott szabályok szerint.

A szabályok és korlátozások nem vonatkoznak a létesítmény bárki által szabadon látogatható vagy igénybe vehető helyiségeire.

Nyitott területen a Szervezet által használt EIR-ekhez közvetlenül vagy közvetett módon hozzáférést biztosító hálózati végpont vagy egyéb informatikai eszköz esetében gondoskodni kell az adott eszköz típusának megfelelő hozzáférésvédelem kialakításáról (pl.: hálózati végpont letiltása, fizikai csatlakozásának megszüntetése a központi hálózati elosztón, nyomtató vagy multifunkciós berendezés kizárólag azonosítást követően történő használatának kikényszerítése, beállítása jelszavas vagy PIN kódos védelem alkalmazásával, stb.). Amennyiben a hozzáférésvédelem nem alakítható ki, a Szervezet a végpont fizikai megszüntetéséről, illetve az eszköz zárt területre történő áthelyezéséről köteles gondoskodni.

A Szervezet *Szervezeti és Működési Szabályzatában* meghatározott nyitvatartási (ügyfélfogadási) időn belül a Szervezet minden épületének ügyfelek és látogatók számára nyitott területeire (pl.: ügyfélváró, folyosó, stb.) bárki szabadon beléphet.

A Szervezet ügyintézésre használt helyiségeibe, irodáiba az ügyfelek ügyintézési célból az ügyintézésben eljáró munkatárs engedélyét követően; ezen helyiségekbe, továbbá a Szervezet egyéb, ügyfelek elől elzárt területeire, köztük a Szervezet által használt EIR-ek elemeinek helyt adó helyiségekbe a látogatók és munkavégzés céljából a Szervezetlal munkavégzésre irányuló szerződéses jogviszonyban álló személyek (pl.: üzemeltető, karbantartó, stb.) a kíséretükkel, illetve felügyeletükkel a Szervezet vezetője által megbízott munkavállaló engedélyével léphetnek be.

Nyitvatartási időn kívül a Szervezet épületeiben ügyfél, látogató vagy a Szervezet számára munkát végző, szerződött partner kizárólag a Szervezet vezetője erre vonatkozó külön írásos – rendkívüli, indokolt esetben szóbeli – engedélyével, s az általa e feladattal megbízott munkavállaló felügyelete mellett tartózkodhat. A nyitvatartási időn kívül történő belépési igényről – vészhelyzet, például tűzeset kivételével – a Szervezet vezetőjet minden esetben előzetesen tájékoztatni kell.

Minden munkatárs kötelessége, hogy a Szervezetben kialakított fizikai és elektronikus védelem elemeit (zárható nyílászárók, riasztó rendszer stb.) rendeltetésüknek és a jelen fejezetben meghatározott szabályoknak megfelelően használja.

Tilos a védelmi eszközök funkcionalitásának megváltoztatása, mint például:

- az automatikusan záródó, illetve a folyamatosan zárt állapotban tartandó nyílászárók kitámasztása;
- az elektronikus védelmi rendszerek érzékelőinek (pl.: mozgásérzékelő szenzor) letakarása, pozíciójának megváltoztatása (pl.: elforgatása) vagy leszerelése, megbontása.

A zárható helyiségeket azok elhagyását követően minden alkalommal zárt állapotba kell helyezni.

Minden munkatárs köteles azonnal jelezni a Szervezet vezetője felé, ha a védelmi rendszerek működésében rendellenességet vagy hibát észlel.

Őrzés, védelem szempontjai

- A Szervezet törekszik az élő erős őrzés megvalósítására. Ha ez megvalósul, akkor Szabályzatban rögzítjük az őrszolgálat működési rendjét, az incidenskezelés folyamatát.
- Az EIR-t is futtató helységeibe a bejutás ellenőrzötten történik az oda beosztottakon és ügyintézés miatt jelenlévőkön kívül (pl. vendégek, karbantartók stb.) ellenőrzésről nyilvántartást vezetünk.
- A Szervezet a lehetőségeihez képest kialakít az objektum védelme érdekében behatolás védelmi, tűzjelző és szükség szerint video-megfigyelő rendszert. A biztonsági rendszerek adatai archiváljuk, és akár több hónapra visszamenőleg megőrizve a hazai jogszabályokat figyelembe véve.
- Földszinti ablakokon lehetőség szerint vasrácsokkal védekezünk az illetéktelen behatolástól. Az Információbiztonsági felelős rendszeresen (évente) ellenőrzést hajt végre, az eredményt Szervezet jegyzőkönyvben rögzíti, mely része,

kiegészítése a Cselekvési tervnek. A Szervezet jegyzőkönyvet az EIR Szolgáltatási szerződésben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

A fizikai belépési engedélyek

A Szervezet vezetője megköveteli, hogy az információs rendszereinek helyt adó helyiségeibe való belépésre jogosult Szervezeti munkavállalók (jelenléti ív) és a Szervezettel munkavégzésre irányuló szerződéses jogviszonyban álló személyek listájának elkészítéséről és kezeléséről, valamint naprakész állapotban tartásáról a Szervezet vezetője gondoskodik. A Szervezet vezetője által jóváhagyott lista írásos belépési engedélynek minősül.

A Szervezet vezetője:

a) összeállítja, jóváhagyja és kezeli az elektronikus információs rendszereknek helyt adó létesítményekbe belépésre jogosultak listáját;

b) rendszeresen felülvizsgálja a belépésre jogosult személyek listáját;

c) eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt;

d) intézkedik a b) pont szerinti dokumentumok visszavonása, érvénytelenítése, törlése, megsemmisítése iránt.

A fizikai belépés ellenőrzése

A Szervezet vezetője megköveteli, hogy:

a) kizárólag a Szervezet által meghatározott be-, és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést;

b) ellenőrzés alatt legyen tartva a létesítményen belüli, belépésre jogosultak által elérhető helyiségeket;

c) gondoskodik a létesítmény információs ezsközeinek helyt adó létesítményeibe, eseti jelleggel belépők kíséretéről és figyelemmel követi a tevékenységüket;

d) megóvja a kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést ellenőrző eszközöket;

e) meghatározott rendszerességgel változtatja meg a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti a belépési jogosultságát;

f) felhívja a Szervezet tagjainak figyelmét a rendellenességek jelentésére.

Az informatikai rendszereken történő adatfeldolgozás biztonsága érdekében megakadályozza az informatikai eszközökhöz történő jogosulatlan fizikai hozzáférést, illetve biztosítja az eszközök megbízható működéséhez szükséges környezeti feltételeket (pl. hőmérséklet, páratartalom).

A Szervezet vezetője felelőssége biztosítani, hogy a Szervezet helyiségeinek kialakítása, illetve az informatikai eszközök elhelyezése során a helyi adottságokat figyelembe véve elfogadható szintre csökkentse az informatikai eszközök jogosulatlan fizikai hozzáféréséből eredő kockázatokat, a lehetőségekhez képest legoptimálisabb módon

biztosítottak legyenek az egyes informatikai rendszerek megbízható működéséhez szükséges környezeti és infrastrukturális körülmények.

A fizikai belépés ellenőrzése - Rendszer hozzáférés

A szervezet vezetője a létesítménybe történő fizikai belépés ellenőrzésén túlmenően külön engedélyhez és az informatikai osztály által biztosított kisérőhöt köti a fizikai belépést a szervezet által meghatározott fizikai helyiségekbe, amelyek egy vagy több rendszerelemet tartalmaznak.

Hozzáférés az adatátviteli eszközökhöz és csatornákhoz

A Szervezet vezetője engedélyhez köti és ellenőrzi az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerei adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést. Továbbá, feladatául szabja az EIR-t működtetőnek, hogy a saját létesítményeiben található meghatározott rendszerelosztókat (például: csatlakozók, elosztók) és átviteli vezetékeket fizikailag is védje az illetéktelen hozzáféréstől.

A kimeneti eszközök hozzáférés-ellenőrzése

A Szervezet vezetője megköveteli, hogy jogosultsághoz legyen kötve és ellenőrizve az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereihez, kimeneti eszközeihez való fizikai hozzáférés annak érdekében, hogy jogosulatlan személyek ne férjenek azokhoz hozzá. A jogosultság történhet szóban, szerződés és munkaköri feladat keretében.

A fizikai hozzáférések felügyelete

A Szervezet vezetője jogosultsághoz köti és ellenőrzi az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereknek helyt adó létesítményekbe történt fizikai hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményt és szükség esetén reagáljon arra.

A fizikai hozzáférések felügyelete – Behatolásjelző és megfigyelő berendezések

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél (ha azt naplózást biztosító védelmi rendszer biztosítja) rendszeresen átvizsgáltatja a fizikai hozzáférésekről készült naplókat.

A fizikai hozzáférések felügyelete – Rendszerekhez való fizikai hozzáférés-ellenőrzése

A szervezet a létesítménybe történő fizikai belépések ellenőrzésén túl külön figyelmet fordít az EIR egy vagy több elemét tartalmazó helyiségekbe történő fizikai belépésekre. lásd a „A fizikai belépés ellenőrzése - Rendszer hozzáférés" pontot.

Látogatói hozzáférési naplók

Az irodahelyiségekben harmadik személy nem tartózkodhat felügyelet nélkül, az üres irodákat be kell zárni, annak érdekben, hogy ellenőrizetlenül senki ne férjen hozzá informatikai eszközhöz vagy egyéb adathordozóhoz.

Látogató fogadásakor a látogató felügyeletét az irodahelyiségben a felhasználónak biztosítja. Az irodahelyiségben a látogatóért a felhasználó felelősséggel tartozik.

Amennyiben nem biztosítható a látogató felügyelete, akkor a látogatók adatait rögzíteni kell. Így a belépési nyilvántartás tartalmazza a látogató személy

- nevét és a képviselt Szervezetet,
- a látogató aláírását,
- az azonosítás módját,
- a belépés dátumát,
- a belépés és a távozás időpontjait,
- a látogatás célját,
- valamint a felkeresett személyek nevét és Szervezetét vagy Szervezeti egységét.

Látogatói hozzáférési naplók - Nyilvántartások automatizált karbantartása és felülvizsgálata

Az informatikai osztály vezetője az szükség szerint automatizált eszközöket alkalmaz a látogatói belépésekről készített információk és felvételek kezeléséhez és átvizsgálásához. A látogatói belépésekkel kapcsolatos nyilvántartásokat célszerűen egy füzetben vezeti.

Áramellátó berendezések és kábelezés

A Szervezet vezetője megköveteli, hogy a szükséges mértékben és optimális módon védjék az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereit árammal ellátó berendezéseket és a kábelezést a sérüléssel és rongálással szemben (kábelcsatornák, rejtett kábelezés). Az erőforrásokat koncentráltan tartalmazó helyiségekben a hőmérsékletnek és a páratartalomnak az erőforrások biztonságos működéséhez szükséges szinten tartása és folyamatos figyelemmel kísérése, ellenőrzése céljából erre alkalmas légkondicionáló berendezést üzemeltet.

Vészkikapcsolás

A Szervezet vezetője megköveteli, hogy a működés során biztosítva legyen az EIR vagy egyedi rendszerelemek áramellátásának kikapcsolása egy esetleges vészhelyzetben. Gondoskodik a vészkikapcsoló berendezések biztonságos és könnyű megközelíthetőségéről az arra jogosult személyek számára. Megakadályozza a jogosulatlan vészkikapcsolást.

Vészhelyzeti tápellátás

A Szervezet vezetője szükséges és elégséges mértékben, az elsődleges áramforrás kiesése esetén, a tevékenységéhez méretezett szünetmentes áramellátást biztosít az EIR szabályos leállításához, vagy a hosszútávú tartalék áramellátásra történő átkapcsoláshoz.

Vészhelyzeti tápellátás - Tartalék áramellátás – Minimális működési képesség

A szervezet vezetője kötelezi az informatikai osztály vezetőjét, hogy az elsődleges áramforrás kiesése esetén automatikus vagy manuális aktiválású hosszútávú alternatív áramellátás biztosításáról gondoskodjon az EIR-ek minimálisan elvárt működési képességének és előre definiált minimálisan elvárt működési idejének fenntartására.

Vészvilágítás

A Szervezet a jogszabályoknak megfelelően alkalmaz és karbantart egy automatikus vészvilágítási rendszert a létesítményben, amely áramszünet esetén aktiválódik, és megvilágítja a vészkijáratokat és a menekülési útvonalakat.

Tűzvédelem

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerei számára - amennyiben azt arra alkalmas, elkülönített helységben (szerverszoba) működteti - független áramellátással támogatott tűz és vagy füstészlelő, az informatikai eszközökhöz megfelelő és a vonatkozó rendeleteknek megfelelő tűzelfojtó berendezéseket alkalmaz, és tartat karban.

Tűzvédelem – Érzékelőrendszerek – Automatikus élesítés és értesítés

A Szervezet vezetője az EIR védelmére olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a Szervezet által kijelölt tűzvédelmi felelősnek.

Tűzvédelem – Tűzoltó berendezések– Automatikus élesítés és értesítés

A szervezet vezetője:

- Az EIR védelmére, ahol lehet olyan tűzjelző berendezést vagy rendszert alkalmaz, amely tűz esetén automatikusan működésbe lép, és értesítést küld a szervezet által kijelölt tűzvédelmi felelősnek.
- Akkor is automatikus tűzoltó berendezést alkalmaz, ha a létesítményben nincs állandó személyzet.

Környezeti védelmi intézkedések

A Szervezet vezetője, megköveteli, hogy a saját működtetésű elektronikus információs rendszerei számára - amennyiben azt arra alkalmas, elkülönített helységben (szerverszoba) működteti - meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és felügyeli azt.

Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél megköveteli, hogy az elektronikus információs rendszer optimális és célszerű kialakítással védjék a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek legyenek.

Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem - Automatizálás támogatása

A szervezet vezetője megköveteli az informatikai osztály vezetőjétől, hogy ha technikailag lehetséges, automatizált mechanizmusokat alkalmazzon az EIR-ek közelében megjelenő folyadékszivárgás észlelésére, vagy alakítson ki olyan fizikai ellenőrzési módszert (szemlék, bejárás) hogy azok időben felismerhetőek legyenek, valamint a szervezet által kijelölt személyek riasztására.

Be- és kiszállítás

A Szervezet vezetője mindig engedélyezi, vagy tiltja, továbbá figyelteti és ellenőrizteti a létesítménybe bevitt, onnan kivitt az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeket, és nyilvántartást vezettet ezekről.

A be- és kiszállítás felügyeletét, figyelemmel kísérését a Szervezettel munkavégzésre irányuló szerződéses jogviszonyban álló személy felügyeletével megbízott munkatárs esetében is engedélyhez köti, szakmai ellenőrzésében szükség szerint közreműködik az IT üzemeltető, rendszergazda

Munkavégzésre kijelölt alternatív helyszín

A Szervezet vezetője meghatározza és dokumentálja az alternatív munkavégzési helyeket a munkavállalók számára (pl. home office). Megköveteli a védelmi intézkedéseket az alternatív munkavégzési helyeken. Szükség szerint biztosítja a szükséges eszközöket a munkavállalók számára, hogy egy biztonsági esemény bekövetkezése esetén kommunikálni tudjanak az információbiztonságért felelős személyekkel.

Az elektronikus információs rendszer elemeinek elhelyezése

A Szervezet vezetője úgy helyezi, vagy helyezteti el az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerelemeit, hogy a legkisebb mértékre csökkentse a Szervezet által meghatározott fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

3.13 Tervezés

Biztonságtervezési Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett Szervezeten belül kihirdeti a tervezéssel kapcsolatos szabályokat, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

Rendszerbiztonsági terv

A *rendszerbiztonsági terv* a meghatározott hatókörön belüli EIR-re és annak rendszerelemeire terjed ki, és tartalmazza a rendszer biztonsági követelményeinek áttekintését, valamint a követelmények teljesítéséhez kiválasztott intézkedéseket. A Szervezet vezetője a saját működtetésű elektronikus információs rendszereihez jelen dokumentumban rendszerbiztonsági tervet készít, amely

a) összhangban áll a Biztonságtervezési Eljárásrenddel, valamint igazodik a Szervezet felépítéséhez és architektúrájához,

b) meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait és azok elvárt szolgáltatási szintjeit [angolul SLA]), biztonságkritikus elemeit és alapfunkcióit;

c) meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

d) meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

e) a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit (naplózás, mentés és helyreállítás, üzletmenet-folytonosság);

f) meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és azok bővítését, végrehajtja a jogszabály szerinti biztonsági feladatokat;

g) gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

h) belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét (belső audit);

i) frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;

j) elvégzi a szükséges belső egyeztetéseket;

k) gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

l) gondoskodik a rendszerbiztonsági terv incidenkor, vagy rendkívüli esemény bekövetkeztekor ezek hiányában, legalább évenkénti felülvizsgálatáról.

Viselkedési szabályok

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-hez hozzáférési jogosultsággal rendelkező személyekkel, felhasználókkal szembeni viselkedési szabályokat, elvárásokat.

A hozzáférési megállapodások egyéb típusai közé tartoznak a titoktartási megállapodások, az összeférhetetlenségi megállapodások és az elfogadható használati megállapodások. A Szervezet gondoskodik arról, hogy a viselkedési szabályok korábbi változatát megismerő személyek elolvassák és újra dokumentált nyilatkozattételt tegyenek a viselkedési szabályok elfogadásáról, azok felülvizsgálata vagy frissítése esetén.

Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások

A viselkedési szabályoknak ki kell terjedniük a közösségi média, a közösségi hálózatok és a külső webhelyek/alkalmazások használatára vonatkozó korlátozásokra. Abban az esetben, ha egy Szervezethez köthető személy ezeket használja hivatalos feladatának ellátására vagy hivatalos ügyek intézésére a közösségi médiával és a közösségi hálózatokkal kapcsolatos hálózati üzenetváltásban Szervezeti információk vesznek részt, mert az adott személy(ek) a közösségi médiához és a webhelyekhez a Szervezeti EIR-en keresztül fér(nek) hozzá.

Viselkedési szabályok az interneten

a) tilos a Szervezetlal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;

b) tiltosak az *Engedélyezési és jogosultsági Szabályzatban* meghatározott, interneten megvalósuló tevékenységek (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt leveleződlisták, „sötét web" stb.) végezni;

c) a Szervezeti gépeken nem korlátozza a közösségi oldalak használatát, tiltja magánpostafiók elérését, és más, a Szervezettól idegen tevékenységet.

d) Tilos a Szervezet informatikai eszközein tárolni, feldolgozni vagy továbbítani olyan anyagokat, melyek közízlést, vagy törvényt sértenek, mint például:

- betiltott filmeket, publikációkat;
- számítógépes játékot;
- pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
- megbotránkoztató, a jó ízlés határait sértő anyagokat;
- gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

A Szervezet az elektronikus információbiztonsággal kapcsolatos engedélyezési és hozzáférési szabályokat egy külön dokumentumban *(Engedélyezési és jogosultsági Szabályzat)* kezeli.

A Szervezet vezetője a 2011.évi CXII tv. (info tv) alapján szabályozza, illetve korlátozza az internet- és email használatot. Az internet és az IT rendszer kizárólag a Szervezetai munkát segíti, tehát kizárólag munkahelyi célra engedi használni azokat. A rendszergazda (ill. erre feljogosított, megbízott személy) jogosult ellenőrizni az internet használatát, hogy betartották-e a tiltásra vonatkozó szabályokat, valamint a hálózati kommunikációt, Szervezeti levelezést az egyes IT eszközök jogos és szakszerű használatát. Ezt követően, a munkáltatónak joga van bármikor ellenőrizni a dolgozókat. Ilyenkor a magáncélból megnyitott honlapokba is betekinthet. Ugyanis, amennyiben a tájékoztatás ellenére a munkavállaló magáncélu oldalakat is megnyit, akkor a honlap letöltésével már hozzájárulását is adja az adatok kezeléséhez.

Az e-mailek ellenőrzése

A szabályozás célja, hogy biztosítsák az elektronikus levelezés zavartalanságát valamint védjék a Szervezet érdekeit. Minden felhasználónak és Szervezeti egységnek lehetősége van felhasználói *nev@szervezet.hu* című postafiókot igényelni, és ezt kizárólagosan Szervezeti célra használni. A Szervezet e szabályokra figyelemmel monitorozhatja a hálózatból küldött, illetve fogadott levelek tartalmát az adatvédelmi szabályok és ajánlások figyelembevételével.

a) A Szervezet hálózatán keresztül küldött vagy fogadott levelek központilag vírus- és kémprogram ellenőrzés történik, ami különböző védelmi és szűri funkciókkal egészül ki.
b) A Szervezet hálózatán keresztül küldött levelek központilag spam ellenőrzésen esnek át.

Alapelvek

- A levelek nem tartalmazhatnak a hatályos magyar jogszabályokba ütköző tartalmat.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

Szabályok

- Tilos kéretlen leveleket, hirdetéseket, kör e-maileket küldeni.
- Tilos kör e-maileket reklám anyagokat tovább küldeni.
- Tilos az e-mail címet olyan kereskedelmi listára feltenni, amelyről a Szervezeti levelező rendszert e-mail szeméttel (spam) terhelhetik meg.
- Tilos a Szervezeti e-mail cím magánjellegű felhasználása.
- Tilos a Szervezeti e-mail címet bármely weboldalon regisztrációhoz felhasználni.
- Tilos ismeretlen vagy gyanúsnak tűnő feladótól érkezett levelek mellékletének megnyitása, vagy továbbítása.
- Tilos nagy méretű file-okat e-mail-ben küldeni mert ez túlzott mértékben terheli a hálózatot vagy esetlegesen blokkolhatja postafiókját. Az ilyen nagy méretű (adatbiztonságot nem sértő!) tartalmat publikus helyen kell elérhetővé tenni. Ha tájékoztatás keretében a munkáltató részletesen meghatározza azokat a címeket, ahonnan e-mail fogadható vagy küldhető és a levelező rendszer magáncélu használatát megtiltja, ezt követően a dolgozó teljes levelezése ellenőrizhetővé válik. A Szervezet az ellenőrzés során betartja a jogviszonyban nem álló harmadik személyek személyes adatainak védelmére vonatkozó jogait.

Az ellenőrzések alakalmával a dolgozónak vagy általa megbízott képviselőjének joga van jelen lenni, erre a munkáltatónak kell felhívnia a figyelmét.

Információbiztonsági architektúra leírás

A Szervezet vezetője, elkészíti az EIR információbiztonsági architektúra leírását, melyben

- leírja az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló követelményeket és megközelítést;
- leírja, hogy az információbiztonsági architektúra hogyan illeszkedik a Szervezet általános architektúrájába, és hogyan támogatja azt;
- leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket;
- az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja és frissíti az információbiztonsági architektúra leírást;
- biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben, a működési koncepcióban és a beszerzésekben.

Biztonsági követelmények kiválasztása

Az érintett Szervezet a rendszerbiztonsági terv részeként meghatározza a szükséges biztonsági követelményeket az EIR számára. Ezek a követelmények adott jogszabályok, végrehajtási rendeletek, irányelvek, Szabályzatok, szabályok, szabványok és útmutatók által előírtak, vagy olyan fenyegetéseket kezelhetnek, amelyek minden felhasználóra közösek.

Biztonsági követelmények testre szabása

A Szervezet testre szabja az így kiválasztott biztonsági követelményeket.

3.14 Személyi biztonság

Személyi biztonsági Szabályzat és eljárásrendek

A Szervezet vezetője - amennyiben a Szervezeti struktúra indokolja - megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-hez hozzáférési jogosultsággal rendelkező személyekkel, felhasználókkal szembeni személyi biztonsággal kapcsolatos, elvárásokat.

A szervezet vezetője kinyilvánítja, hogy a személyi biztonság a szervezettel kapcsolatos belső támadások lehetősége mind a megelőzés mind a felderítés szempontjából egyik létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére.

A személyi biztonsági szabályok alapvető célja, hogy a szervezetben és a szervezeten kívüli felhasználók a jogosultság megszerzése előtt ellenőrizni és bizonyítani lehessen az arra való alkalmasságukat. Az ellenőrzésért felelős a felhasználó felvételének kezdeményezője, ill. a központosított munkaerőfelvétel felelőse.

A személyi biztonsági szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A személyi biztonsági szabályokat az abban résztvevőkkel (munkaerőfelvétellel, beszerzéssel foglalkozók) meg kell ismertetni.

A szervezet vezetője, a személyi biztonsági szabályok kritériumainak megállapítására egy célt tűzött ki. A sikeres nem felderített incidensek száma, ami a személyi biztonsági szabályok helytelen használatára vezethető vissza (0%).

A szervezet egyszerű struktúrájából adódóan a személyi biztonsági szabályokkal kapcsolatos tevékenység az ügyvezető feladata és kiterjed a teljes szervezetre. Nem tagolódik egységekre, és így nem szükséges egységek közötti összehangolásra, együttműködésre.

Az EIR rendszereket használó Szervezeti egység vezetőjének a felelőssége, hogy meghatározza az egyes, EIR szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálattal kapcsolatos elvárások:

- A Szervezet humánpolitikai vezetőjének a felelőssége, hogy foglalkoztatás előtt a betöltendő EIR rendszerhez kapcsolódó munkakör kockázataival arányos mértékű megfelelőségi vizsgálatot végezzen el a foglalkoztatni kívánt munkatárs vonatkozásában.
- A kockázattal arányos mértékben mérlegeli a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképesség stb.).
- Meggyőződik arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.

- Az Információbiztonsági szakterület vezetőjének felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének a felelőssége, hogy a foglalkoztatás alkalmával az önkormányzati Szervezet munkaköri leírásban rögzítse a kockázatokkal arányosan a titoktartás követelményeit (EIR titoktartási nyilatkozat) és a foglalkoztatás egyéb kikötéseit.
- A jogi szakterület vezetőjének felelőssége, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

Munkakörök biztonsági szempontú besorolása

A Szervezet vezetője

- minden az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerrel kapcsolatos Szervezeti munkakört, vagy érintett Szervezethez kapcsolódó feladatot, biztonsági szempontból besorol. A besorolás alapja kétszintű: **Jogosultságot adó** (*tenant adminisztrátor*) és **végrehajtó** (*user*);
- szükség szerint felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat (ha vannak);
- rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

A személyi biztonsági szabályokat, besorolásokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A személyi biztonsági szabályokat az abban résztvevőkkel (munkaerőfelvétellel, beszerzéssel foglalkozók) meg kell ismertetni. Az átvilágítási kritériumokat a 12_5_munkakörök_kockázati_nyilvántartása.xlsx tartalmazza.

Személyek háttérellenőrzése

A Szervezet vezetője:

- az EIR-vel kapcsolatban a saját működtetésű elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrzi, hogy az érintett személy a besorolásnak megfelelő feltételekkel rendelkezik-e;
- a munkaköröket betöltő vagy feladatokat ellátó személyek tekintetében szükség szerint kezdeményezi a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nemzetbiztonsági ellenőrzést (ha szükséges);
- folyamatosan ellenőrzi (az évenkénti felülvizsgálatok alkalmával) e pont szerinti feltételek fennállását.

Személyek munkaviszonyának megszűnése

A Szervezet vezetője vagy erre jogosult megbízottja

a) megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit;

b) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;

c) visszaveszi az érintett Szervezet elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt;

d) megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és a Szervezeti információkhoz;

e) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;

f) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodik;

g) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartására megelőző intézkedéseket tesz.

h) Normál kilépésnél 24 órán belül szünteti meg a jogosultságát a felhasználónak, míg rendkívüli, fegyelmi elbocsátásnál a közlést megelőzően, vagy azzal párhuzamosan, hogy a felhasználó a közlést követően már ne férjen hozzá a fiókjához. Az erre vonatkozó információkat az elbocsátást kezdeményezőnek még az elbocsátást megelőzően jelezni kell a rendszergazdának, hogy az technikailag fel tudjon rá készülni.

Személyek munkaviszonyának megszűnése - Automatizált intézkedések

A szervezet vezetője megköveteli, hogy a személyzet kilépésével párhuzamosan, késedelem nélkül, e-mailen értesítse az informatikai osztály vezetőjét az egyén kilépésével összefüggő tevékenységekről, annak érdekében, hogy az megszüntesse a hozzáféréseket a rendszer erőforrásaihoz.

A hozzáférési jogok visszavonása

A felhasználó informatikai rendszerekhez való hozzáférési jogát visszavonja az arra jogosult személy a felhasználó jogviszonyának megszűnésekor, illetve módosítja a felhasználó feladatainak változása esetén. A Szervezet vezetőjének felelőssége, hogy az egyes felhasználók jogviszonyának megszűnése esetén a Szervezet érintett munkatársait értesítse.

Amennyiben a felhasználó jogainak visszavonása fegyelmi vétséggel kapcsolatos és fennál a gyanúja a bizonyítékok megsemmisítésének illetve szándékos károkozásank akkor, a jogosultásg visszavonását még a fegyelmi eljárás megkezdéséről való tájékoztaás a felhasználóval előtt meg kell tenni.

Általánosságban elmondható, hogy a Szervezet vezetője felelőssége, hogy a felhasználók csak a feladatkörük ellátásához minimálisan szükséges jogosultságokkal rendelkezzenek az informatikai rendszereken. Ennek megfelelően a Szervezet vezetője felelőssége, hogy

- a Szervezet informatikai rendszerét üzemeltető megbízott értesüljön a jogosultságok megváltoztatásának szükségességéről;

- a jogviszony megszűnésekor az érintett felhasználó hozzáférési jogosultsága visszavonásra kerüljön minden olyan informatikai rendszeren, ahol a felhasználó a jogviszony keretében végzendő feladatai miatt kapott hozzáférést;
- a felhasználó feladatkörének változása esetén az új feladatokhoz már nem szükséges jogosultságok visszavonásra kerüljenek;
- tartós távollét esetén a nem használt hozzáférések felfüggesztésre, illetve tiltásra kerüljenek.

A vagyontárgyak visszaszolgáltatása

Minden munkatárs köteles a részére átadott vagyontárgyat visszaszolgáltatni a jogviszony megszűnése előtt.

A kilépő munkatárs munkakörét a Szervezet vezetője által előírt rendben köteles átadni és a munkáltatóval elszámolni. A munkakör-átadás és az elszámolás feltételeit a Szervezet vezetője köteles biztosítani.

A Szervezet vezetője meggyőződik arról, hogy a munkatárs minden munkával kapcsolatos adatot és információt, valamint munkájához használt eszközt (laptop, mobiltelefon, fényképezőgép stb.) átadott, valamint a jogosultságai és hozzáférései visszavonásra kerültek.

Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezés esetén a Szervezet vezetője a jogosultságot kiadóval együttműködve gondoskodik a munkavállaló meglévő jogosultságainak visszavonásáról, majd az új munkakörnek megfelelő új jogosultságok igényléséről, biztosításáról.

Az új munka-, illetve feladatkör által nem igényelt korábbi, meglévő fizikai és logikai hozzáférések megszüntetését, illetve az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését, továbbá az ahhoz nem szükséges eszközök visszavételét követően a Szervezet vezetőjének feladata gondoskodni arról, hogy a használandó, új rendszerek és azokhoz szükséges jogosultságok, hozzáférések beállítása, valamint a kapcsolódó felhasználói fiókok létrehozása, módosítása, illetve indokolt esetben törlése megtörténjen. Így

- az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereknél szükség esetén elvégzi a személyek ellenőrzésére vonatkozó eljárást;
- logikai és fizikai hozzáférést engedélyez az újonnan használni kívánt az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerekhez;
- szükség esetén elvégzi az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését;
- a jogviszony változásáról szóban és szükség szerint írásban (pl.: e-mail) értesíti az EIR rendszereket használó szerepköröket betöltő, feladatokat ellátó személyeket.

Hozzáférési megállapodások

Lásd. *3.13 Tervezés - Viselkedési szabályok* pontban.

Külső személyekhez kapcsolódó biztonsági követelmények

A Szervezet vezetője:

- az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a külső Szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső Szervezet határozza meg a Szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
- szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg a Szervezet vezetője és a vonatkozó rendeletek által meghatározott személybiztonsági követelményeknek;
- a szerződő féltől megköveteli, hogy dokumentálja a személybiztonsági követelményeket;
- előírja, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön írásos (pl. e-mail) értesítést a Szervezet vezetőjenek;
- folyamatosan ellenőrzi a szerződő féltől személybiztonsági követelményeknek való megfelelését.

A külső személyekben történt változásokat a szerződésszerinti szolgáltató 24 órán belül kell jeleznie, hogy időben meg lehessen szünteti jogosultságát a felhasználónak, míg rendkívüli, változásnál (elbocsátás, áthelyezés) a közlést megelőzően, vagy azzal párhuzamosan, hogy a felhasználó a közlést követően már ne férjen hozzá a fiókjához. Az erre vonatkozó információkat a szervezetnek még a rendkívüli változást megelőzően jelezni kell a szervezet rendszergazdájának, hogy az technikailag fel tudjon rá készülni.

Fegyelmi intézkedések

Az informatikai rendszerek biztonságának gondatlan veszélyeztetése, az Információbiztonsági szabályok megsértése, illetve a felhasználó súlyos mulasztása esetén a Szervezet vezetőjének felelőssége a szükséges fegyelmi eljárás lefolytatása. A Szervezet vezetője a fegyelmi eljárás megindításáról köteles írásban értesíteni az érintettet és a vizsgálat végrehajtására vizsgálóbiztost jelölhet ki. Az IBSZ hatálya alá tartozó szabályok megszegése esetén is a fegyelmi eljárás vizsgálóbiztosa a Szervezet vezetője. A vizsgálatba a Szervezet vezetője bevonhatja a rendszergazdát, az elektronikus információs rendszer biztonságáért felelős személyt és más külső szakértőket.

A fegyelmi eljárást a vonatkozó jogszabályi rendelkezéseknek megfelelően kell lefolytatni.

A szakértői jelentésről jegyzőkönyv készül, mely a fegyelmi eljárás jegyzőkönyvének része.

A jelentésnek tartalmaznia kell:

- a biztonságsértés időpontját,
- a biztonságsértést elkövető nevét és beosztását,
- a tevékenység által közvetlenül okozott kárt,
- a tevékenységgel közvetve okozható kár becsült mértékét,
- a felelősségre vonás javasolt módját.

Amennyiben az információbiztonsági szabályokat nem a Szervezet személyi állományába tartozó személy sérti meg, a Szervezet vezetőjének felelőssége érvényesíteni a vonatkozó szerződésben meghatározott és alkalmazható jogi és vagyoni

következményeket, továbbá az ő feladata az egyéb jogi lépések lehetőségének vizsgálata, szükség esetén azok alkalmazása.

Ha az IBSZ megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor a szabálysértőt írásban figyelmeztetheti a Szervezet vezetője. A figyelmeztetés utáni ismételt szabályszegést szándékosnak tekintendő. Különösen súlyos esetben, illetve szándékosság esetén a rendszergazdák a használati jogot megvonhatják és az IBSZ megsértője a teljes információs rendszerből kitiltható. Ha szükséges, a Szervezet vezetője (vagy erre feljogosított személy) fegyelmi eljárást, polgári jogi pert is indíthat. Amennyiben az elkövetett cselekmény a Büntető Törvénykönyv szerint bűncselekménynek minősül, a Szervezet vezetője köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

Munkaköri leírások

A Szervezet belefoglalja a biztonsági szerepköröket és felelősségeket a Szervezeti munkaköri leírásokba.

3.15 Kockázatkezelés

Kockázatkezelési Szabályzat és eljárásrendek

A Szervezet vezetője, megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-rel kapcsolatos, kockázatkezelési elvárásokat. A kockázatkezelési szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A kockázatkezelési szabályokat az abban résztvevőkkel (rendszergazda, ügyvezetés) meg kell ismertetni.

A szervezet egyszerű struktúrájából adódóan a kockázatkezeléssel kapcsolatos szabályokkal kapcsolatos tevékenység az IBF és az Ügyvezető feladata és kiterjed a teljes szervezetre. Nem tagolódik egységekre, és így nem szükséges egységek közötti összehangolásra, együttműködésre.

A Szervezet a kockázatkezeléssel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Kockázatkezelési Szabályzat)* kezeli.

Biztonsági osztályba sorolás

A Szervezet vezetője az IBF-fel közösen, biztonsági osztályba sorolja az EIR-t. A rendszerbiztonsági terv részeként dokumentálja a biztonsági osztályba sorolás eredményeit, beleértve az azt alátámasztó indoklást is.

Kockázatelemzés

A Szervezet vezetője az IBF-fel közösen, rendszerszintű kockázatelemzést végez, melyben figyelembe veszik a fenyegetéseket, a sérülékenységeket, a káresemények bekövetkezésének valószínűségét, valamint a Szervezet működésére és eszközeire, az egyénekre, más Szervezetekre és a nemzetre gyakorolt hatásokat. Dokumentálják a kockázatelemzés eredményeit a kockázatelemzési jelentésben. 2 évenkénti gyakorisággal frissíti a kockázatelemzést vagy minden olyan esetben, amikor jelentős változások

történnek a rendszerben, annak működési környezetében, vagy más olyan körülményekben, amelyek befolyásolhatják a rendszer biztonsági állapotát.

Kockázatelemzés – Ellátási lánc

A Szervezet vezetője az IBF-fel közösen a kockázatkezelés keretében felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.

Sérülékenységek ellenőrzése

A Szervezet a kockázatértékelésekor - vagy amikor az EIR-t potenciálisan érintő sérülékenységet azonosítanak, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek - ellenőrzi az EIR sérülékenységeit, majd kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően. Ilyen tevékenységnek tekintendő az NBSZ NKI, a jelentős gyártók, valamint egyéb iparági szereplők által publikált sérülékenységek nyomonkövetése, és a kiadott biztonsági frissítések, valamint új szoftver- és firmware verziók telepítése.

A sérülékenységi szabályokat felülvizsgálni és az informatikai rendszerelemeket azonosítani minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A szabályokat az abban résztvevőkkel (rendszergazda, ügyvezetés) meg kell ismertetni.

Sérülékenységmenedzsment

A Szervezet a fenti folyamat szerint szkenneli az EIR sérülékenységeit a következők szerint:

- felsorolja a platformokat, szoftverhibákat és helytelen konfigurációkat;
- ellenőrző listákat és tesztelési eljárásokat alkalmaz; és
- méri az egyes sérülékenységek hatásait.
- elemzi a sérülékenységmenedzsment jelentéseket és a vizsgálatok eredményeit,
- kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.
- megosztja a sérülékenységmenedzsment folyamatból és a követelmények értékeléséből származó információkat a meghatározott személyekkel vagy szerepkörökkel, hogy segítsenek kiküszöbölni a hasonló sérülékenységeket más rendszerekben.

Sérülékenységmenedzsment – Sérülékenységi adatbázis frissítése

A Szervezet - amennyiben ez alkalmazható - meghatározott gyakorisággal, valamint minden új vizsgálat megkezdése előtt, továbbá új sérülékenységek azonosítása és jelentése esetén frissíti az EIR-ben szkennelt sérülékenységek körét.

Sérülékenységmenedzsment – Felfedezhető információk

A Szervezet a fenti vizsgálatkor feltárja, hogy milyen információk érhetők el az EIR-ről, annak kompromittálása nélkül, és ez alapján szükség esetén korrekciós intézkedéseket hajt végre.

Sérülékenységmenedzsment – Privilegizált hozzáférés

A Szervezet - amennyiben ez alkalmazható - privilegizált hozzáférést biztosít a meghatározott rendszerelemekhez a Szervezet által meghatározott sérülékenységmenedzsment tevékenységek elvégzéséhez.

Sérülékenységmenedzsment – Sérülékenységi információk fogadása

A Szervezet törekszik arra, hogy létrehozzon egy, vagy több csatornát, amelyen keresztül fogadhatja a Szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket. Ez a csatorna lehet az NBSZ NKI által kiadott riasztások, figyelmeztetése.

Kockázatokra adott válasz

A Szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira. A kockázat megfelelő indoklással elfogadható, csökkenthető, megosztható vagy átadható, illetve megszüntethető elveket alkalmazva.

Rendszerelemek kritikusságának elemzése

A Szervezet vezetője az IBSz-el és rendszergazdával együtt, azonosítja a Szervezet működése szempontjából kritikus rendszerelemeket és funkciókat - a meghatározott EIR-ekre, rendszerelemekre vagy rendszerszolgáltatásokra vonatkozó kritikussági elemzés végrehajtásával - a rendszerfejlesztési életciklus meghatározott döntési pontjain.

3.16 Rendszer- és szolgáltatásbeszerzés

Általános szabályok

a) A Szervezet vezetője az informatikai eszközök és szoftverek beszerzésénél mindig a beszerzésekre vonatkozó Szervezeti és a törvényi szabályok szerint jár el. A beszerzett számítástechnikai eszközöket és szoftvereket nyilvántartásba veszi.

b) A rendszergazda, egyeztetve az igénylő osztályok vezetőivel értékeli az igényeket, majd a Szervezet vezetőjével való egyeztetés után, egy fontossági rangsort alkotva, beruházási igényként betervezik a költségvetésbe. Ha nincs az aktuális költségvetésben forrás a beruházásra, akkor nem tervezett beszerzés történik.

c) Az eszközök rendeltetésszerű használatáért a személyi leltár szerint használatra kijelölt személy a felelős.

A szervezet vezetője kinyilvánítja, hogy a beszerzések a szervezettel kapcsolatos belső támadások lehetősége mind a megelőzés mind a felderítés szempontjából egyik létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére.

A beszerzési szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A beszerzési szabályokat az abban résztvevőkkel (rendszergazda, beszerzéssel foglalkozók) meg kell ismertetni.

A szervezet egyszerű struktúrájából adódóan a beszerzési szabályokkal kapcsolatos tevékenység az ügyvezető feladata és kiterjed a teljes szervezetre.

Hardver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Szervezet Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégzi. Ezen felül törekszik az egységes (homogén) eszközpark kialakítására.

Szoftver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Szervezet Informatikai rendszeréhez való illeszthetőségi (kompatibilitási) vizsgálatát elvégzi. Ingyenes (freeware) alkalmazások esetén ellenőrzi hogy üzleti jellegű felhasználásra is szabadon használható-e. A szoftverkörnyezet kialakításánál is törekszik az egységességre (homogenitásra).

A Szervezet számítógépes rendszerében csak legális, jogtiszta szoftverek üzemeltethetőek. További követelmény, hogy a szoftverek integráltan, összehangoltan működjenek. Ezen célok biztosítása érdekében új szoftverek beszerzése kizárólag a rendszergazda véleménye után lehetséges. A beszerzések során az alábbiak megtartása szükséges:

Források

A szoftverek beszerzésére fordítható összegeket a Szervezet költségvetése szabja meg. Az egyes Szervezeti egységek igényeiket a Szervezet vezetője felé a költségvetés összeállítása előtt jelzik. A rendszergazda feladata a szükségszerű cserékről, frissítésekről a Szervezet vezetőjével konzultálni.

A rendszergazda véleményezi a beszerezni kívánt szoftver igényeket, véleménye a szoftver tartalmára és árára egyaránt vonatkozik.

Szoftverek kiválasztása

A szoftverek kiválasztására szóló javaslattétel a rendszergazda feladatkörébe tartozik. A különböző felhasználói igények megfelelő szintű kielégítése érdekében a megfelelő alkalmazói szoftver kiválasztása előtt a rendszergazda konzultál az igénylő iroda szakembereivel.

Beszerzési módok

A kiválasztott szoftverek beszerzése a Szervezet vezetőjének hatásköre.

Szoftver vásárlás

Szoftver vásárlása csak közvetlenül a szoftver gyártójától, vagy annak hivatalos viszonteladójától történhet. A vásárlásnál figyelembe kell venni a tervezett felhasználói számot. A szoftvert a megfelelő számú felhasználói licensszel együtt kell megvásárolni, illetve regisztráltatni.

Külső fejlesztés (outsourcing)

Külső fejlesztést csak fejlesztési szerződés alapján lehet végeztetni. A szerződésnek pontos specifikációt és ütemtervet kell tartalmaznia.

Szoftverek telepítése

Szoftver telepítését csak a rendszergazda, szerződés alapján a beszállító, illetve meghibásodás esetén a karbantartásra szerződött cég végezhet. Ez egyaránt vonatkozik hálózatos szoftverek esetén a szerverre történő telepítésre és a felhasználókhoz való installálásra is.

Jogvédelem

A Szervezet rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtiszta szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtiszta szoftverek tarthatóak. Ennek központi ellenőrzéséről a rendszergazda gondoskodik.

Szoftverek üzemeltetése

A szoftverek üzemeltetési feladatait a rendszergazda látja el. Ez folyamatos tevékenységet igénylő feladat, mind a szoftverkövetés, rendszeres mentés, mind pedig a rendszerhasználat felügyelete, ellenőrzése.

A rendszergazda feladata a felhasználók rendelkezésére állás azok szoftver kezelési, szoftver működési problémáival kapcsolatban. A szoftverek kezelési problémáira helyszíni vagy telefonos segítségnyújtással, dokumentációkkal adhat megoldást.

A felhasználók problémáik megoldását a rendszergazdától közvetlenül kérhetik. A rendszerfelügyelet célja a rendeltetésszerű használat ellenőrzése, biztosítása. Ebbe beletartozik az illegális szoftver- ill. rendszerhasználatok kiderítése és megakadályozása, a vírusfertőzések ellenőrzése, jelentése és megszüntetése éppúgy, mint a nem használt szoftverelemek behatárolása, kivonásukra vagy kiváltásukra történő javaslattétel.

Kellékanyag beszerzés

Az informatikai üzemeltetéshez szükséges irodatechnikai eszközök megfelelő minőségben és mennyiségben történő készletezése a rendszergazdák feladata. Ezekből a kellékekből mindig akkora készlettel rendelkezik mely biztosítja a folyamatos üzletmenetet, ügymenetet.

Beszeerzési Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-rel kapcsolatos, kockázatkezelési elvárásokat.

Erőforrások rendelkezésre állása

Az EIR-vel kapcsolatban saját működtetésben működtetett elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a Szervezet meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházások tervezése részeként. Elkülönítetten kezeli az EIR-vel kapcsolatban saját működtetésű az elektronikus információs rendszerek biztonságát leíró dokumentumokat a beruházás tervezési dokumentációjában.

A rendszer fejlesztési életciklusa

A Szervezet vezetője a rendszergazda segítségével az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri Információbiztonsági helyzetüket.

A Szervezet vezetője a fejlesztési életciklus egészére meghatározza és dokumentáltatja az információbiztonsági szerepköröket és felelősségeket.

A Szervezet vezetője a saját működtetésű elektronikus információs rendszerhez meghatározza és a Szervezetre érvényes szabályok szerint kijelöli az információbiztonsági szerepköröket betöltő, felelős személyeket.

A rendszer életciklus szakaszai a következők:

a) követelmény meghatározás;

b) fejlesztés vagy beszerzés;

c) megvalósítás vagy értékelés;

d) üzemeltetés és fenntartás;

e) kivonás (archiválás, megsemmisítés).

Beszerzések

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű, az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meghatározza:

- a 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.

A védelem szempontjainak érvényesítése a beszerzés során

- A Szervezet vezetője védi az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.
- A Szervezet vezetője ugyancsak szerződéses követelményként határozza meg az EIR-vel kapcsolatban saját működtetésű rendszerrel kapcsolatban a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai

A Szervezet vezetője - amennyiben ez alkalmazható - megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőtől, hogy adjon részletes leírást az alkalmazandó védelmi intézkedések funkcionális tulajdonságairól.

Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez

A Szervezet vezetője - amennyiben ez alkalmazható - megköveteli, hogy az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztője biztosítson tervezési és megvalósítási

információkat a védelmi intézkedésekhez. A tervezési és megvalósítási dokumentáció tartalmazhatja a gyártót, a verziót, a sorozatszámot, az ellenőrző hash aláírást, a használt szoftverkönyvtárakat, a vásárlás vagy letöltés dátumát, valamint a szállítót vagy a letöltés forrását. A forráskód és a hardverséma reprezentálja az EIR megvalósítását.

Beszerzések – Rendszer, rendszerelem és szolgáltatás konfigurációk – Rendszer, rendszerelem és szolgáltatás konfigurációk

A szervezet vezetője, megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás:

- hogy az EIR, rendszerelem vagy szolgáltatás szállítása a meghatározott biztonsági konfigurációk alkalmazásával történhet.
- Minden EIR, rendszerelem vagy szolgáltatás későbbi újratelepítése vagy frissítése során az alapkonfigurációkat kell használni.

Beszerzések – Használatban lévő funkciók, portok, protokollok és szolgáltatások

A Szervezet vezetője, szerződéses rendelkezésként megköveteli a fejlesztőtől, szállítótól, hogy határozza meg a használatra tervezett funkciókat, portokat, protokollokat és szolgáltatásokat. A funkciók, portok, protokollok és szolgáltatások azonosítása a rendszer fejlesztési életciklusának korai szakaszában lehetővé teszi a Szervezetek számára, hogy befolyásolják az EIR, a rendszerelem vagy szolgáltatás tervezését.

Az elektronikus információs rendszerre vonatkozó dokumentáció

A Szervezet beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás **adminisztrátori** és üzemeltetői dokumentációját, amely tartalmazza:

- az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;
- a biztonsági funkciók hatékony használatát és karbantartását;
- az ismert sérülékenységeket a konfigurációval és az Informatikusi vagy privilegizált funkciók használatával kapcsolatban.

Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás **felhasználói** dokumentációját, amely tartalmazza:

- a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;
- a felhasználói interakció biztonságos módját;
- a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.

Biztonságtervezési elvek

A Szervezet vezetője - amennyiben ez alkalmazható - az általa meghatározott biztonságtervezési elveket (pl. többszintű védelem kialakítása, a tervezés és fejlesztés alapjául szolgáló biztonsági irányelvek, architektúra és biztonsági intézkedések kialakítása, a biztonsági követelmények beépítése a rendszerfejlesztési életciklusba) alkalmazza és megköveteli a specifikáció, a tervezés, a fejlesztés, a megvalósítás és az EIR, valamint a rendszerelemek módosítása során.

Külső elektronikus információs rendszerek szolgáltatásai

Amennyiben a Szervezet a saját hatókörében szerez be informatikai szolgáltatást vagy eszközöket, végez vagy végeztet olyan rendszerfejlesztési tevékenységet, amely a Tv. végrehajtási rendeletében meghatározott védelmi követelmények teljesítési kötelezettségét vonná maga után, akkor a Szervezet vezetője

a) szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Szervezet elektronikus információbiztonsági követelményeinek;

b) a vonatkozó rendelet szempontjai szerint a szerződésben meghatározza az érintett Szervezet felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban, így

- a külső Szervezet határozza meg az érintett Szervezettel kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
- a szerződő fél feleljen meg az érintett Szervezet által meghatározott személybiztonsági követelményeknek;
- dokumentálja a személybiztonsági követelményeket;
- ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett Szervezet elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett Szervezetnek;
- ha az elektronikus információbiztonsági szabályokat nem az érintett Szervezet személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja az egyéb jogi lépések fennállásának lehetőségét, szükség szerint bevezeti ezeket az eljárásokat.

c) külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső elektronikus információs rendszer szolgáltatója biztosítja-e az elvárt védelmi intézkedéseket.

Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása

A Szervezet vezetője szükség szerint szerződésben rögzített módon megköveteli a szolgáltatóktól, hogy azonosítsák az általuk nyújtott rendszerszolgáltatásokhoz szükséges funkciókat, portokat, protokollokat és szolgáltatásokat.

Fejlesztői változáskövetés

A Szervezet vezetője, szükség szerint szerződésben megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy

- alkalmazzon konfigurációkezelési folyamatokat az EIR, rendszerelem vagy szolgáltatás tervezése, fejlesztése, bevezetése, üzemeltetése vagy kivonása (teljes életciklusa) során;
- dokumentálja, kezelje és ellenőrizze a Szervezet által a konfigurációkezelés keretében meghatározott konfigurációs elemek változtatásait, és biztosítsa ezek sértetlenségét;

- csak a Szervezet által jóváhagyott változtatásokat hajtsa végre az EIR-en, rendszerelemen vagy rendszerszolgáltatáson;
- dokumentálja a jóváhagyott változtatásokat és ezek lehetséges biztonsági hatásait;
- kövesse nyomon az EIR, rendszerelem vagy rendszerszolgáltatás biztonsági hibáit és azok javításait, továbbá jelentse észrevételeit a Szervezet által meghatározott személyeknek.

Fejlesztői biztonsági tesztelés

A Szervezet vezetője szükség szerint szerződésben megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy

- készítsen biztonságértékelési tervet, és hajtsa végre az abban foglaltakat;
- meghatározott gyakorisággal hajtson végre (a fejlesztéshez illeszkedő módon) egység-, integrációs-, rendszer-, illetve regressziós tesztelést, és értékelje ki a Szervezet által meghatározottak szerint;
- dokumentálja, hogy végrehajtotta a biztonságértékelési tervben foglaltakat, és ismertesse a biztonsági tesztelés és értékelés eredményeit;
- vezessen be egy ellenőrizhető hibajavítási folyamatot;
- javítsa ki a tesztelés és értékelés során azonosított hibákat.

Fejlesztési folyamat, szabványok és eszközök

A Szervezet vezetője szükség szerint szerződésben megköveteli a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy

- dokumentált fejlesztési folyamatot kövessen;
- kiemelten kezelje a biztonsági követelményeket;
- határozza meg a fejlesztés során alkalmazott szabványokat és eszközöket;
- dokumentálja a fejlesztés során alkalmazott speciális eszköz konfigurációkat és opciókat;
- tartsa nyilván a változtatásokat, és biztosítsa ezek jogosulatlan változtatás elleni védelmét; továbbá
- előírja, hogy az általa meghatározott biztonsági követelményeknek való megfelelés érdekében általa meghatározott gyakorisággal a fejlesztő tekintse át a fejlesztési folyamatot, szabványokat, eszközöket és eszköz opciókat, konfigurációkat.

Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés

A Szervezet vezetője szükség szerint szerződésben megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy végezzen kritikussági elemzést a rendszerfejlesztési életciklus alatt, a Szervezet által meghatározott döntési pontokon és megfelelő szigorúsággal.

Szoftverfejlesztők oktatása

A szervezet vezetője kötelezi a rendszerfejlesztőt, hogy biztosítson képzést a szoftverfejlesztőknek a megvalósított biztonsági funkciók, szabályozások és mechanizmusok helyes használatáról és működéséről.

Fejlesztői biztonsági architektúra és tervezés

A szervezet vezetője megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy olyan tervezési specifikációt és biztonsági architektúrát hozzon létre, amely:

- Illeszkedik a szervezet biztonsági architektúrájához és támogatja azt.
- Leírja a szükséges biztonsági funkciókat, valamint a védelmi intézkedések megosztását a fizikai és logikai összetevők között.
- Bemutatja az egyes biztonsági funkciók, mechanizmusok és szolgáltatások együttműködését az előírt biztonsági követelmények megvalósításában, valamint a védelem egységes megközelítésében.

Külső fejlesztők háttérellenőrzése

A szervezet vezetője megköveteli az EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőjétől, hogy:

- rendelkezzen a hivatalos feladatok alapján meghatározott megfelelő hozzáférési jogosultságokkal; és
- teljesítse a szervezet által meghatározott (pl. biztonsági átvilágítások, háttérellenőrzések, állampolgárság és a nemzetiség ellenőrzése) átvilágítási kritériumokat.

Támogatással nem rendelkező rendszerelemek

A Szervezet vezetője megköveteli az EIR-t működtetőtől, hogy cserélje le a rendszerelemeket, amikor azok támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól; illetve amennyiben megvalósítható, a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást biztosít, amelyet belső erőforrásokkal vagy a Szervezet által meghatározott külső szolgáltatók bevonásával valósít meg.

3.17 Rendszer- és kommunikációvédelem

Rendszer- és kommunikációvédelmi Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti és kötelezővé teszi az EIR-rel kapcsolatos, rendszer és kommunikációvédelmi elvárásokat az IBF, Rendszergazda és a szervezet vezetésének.

A szervezet vezetője kinyilvánítja, hogy a személyi biztonság a szervezettel kapcsolatos belső támadások lehetősége mind a megelőzés mind a felderítés szempontjából egyik létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére.

A személyi biztonsági szabályok alapvető célja, hogy a szervezetben és a szervezeten kívüli felhasználók a jogosultság megszerzése előtt ellenőrizni és bizonyítani lehessen az arra való alkalmasságukat. Az ellenőrzésért felelős a felhasználó felvételének kezdeményezője, ill. a központosított munkaerőfelvétel felelőse.

A rendszer- és kommunikációvédelmi szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A rendszer- és kommunikációvédelmi szabályokat az abban résztvevőkkel (munkaerőfelvétellel, beszerzéssel foglalkozók) meg kell ismertetni.

A szervezet vezetője, a rendszer- és kommunikációvédelmi szabályok kritériumainak megállapítására egy célt tűzött ki. A sikeres nem felderített incidensek száma, ami a

rendszer- és kommunikációvédelmi szabályok helytelen alkalmazására vezethető vissza (0%).

A Szervezet a rendszer és kommunikációvédelemmel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Rendszer- és kommunikációvédelmi Szabályzat)* kezeli.

A rendszer- és kommunikációvédelem megvalósítása során a Szervezet vezetője az IBSZ követelményei szerint jár el, valamint alkalmazza a biztonságtervezési eljárásrendben foglaltakat.

A fentieken túlmenően – de azokkal összhangban – a Szervezet az alábbi követelményeket fogalmazza meg a rendszer- és kommunikációvédelem érdekében:

A hálózat használatának szabályai

A Szervezet hálózata nem használható az alábbi tevékenységekre:

- a hálózat, a kapcsolódó hálóztok, illetve ezek erőforrásainak rendeltetésszem működését és biztonságát zavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése
- a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásokat indokolatlanul igénybe vevő tevékenységek
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, gépek/szolgáltatások - akár tesztelés céljából történő - túlzott mértékben való szisztematikus próbálgatása
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítása, megrongálása, megsemmisítése, vagy bármely károkozásra irányuló tevékenység
- hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna.

A felhasználók kötelességei

A felhasználók kötelessége a Szabályzat megismerése és az abban foglaltak betartása, valamint együttműködés a hálózat üzemeltetőjével a Szabályzat betartása érdekében a felhasználó viseli a felelősséget minden műveletért, amely az adott felhasználó azonosítóval kerül végrehajtásra.

A felhasználók jogai

- Minden Szervezeti dolgozónak joga van saját felhasználói fiókhoz és levelezéshez (e- mail címhez) és a munkavégzéshez szükséges web szolgáltatáshoz
- A felhasználó személyiségi jogait és a levéltitkot a hálózat üzemeltetője tiszteletben tartja, ettől eltérni csak jogszabály által meghatározott esetekben lehet
- A rendszer technikai karbantartásairól tájékoztatni kell a felhasználókat, hogy kellő idő maradjon a felhasználók felkészülésére. A karbantartásokat lehetőleg hivatalos munkaidőn kívül kell lebonyolítani.

A felhasználók regisztrálásának szabályai

- Felhasználó a Szervezet dolgozója lehet.
- A felhasználói azonosítók kiadása központilag a felelős rendszergazda által történik.

- A felhasználót az azonosító átadásakor tájékoztatni kell a használat feltételeiről és szabályairól. A tájékoztatást követően a felhasználó aláírásával igazolja, hogy azokat megismerte és magára nézve kötelezőnek ismerte el.
- Az EIR-hez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni annak használatáról.
- A felhasználói azonosítót le kell tiltani, ha azzal visszaélés történt és az esetet ki kell vizsgálni
- A felhasználó azonosítókat a rendszerből törölni kell, ha felhasználó már nem a Szervezet dolgozója, illetve az adott rendszer használatához már nincs joga. A törlést az érintett Szervezeti egység vezetője kezdeményezi a rendszergazdánál.
- A rendszergazda a felhasználói azonosítókról és kapcsolódó hozzáférési jogosultságokról teljeskörű és naprakész nyilvántartást vezet. A nyilvántartásnak tartalmaznia kell azon felhasználói azonosítókat és kapcsolódó jelszavakat, hozzáférési jogosultságokat, amelyek más, nem a Szervezet rendszeréhez tartoznak, de valamely feladat kapcsán a Szervezet vagy a Szervezet dolgozója hozzáférést igényelt, kapott ahhoz (pl pályázati rendszerhez történő hozzáférés, Cégkapuhoz történő hozzáférés) A nyilvántartásba vételt az érintett Szervezeti egység vezetője írásban kezdeményezi.

Rendszer és felhasználói funkciók szétválasztása

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy válassza szét a felhasználók által elérhető funkciókat - beleértve a felhasználói interfész szolgáltatásait - a rendszer üzemeltetési funkcióktól. A felhasználói funkciók szétválasztása a rendszerüzemeltetési funkcióktól történhet fizikai vagy logikai szinten. A Szervezet külön számítógépekkel, különböző központi feldolgozóegységekkel, operációsrendszerek különböző példányaival, külön hálózati címekkel, virtualizációs technikákkal vagy ezek kombinációival valósíthatja meg a rendszerüzemeltetéssel kapcsolatos funkciók szétválasztását a felhasználói funkcióktól.

Biztonsági funkciók elkülönítése

A szervezet vezetője, kötelezi az informatikai osztály vezetőjét, hogy különítse el az EIR a biztonsági funkciókat a nem biztonsági funkcióktól (pl. rendszeren belül partíciók és tartományok segítségével megvalósított határokkal).

Információk az osztott használatú rendszererőforrásokban

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR gátolja meg a megosztott erőforrásokon keresztül történő jogosulatlan vagy véletlen információátvitelt, megakadályozza, amikor a korábbi felhasználók vagy szerepkörök által végzett tevékenységek információihoz (beleértve a titkosított információkat) hozzáférjenek a megosztott erőforrások (pl. regiszterek, memória, merevlemezek) jelenlegi felhasználói (vagy folyamatai), miután azokat az információs rendszer felszabadította.

Szolgáltatásmegtagadással járó támadások elleni védelem

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy - amennyiben ez értelmezhető és kivitelezhető - alakítson ki védelmet a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait és

alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével csökkentheti annak sikerességét.

A határok védelme

A Szervezet vezetője a belső hálózat védelmének biztosítása érdekében kötelezi az EIR működéséért felelős rendszergazdát, hogy határvédelmi megoldást (tűzfal) működtessen a hálózati forgalom felügyeletére, irányítására. Az így kialakított megoldás

a) felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;

b) a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a Szervezet belső hálózatától;

c) csak a Szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

A határok védelme – Hozzáférési pontok

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy korlátozza az EIR külső hálózati kapcsolatainak számát. Így a külső hálózati kapcsolatok számának korlátozása megkönnyíti a bejövő és kimenő kommunikációs forgalom felügyeletét.

A határok védelme – Külső infokommunikációs szolgáltatások

A Szervezet vezetője, - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az interfészek védelmével akadályozza meg a nem engedélyezett vezérlőadat-forgalom (control plane traffic) (vezérlőadat-forgalmára példa: BGP, DNS és kezelési protokollok) cseréjét a külső hálózatokkal. Ez azt jelenti, hogy az EIR blokkolja azokat az adatokat, amelyeket nem szabadna átvinni a külső hálózatokra.

A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a beállításokban az EIR alapértelmezés szerint utasítja el a hálózati kommunikációs forgalmat, és csak kivételként engedélyezi azt a menedzselt interfészeknél.

A határok védelme – Megosztott csatornahasználat távoli eszközök esetén

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a beállításokban az EIR akadályozza meg a megosztott csatornahasználatot az EIR-ekhez csatlakozó távoli eszközök számára, kivéve, ha a megosztott csatornát biztonságosan konfigurálják a Szervezet által meghatározott védelmi intézkedések használatával.

A határok védelme – A forgalom átirányítása hitelesített proxykiszolgálókra

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR a meghatározott belső kommunikációs forgalmat a

meghatározott külső hálózatok felé a menedzselt interfészeken lévő hitelesített proxykiszolgálókon keresztül irányítsa.

A határok védelme – Biztonságos állapot fenntartása

Az informatikai osztály vezetője úgy alakítja ki a határvédelmi rendszereket, hogy azok megakadályozzák, hogy az EIR nem biztonságos állapotba kerüljön egy határvédelmi berendezés működési hibája esetén. A határvédelmi eszközök meghibásodásai nem vezethetnek információk külső eszközbe jutásához, és a meghibásodások nem tehetik lehetővé a jogosulatlan információkiadást.

A határok védelme – Rendszerelemek elkülönítése

Az informatikai osztály vezetője úgy alakítja ki a határvédelmi mechanizmusokat, hogy a szervezet által meghatározott rendszerelemeket (routerek, átjárók és a tűzfalak, segítségével, elkülönülő hálózatokra vagy alhálózatokra osztják, vagy az alhálózatokat elválasztó kereszt-tartományú eszközök, virtualizációs technikák és a rendszerelemek közötti információáramlás titkosítása segítségével) elkülönítse.

Az adatátvitel bizalmassága és sértetlensége

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a beállításokban az EIR védje meg a továbbított információk bizalmasságát és sértetlenségét.

Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR-ben kriptográfiai mechanizmusokat alkalmazzon az adatátvitel során, hogy megelőzze az információk jogosulatlan felfedését, illetve kimutassa az információk módosításait.

A hálózati kapcsolat megszakítása

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR szakítsa meg a hálózati kapcsolatot mind belső, mind külső hálózatokban a kommunikációs munkaszakasz befejezésekor vagy meghatározott időtartamú inaktivitás után.

Kriptográfiai kulcs előállítása és kezelése

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Szervezet állítson elő és kezeljen kriptográfiai kulcsokat a Szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.

Kriptográfiai kulcs előállítása és kezelése - Rendelkezésre állás

A szervezet biztosítja az információk rendelkezésre állását abban az esetben is, amikor a felhasználók elveszítik a kriptográfiai kulcsaikat.

Kriptográfiai védelem

A Szervezet vezetője - amennyiben ez alkalmazható - meghatározza a kriptográfia Szervezeten belüli felhasználási területeit és megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.

Együttműködésen alapuló számítástechnikai eszközök

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy gátolja meg az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha az érintett Szervezet engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a személyeknek, akik fizikailag jelen vannak az eszköznél.

Nyilvános kulcsú infrastruktúra tanúsítványok

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy szükség szerint nyilvános kulcsú tanúsítványokat állítson ki a Szervezet által meghatározott tanúsítványkiadási szabályok szerint, vagy nyilvános kulcsú tanúsítványokat szerez be egy bizalmi szolgáltatótól és a Szervezet által kezelt tanúsítványtárolókban, csak jóváhagyott, hitelesített tanúsítvány vehető fel.

Mobilkód korlátozása

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy határozza meg az elfogadható és a nem elfogadható mobilkódokat, valamint a mobilkód technológiákat (a mobilkód-technológiák közé tartozik például a Java, a JavaScript, a HTML5, a WebGL és a VBScript), valamint, felügyelje és ellenőrizze a mobilkódok használatát az EIR-en belül.

Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a név- és címfeloldási kérésekre (A név- és címfeloldási szolgáltatásokat nyújtó információs rendszerek közé tartoznak például a DNS-kiszolgálók. A további lehetőségek közé tartozik például a DNS biztonsági elektronikus) a hiteles névfeloldási adatokon kívül az információ eredetére és a tartalom sértetlenségére vonatkozó kiegészítő adatokat is biztosítsa. Amennyiben egy elosztott, hierarchikus névtér részeként működik, jelezze a gyermektartományok biztonsági állapotát is, és ha azok támogatják a biztonságos névfeloldási szolgáltatásokat, tegye lehetővé a szülő- és gyermektartományok közötti bizalmi lánc ellenőrzését.

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

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR eredet-hitelesítést és adatsértetlenség-ellenőrzést kérjen és hajtson végre a hiteles forrásból származó név- és címfeloldó válaszokon.

Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Szervezet számára név- és címfeloldási szolgáltatást

együttesen biztosító EIR-ek hibatűrő képességgel rendelkezzenek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.

Munkaszakasz hitelessége

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR védje a kommunikációs munkaszakaszok (munkaszakaszra fókuszálva, nem pedig csomagszinten vizsgálva) hitelességét. A hitelességgel kapcsolatos védelmi intézkedések magában foglalják például a közbeékelődéses (man-in-the-middle) támadások/munkaszakasz-eltérítések és a hamis információk munkaszakaszba illesztése elleni védelmet is.

Ismert állapotba való visszatérés

Az informatikai osztály vezetője, ahol ez megvalósítható, úgy alakítja ki a rendszer meghatározott rendszerelemeit, hogy azok meghatározott hibák bekövetkezése estén őrízzék meg a hiba bekövetkezése előtti ismert rendszerállapotukat. Így a hiba bekövetkezése előtti ismert állapot megőrzése megakadályozza, hogy a rendszerek olyan állapotba kerüljenek, amely személyi sérülést vagy vagyonelemek megsemmisülését okozhatják.

Tárolt (at rest) adatok védelme

A Szervezet vezetője, - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Szervezetben óvja meg a meghatározott tárolt, illetve archivált (at rest) adatok (tárolt információk arra az állapotra utalnak, amikor az információk kifejezetten a rendszerösszetevők tárolóeszközein helyezkednek el és éppen nem állnak feldolgozás vagy továbbítás alatt) bizalmasságát és sértetlenségét a feldolgozás vagy továbbítás alatt álló adatokkal megegyező szinten.

Tárolt (at rest) adatok védelme – Kriptográfiai védelem

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmazzon a Szervezet által meghatározott tárolt vagy archivált adatok jogosulatlan felfedésének és módosításának megelőzésére.

Folyamatok elkülönítése

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Szervezet elektronikus információs rendszereit egymástól elkülönítetten (végrehajtási tartományban tartja) működteti minden végrehajtó folyamatban. Mindegyik EIR folyamatnak egy külön címtartománya legyen, így a folyamatok közötti kommunikáció a biztonsági funkciók által ellenőrzött módon történhet, és az egyik folyamat nem tudja módosítani egy másik folyamat végrehajtó kódját.

3.18 Rendszer- és információsértetlenség

Információsértetlenségi Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-rel kapcsolatos, rendszer és információsértetlenségi elvárásokat.

A szervezet vezetője kinyilvánítja, hogy a rendszer- és információsértetlenség a szervezettel kapcsolatos belső támadások lehetősége mind a megelőzés mind a felderítés szempontjából egyik létfontosságú eleme. Emiatt, annak kialakítását és ellenőrzési mechanizmusát elkötelezetten támogatja, forrásokat biztosít annak működtetésére.

A rendszer- és információsértetlenség szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. A rendszer- és kommunikációvédelmi szabályokat az abban résztvevőkkel (rendszergazdal) meg kell ismertetni.

A szervezet vezetője, a rendszer- és információsértetlenség szabályok kritériumainak megállapítására egy célt tűzött ki. A sikeres nem felderített incidensek száma, ami a rendszer- és információsértetlenség szabályok helytelen alkalmazására vezethető vissza (0%).

A Szervezet a rendszer- és kommunikációvédelemmel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Rendszer- és információsértetlenségi Szabályzat)* kezeli.

Hibajavítás

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy

a) azonosítsa, belső eljárásrendje alapján jelentse és javítsa, vagy javíttassa az elektronikus információs rendszer hibáit;

b) telepítés előtt tesztelje a hibajavítással kapcsolatos szoftverfrissítéseket a Szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;

c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepítse, vagy telepíttesse;

d) építise be a hibajavítást a konfigurációkezelési folyamatba.

Hibajavítás – Automatizált hibaelhárítás állapota

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy szükséges és elégséges gyakorisággal automatizált mechanizmusokat alkalmazzon annak ellenőrzésére, hogy a rendszerelemek rendelkeznek-e a biztonsági szempontból releváns szoftver- és firmware-frissítésekkel.

Kártékony kódok elleni védelem

A Szervezet vezetője, kötelezi az EIR működéséért felelős rendszergazdát, hogy

a) az elektronikus információs rendszerét annak belépési és kilépési pontjain védje a kártékony kódok ellen, felderítse és semmisítse meg azokat;

b) frissítse a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

A rendszergazda konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

a) rendszeres ellenőrzéseket hajt végre az elektronikus információs rendszeren és végrehajtja a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon a hálózati belépési, vagy kilépési pontokon a biztonsági Szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják;

b) a kártékony kód észlelése esetén blokkolja vagy karanténba helyezi azt; és riasztja a rendszeradminisztrátort és az érintett Szervezet által meghatározott további személy(eke)t;

c) ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

d) A Szervezet minden munkaállomásán és szerverén jogtiszta vírusvédelmi rendszert üzemeltet, mely minden, az adathálózatról fogadott illetve oda továbbított adatállományt átvizsgál.

e) A felhasználó rendelkezésére bocsátott informatikai eszközön vírusvédelmi rendszert üzemeltet. A vírusvédelmi rendszert a felhasználónak tilos kikapcsolnia vagy módosítania, illetve tilos módosítani annak beállításait. Abban az esetben, ha a vírusvédelmi rendszer vagy a felhasználó kártékony kódot – pl.: vírust -, vagy annak gyanúját észleli, akkor a felhasználó kötelessége azonnal jelenteni az eseményt az adott eszköz üzemeltetési feladataival megbízott rendszergazdának.

f) A felhasználónak tilos a rendelkezésére bocsátott informatikai eszközökön szándékosan kártékony kódokat, illetve Szervezet Információbiztonsági rendszereinek állapotát bármilyen formában feltérképező szoftvereket tárolni, működtetni, módosítani (mutációkat létrehozni), illetve fejleszteni.

g) A felhasználónak tilos a biztonsági szoftvereket kikapcsolni, működésüket módosítani,

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani. A vírusvédelmi programok adatbázisát naprakészen kell tartani. Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, informatikusnak. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, informatikus meg nem vizsgálta. A vírusfertőzést jelenteni kell a Szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a Szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

A szervezet vezetője megköveteli, hogy aláírás-alapú védelmi mechanizmusokat alkalmazzanak a kártékony kódok elleni védekezés során, pl. előre ismert minták (ún. *szignatúrák*) alapján azonosítják a fenyegetéseket.

Az EIR monitorozása

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy a rendelkezésre álló információbiztonsági eszköz és alkalmazás segítségével

- felügyelje az elektronikus információs rendszert, észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
- azonosítsa az elektronikus információs rendszer jogosulatlan használatát;
- felügyeleti eszközöket alkalmazzon a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;
- védje a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
- erősítse az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;
- meghatározott gyakorisággal biztosítsa az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

Az EIR monitorozása – Automatizált eszközök és mechanizmusok valós idejű elemzéshez

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél automatikusan frissítse a kártékony kódok elleni védelmi mechanizmusokat.

Az EIR monitorozása – Bejövő és kimenő kommunikációs forgalom

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a bejövő és kimenő kommunikációs forgalomra vonatkozóan kritériumokat állítson fel a szokatlan vagy nem engedélyezett tevékenységek és körülmények azonosítására. Szükség szerint ellenőrzi a bejövő és kimenő kommunikációs forgalmat a szokatlan vagy jogosulatlan tevékenységek vagy körülmények tekintetében.

Az EIR monitorozása – Rendszer által generált riasztások

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy EIR-t úgy alakítsa ki, hogy az riasztást küldjön a meghatározott személyeknek vagy szerepköröknek, amikor a rendszer által generált meghatározott indikátorok a rendszer potenciális kompromittálódására utaló jeleket mutatnak.

Az EIR monitorozása – Az titkosított kommunikáció láthatósága

A szervezet vezetője intézkedéseket tesz arra, hogy a meghatározott titkosított kommunikációs forgalom átlátható legyen a meghatározott rendszerfelügyeleti eszközök és mechanizmusok számára.

Az EIR monitorozása – Automatikusan generált szervezeti riasztások

Az informatikai osztály vezetője úgy alakítja ki a rendszereket, hogy azok riasztást küldjenek az általa meghatározott személyeknek vagy munkaköröknek, ha olyan meghatározott, nem megfelelő vagy szokatlan tevékenységek történnek, amelyek biztonsági következményekkel járó tevékenységekre utalnak.

Az EIR monitorozása – Vezeték nélküli behatolást érzékelő rendszer

Az informatikai osztály vezetője, ha ez kivitelezhető, egy vezeték nélküli behatolást érzékelő rendszert használ, amely képes felismerni a nem engedélyezett vezeték nélküli eszközöket, valamint észlelni a támadási kísérleteket és a rendszer potenciális kompromittálását vagy sérülését.

Az EIR monitorozása – Privilegizált felhasználók

Az informatikai osztály vezetője, az EIRe-k jogosultság felülvizsgálata során külön odafigyeléssel ellenőrzi a privilegizált felhasználókat.

Az EIR monitorozása – Engedély nélküli hálózati szolgáltatások

Az informatikai osztály vezetője úgy alakítja ki a hálózati rendszereit:

- hogy észlelje azokat a hálózati szolgáltatásokat, amelyeket a szervezet által meghatározott engedélyezési és jóváhagyási folyamatok alapján nem engedélyezettek vagy nem hagytak jóvá; és
- naplózza a nem engedélyezett hálózati szolgáltatások észlelését, és egyben riasztást küldjön az informatikai osztály vezetőjének ill. az általa megbízott személynek, a nem engedélyezett észlelésekor.
- az így alkalmazott „Eszközmenedzsment rendszer" automatikus működéséért, frissítéséért, annak biztosításáért, hogy a felhasználókat kizára a rendszer befolyásolásából;
- Amennyiben egy szolgáltatást kihelyez a szervezet (pl. üzemeltetés), akkor a szerződésekben, vagy külön jogi állásfoglalásban kell tisztázni, hogy ki, milyen szinten felelős a biztonsági követelmények teljesítéséért.

Biztonsági riasztások és tájékoztatások

A Szervezet vezetője az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél

- folyamatosan figyeli, illetve az Információbiztonsági felelősön keresztül figyelteti a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri, illetve az Információbiztonsági felelősön keresztül figyelteti a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket;
- szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki;
- a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
- kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart, illetve az Információbiztonsági felelősön keresztül tartat az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz, vagy intézkedik annak tételére a megbízott személyekkel, Szervezetekkel.

Biztonsági riasztások és tájékoztatások - Automatizált figyelmeztetések és tanácsok

Az informatikai osztály vezetője biztonsági riasztásokat és tanácsokat tesz közzé az egész szervezeten belül az e-mail hálózat segítségével.

Biztonsági funkciók ellenőrzése

Az informatikai osztály vezetője:

- Ellenőrzi a meghatározott biztonsági funkciók helyes működését.
- Az előírt gyakorisággal a megfelelő jogosultsággal rendelkező felhasználók utasítására végrehajtja a meghatározott rendszerállapot-változásokat kezelő funkciók (például: indítás, újraindítás, leállítás) ellenőrzését.
- Figyelmezteti a meghatározott személyeket vagy szerepköröket a fentiek sikertelensége esetén.
- Amennyiben rendellenességeket észlel, leállítja vagy újraindítja a rendszert, illetve a szervezet által meghatározott alternatív intézkedéseket hajt végre.

Szoftver- és információsértetlenség

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy sértetlenségellenőrző eszközöket alkalmazzon, annak érdekében, hogy észlelje a jogosulatlan változtatásokat a meghatározott szoftverekben, firmware-ekben és információkban, hogy szükség szerint intézkedéseket hajtson végre, amikor engedély nélküli változásokat észlel a szoftverekben, firmware-ekben vagy az információkban.

Szoftver-, firmware- és információsértetlenség – Sértetlenség ellenőrzése

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy az EIR-n szükséges gyakorisággal sértetlenségellenőrzést végezzen a meghatározott szoftvereken, firmware-eken és információkon, a rendszer indításakor, az átmeneti rendszerállapotokban vagy a biztonsági szempontból releváns események esetén.

Szoftver-, firmware- és információsértetlenség – Automatikus értesítések az sértetlenség megszűnéséről

A szervezet olyan automatizált eszközöket alkalmaz, amelyek értesítik a kijelölt személyeket vagy szerepköröket, amennyiben a sértetlenségellenőrzés során eltéréseket észlelnek.

Szoftver-, firmware- és információsértetlenség – Automatikus reagálás

Az EIR automatikusan leáll, vagy újraindul, vagy végrehajtja a szervezet által meghatározott intézkedéseket, amennyiben a sértetlenségellenőrzés során rendellenességet észlel.

Szoftver- és információsértetlenség – Észlelés és a válaszadás integrálása

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy a rendszer biztonsága szempontjából releváns jogosulatlan változtatások észlelését integrálja a Szervezet biztonsági eseményeket kezelő rendszerébe.

Szoftver- és információsértetlenség – Kódok hitelesítése

Az informatikai osztály vezetője kriptográfiai mechanizmusokat alkalmaz a meghatározott szoftver- vagy firmware-elemek hitelesítésére a telepítés előtt.

Kéretlen üzenetek elleni védelem

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy olyan levélszemét elleni védelmet valósít meg az EIR belépési és kilépési pontjain, amelyek felismerik és kezelik az ilyen üzeneteket és új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat a konfigurációkezelési szabályokkal összhangban.

Kéretlen üzenetek elleni védelem – Automatikus frissítések

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy meghatározott gyakorisággal automatikusan frissítse a levélszemét elleni védelmi mechanizmusokat.

Bemeneti információ ellenőrzés

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél ellenőrizze a meghatározott információ belépési pontok érvényességét, hogy a bemenetek megfelelnek-e a meghatározott formai és a tartalmi követelményeknek.

Hibakezelés

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy olyan hibajelzéseket állítson elő, amelyek a hibák kijavításához szükséges információkat szolgáltatnak anélkül, hogy kihasználható információkat tárnának fel a hibaüzeneteket csak a meghatározott személyeknek vagy szerepköröknek teszi elérhetővé.

Információ kezelése és megőrzése

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy az elektronikus információs rendszer kimeneti információit a jogszabályokkal, Szabályzatokkal és az üzemeltetési követelményekkel összhangban kezelje és őrizze meg. Az IBF felelős a mindenkori vonatkozó jogszabályok figyeléséért és ha azokban változás áll be, kezdeményezni a szabályozók és a gyakorlat változtatását.

Memóriavédelem

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy meghatározott védelmi intézkedéseket alkalmazzon annak érdekében, hogy megvédje a rendszermemóriát a jogosulatlan kódok végrehajtásától. A memória védelme érdekében alkalmazott biztonsági biztosítékok közé tartozik például a DEP (Data Execution Prevention) és az ASLR (Address Space Layout Randomization).

3.19 Ellátási lánc kockázatkezelése

Ellátási láncok kockázata Szabályzat és eljárásrendek

A Szervezet vezetője megfogalmazza és a Szervezetre érvényes követelmények szerint dokumentálja, valamint a Szervezeten belül kihirdeti az EIR-rel kapcsolatos, ellátási lánc kockázatokat, elvárásokat.

Az ellátási láncok kockázatai szabályokat, minden rendkívüli esemény, incidens, auditok alakalmával vagy jelentős EIR beszerzésnél, de legkésőbb évente felül kell vizsgálni és szükség szerint módosítani. A módosítást a rendszergazda és az IBF végzi a management döntései alapján. Az ellátási láncok kockázatai az abban résztvevőkkel (rendszergazdal) meg kell ismertetni.

Az ellátási láncok kockázatai szabályok jogosulatlan módosítása elleni védekezés okán a szabályzatot a dokumentumkezelési szabályok szerint, egy pdf formátumban kell tárolni az arra jogosultak számára. Az eredeti szerkeszthető változatot elkülönített módon, védve kell tárolni.

Ellátási láncra vonatkozó kockázatmenedzsment Szabályzat

A Szervezet vezetője az IBF-fel közösen a kockázatértékelés alkalmával beépíti a meghatározott EIR-ek, rendszerelemek vagy rendszerszolgáltatások (kutatás-fejlesztés, tervezés, gyártás, beszerzés, szállítás, integráció, üzemeltetés és karbantartás, kivezetés, valamint a selejtezés) során felmerülő ellátási lánccal kapcsolatos kockázatok kezelését is. A tevékenységek, amelyek növelhetik a biztonsági vagy adatvédelmi kockázatokat, magukban foglalják a jogosulatlan gyártást, a hamisítványokra való cserét, vagy azok használatát, a módosításokat, a lopást, a rosszindulatú szoftverek és hardverek beillesztését, valamint a nem megfelelő gyártási és fejlesztési gyakorlatot az ellátási láncban.

Ellátási láncra vonatkozó követelmények és folyamatok

Szervezet vezetője az IBF-fel közösen a kockázatértékelés alkalmával folyamatot alakít ki, hogy azonosítsa és kezelje a gyengeségeket vagy hiányosságokat a meghatározott EIR ellátási láncának elemeiben és folyamataiban, a Szervezet által meghatározott ellátási láncért felelős személyekkel együttműködve. Az ellátási lánc folyamatai magukban foglalják a hardver-, szoftver- és firmware-fejlesztési folyamatokat; a szállítási és kezelési eljárásokat; a személyi és fizikai biztonsági programokat; a konfigurációs menedzsment eszközeit, technikáit és intézkedéseit az eredetiség biztosítására; vagy más programokat, folyamatokat vagy eljárásokat, amelyek az EIR és a rendszerelemeinek fejlesztésével, beszerzésével, karbantartásával és selejtezésével kapcsolatosak.

Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók

A Szervezet vezetője megköveteli, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.

Beszerzési stratégiák, eszközök és módszerek

Stratégiák az ellátási lánc kockázatai ellen

Beszállítói due diligence (átvilágítás)

Új partnerek, alvállalkozók biztonsági megfelelőségének vizsgálata.

Példák: ISO 27001 tanúsítvány, NIS2 megfelelés, pénzügyi stabilitás.

Szerződéses biztosítékok

SLA-k és szerződéses záradékok, amelyek előírják a kiberbiztonsági intézkedéseket (pl. incidensjelentési kötelezettség, biztonsági audit engedélyezése).

Hozzáférés- és jogosultságkezelés

„Minimum szükséges jogosultság" elve (least privilege).

Külső partnerek hozzáférésének korlátozása, ideiglenes vagy elkülönített fiókok.

Redundancia és diverzifikáció

Ne legyen teljes függés egyetlen beszállítótól.

Kritikus komponensekhez alternatív beszerzési forrás fenntartása.

Folyamatos monitoring és auditálás

Beszállítói teljesítmény és biztonsági szint rendszeres ellenőrzése.

Harmadik fél által végzett biztonsági auditok, penetration testek.

Incident response integráció

Beszállítók bevonása a szervezet incidenskezelési folyamatába.

Kapcsolattartási pontok előre rögzítése.

Tudatosság és képzés

Saját dolgozók és partnerek tájékoztatása a beszállítói láncot érintő kockázatokról (pl. social engineering).

Eszközök és módszerek

Kockázatértékelő keretrendszerek

NIST Cyber Supply Chain Risk Management (C-SCRM),

ISO 28000 (ellátási lánc biztonsági irányítási rendszer).

Biztonsági szabványok és tanúsítványok

ISO 27001, TISAX, SOC 2 → bizonyítják a beszállító biztonsági szintjét.

Technológiai eszközök

Vulnerability Management: beszállítói szoftverek sérülékenység-vizsgálata.

SBOM (Software Bill of Materials): szoftverkomponensek eredetének nyomon követése.

Zero Trust megközelítés: minden kapcsolatot ellenőrizni kell, még a belső/beszállítói forgalmat is.

SIEM / SOC: beszállítói integrációk naplóinak folyamatos figyelése.

Jogosultság- és hozzáférés-kezelő rendszerek

PAM (Privileged Access Management), IAM rendszerek.

Folyamatos biztonsági monitoring szolgáltatások

Threat intelligence szolgáltatások, amelyek jelzik, ha egy beszállító kompromittálódott.

Beszállítók értékelése és felülvizsgálata

A Szervezet vezetője a kockázatértékelések gyakoriságakor értékeli és felülvizsgálja a beszállítókkal vagy szerződéses partnerekkel, illetve az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat is.

Értesítési megállapodások

A Szervezet vezetője szükség szerint megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő Szervezetekkel.

Hamisítás elleni védelem

A szervezet vezetője hamisítás elleni védelmi programot vezet be a rendszer, rendszerelem vagy rendszerszolgáltatás védelmére.

Hamisítás elleni védelem - Rendszerfejlesztési életciklus

A szervezet vezetője hamisítás elleni technológiákat, eszközöket és technikákat alkalmaz a teljes rendszerfejlesztési életciklus során.

Rendszerek vagy rendszerelemek vizsgálata

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy eseti jelleggel vagy meghatározott gyakorisággal és meghatározott esetekben ellenőrizze az EIR-eket vagy rendszerelemeket az esetleges hamisítás felderítése érdekében.

Rendszerelem hitelessége

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy tegyen lépéseket a hamisított rendszerelemek észlelésére és annak megelőzésére, hogy ezek bejussanak az EIR-be, továbbá jelentse a hamisított rendszerelemeket és azok forrását a Szervezet által meghatározott külső Szervezeteknek, illetve a Szervezet által meghatározott személyeknek vagy szerepköröknek.

Rendszerelem hitelessége – Hamisítás elleni képzés

A Szervezet vezetője - amennyiben ez alkalmazható - törekszik arra, hogy a Szervezet a meghatározott személyeknek vagy szerepköröknek képzést biztosítson a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.

Rendszerelem hitelessége – Konfigurációfelügyelet

A Szervezet vezetője - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy tartsa fenn a konfiguráció felügyeletét a meghatározott szervizelésre vagy javításra váró vagy olyan rendszerelemek esetén, amelyeket szervizeltek vagy javítottak, és arra várnak, hogy újból üzembe állítsák őket.

Rendszerelem selejtezése, megsemmisítése

A Szervezet vezetője kötelezi az EIR működéséért felelős rendszergazdát, hogy meghatározott technikákkal és módszerekkel az adatok visszaállításának minimálisra csökkentésével, selejtezze a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.

SZERZŐI JOGOK

EZ A DOKUMENTUM A BONYHÁDI KÓRHÁZ ÉS RENDELEŐINTÉZET TULAJDONA, MELYET A MAXENTROP KFT. KÉSZÍTETT EL SZÁMÁRA. ÍGY A DOKUMENTUM SZERZŐI JOGAIVAL A MAXENTROP KFT. RENDELKEZIK.