

SELLYEI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKABIZTONSÁGI SZABÁLYZAT

Jóváhagyom!
2025.06.20.

.....
Jegyző



Verziókövetés:

Verzió	Módosítás dátuma	Elvégzett módosítás	Módosítást végezte
kezdeti verzió 1.00	2025.06.20.	teljesen új kiadás	Maxentrop Kft.

Tartalomjegyzék

1.	Az Informatikabiztonsági Szabályzat.....	3
1.1	A dokumentum célja.....	3
1.2	A dokumentum hatálya	4
1.3	A dokumentum minősítése, kötelezettségek.....	5
1.4	A dokumentum kiadása, kezelése, felülvizsgálata	6
1.5	Alapfogalmak.....	7
1.6	Kapcsolódó dokumentumok	9
1.7	Szerepkörök.....	10
1.8	Engedélyezési eljárás	16
1.9	Tevékenységek.....	16
2.	Hivatal rendszereinek besorolási nyilatkozata.....	17
3.	Adminisztratív Védelmi Intézkedések.....	21
3.1	Programmenedzsment.....	21
3.2	Hozzáférés felügyelet.....	27
3.3	Tudatosság és képzés.....	31
3.4	Naplózás és elszámoltathatóság.....	34
3.5	Értékelés, engedélyezés és monitorozás.....	36
3.6	Konfigurációkezelés.....	38
3.7	Készenléti tervezés	42
3.8	Azonosítás és hitelesítés.....	48
3.9	Biztonsági események kezelése.....	52
3.10	Karbantartás	54
3.11	Adathordozók védelme	56
3.12	Fizikai és környezeti védelem	57
3.13	Tervezés.....	66
3.14	Személyi biztonság.....	69
3.15	Kockázatkezelés	72
3.16	Rendszer- és szolgáltatásbeszerzés	74
3.17	Rendszer- és kommunikációvédelem	78
3.18	Rendszer- és információértetlenség.....	81
3.19	Ellátási lánc kockázatkezelése.....	84

1. Az Informatikabiztonsági Szabályzat

Az elektronikus biztonságáról szóló 2024. évi LXIX. törvény Magyarország kiberbiztonságáról 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) SELLYEI KÖZÖS ÖNKORMÁNYZATI HIVATAL (továbbiakban: *Hivatal*) Informatikabiztonsági Szabályzatát az alábbiakban határozza meg:

- a) meghatározza a célokat, a Szabályzat tárgyi, személyi és területi hatályát,
- b) az elektronikus információbiztonsággal kapcsolatos szerepköröket,
- c) a szerepkörökhöz rendelt tevékenységeket,
- d) a tevékenységekhez kapcsolódó felelősségeket,
- e) az információbiztonság rendszerének, belső együttműködését.

Területi hatálya:

SELLYEI KÖZÖS ÖNKORMÁNYZATI HIVATAL

7960 Sellye Dózsa Gy utca 1

7966 Bogdása Kossuth L. utca 24

7967 Drávafok Fő utca 1

7960 Drávaiványi Kossuth utca 31

7967 Drávakeresztúr Petőfi utca 66

7960 Drávasztára Kossuth utca 106

7968 Felsőszentmárton Kossuth utca 8

7958 Kákics Petőfi utca 2

7967 Markóc Fő utca 24

7960 Marócsa Kossuth utca 1

7957 Okorág Rákóczi utca 71

7960 Sósvertike Petőfi utca 42

1.1 A dokumentum célja

Az Informatikabiztonsági Szabályzat (a továbbiakban IBSZ, vagy Szabályzat) azon alapvető biztonsági normákat és működési kereteket határozza meg, melyek érvényesítésével a Hivatal 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 Hivatali feladatokat és felelősségi köröket.

A Szabályzat további célja, hogy iránymutatással szolgáljon a Hivatal 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 Hivatal részére az elektronikus információbiztonsággal kapcsolatos elveket, szabályokat, az elvárt és betartandó magatartásformákat és gyakorlatokat.

A Hivatalban üzemelő számítástechnikai infrastruktúra hátteret teremt a Hivatalban 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 Hivatalban 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 Informatikabiztonsági Szabályzat a fenti célok teljesülése érdekében rögzíti a Hivatal elvárt biztonsági szintjének és az általa használt EIR-ek biztonsági osztályba sorolásának megfelelő adminisztratív, fizikai és logikai követelmények teljesítésével összefüggő folyamatokat, eljárásokat, feladatokat és felelőségeket. A Hivatal Vezetőjének (a továbbiakban: *Jegyző*) célja és feladata, hogy minimalizálja a kliens (felhasználó) oldali kockázatokat.

1.2 A dokumentum hatálya

A Szabályzat **tárgyi hatálya** kiterjed a Hivatal minden informatikai rendszerére, teljes informatikai környezetére, beleértve minden olyan adathordozót és informatikai eszközt,

amin a Hivatal 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 Hivatal 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 min ezek védelmét szolgáló (beleértve e dokumentumot is) gyakorlati ismeretekre és vagy ezek dokumentációira.

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 Hivatal 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 Hivatal informatikai rendszereit, eszközeit használó, vagy azokhoz hozzáférő felhasználóra, Munka Törvénykönyve hatálya alá tartozó munkavállalóra, továbbá a Hivatalban megbízási, vagy egyéb jogviszony vagy vállalkozói szerződés alapján az informatikai rendszerekhez bármilyen okból hozzáférő személyre (a továbbiakban együttesen *felhasználó*). Ha a Hivatal más személyeknek (pl: alvállalkozók) is lehetőséget biztosít bármely informatikai rendszerének használatára, akkor rájuk 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 Hivatali vagy rendszerelem változása esetén el kell végezni, de legalább a jogszabályban meghatározott időközönként.

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

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 Jegyző által feljogosított személyek rendelkezhetnek.

A Jegyző felelőssége a Szabályzat napra készen tartása, így a Jegyző 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 Jegyzőnek feladata és felelőssége az IBSZ kiadása, Hivatalon belüli kihirdetése és rendelkezésre állásának biztosítása (megőrzése).

Az IBSZ személyi hatálya alá tartozók munka- és feladatkörének 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 Hivatalban, 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 Jegyzőnek.

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,

behatólászvizsgálat: 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 informatikabiztonsági 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,

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 bízta 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 hatályaon 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,

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 informatikabiztonsági 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 vezetékek 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 hivatalok ellenálló képességéről szóló törvény végrehajtásáról

- g) 475/2024. (XII. 31.) Korm. rendelet az ország védelme és biztonsága szempontjából jelentős hivatalok ellenálló képességéről
- h) 59/2024. (XII. 23.) BM rendelet a kritikus hivatal 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 Hivatalok 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 Hivatal a részletes Hivatali szerepköröket a *Szervezeti és Működési Szabályzatban*, annak hiányában e dokumentumban és a Hivatali organogrammban rögzítette.

SELLEYI KÖZÖS ÖNKORMÁNYZATI HIVATAL vezetője (Jegyző): az Informatikabiztonsági feladatokkal kapcsolatban kitűzi a célokat, programokat határoz meg a cselekvési terv teljesülése érdekében.

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

A Jegyző 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 Hivatalban 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 Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az Informatikabiztonsági Szabályzatot,
- e) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,
- f) a végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a Hivatal 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 Hivatal 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 ellenőrizheti az informatikai, információbiztonsági folyamatok bármely részét.

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

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

Az elektronikus információs rendszer biztonságáért felelős személyt a Jegyző nevezi ki vagy bízta meg. Az elektronikus információs rendszer biztonságáért felelős személy felel a Hivatalnál előforduló információs rendszer védelméhez kapcsolódó feladat ellátásáért. Ennek során

- ◊ a Jegyzőnek kérésre közreműködik az informatikabiztonsági incidensek kivizsgálásában.
- ◊ a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
- ◊ b) gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről,
- ◊ c) előkészíti és a szervezet vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát,
- ◊ d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását,
- ◊ e) előkészíti és a szervezet vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezet elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,
- ◊ f) megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,
- ◊ g) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet elektronikus információbiztonságot érintő szabályzatait és szerződéseit,
- ◊ h) folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a szervezet elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a szervezet vezetője számára,
- ◊ i) felülvizsgálja, hogy a szervezet elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a szervezet belső szabályozóival,
- ◊ j) az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a szervezet vezetője számára,
- ◊ k) legalább évente megvizsgálja a intézkedési tervet és beszámolót készít a szervezet vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket,
- ◊ l) kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal,
- ◊ m) a szervezet bármely elektronikus információs rendszerét érintő incidensről tájékoztatja e rendeletben meghatározott szervet,
- ◊ n) együttműködik a Kszetv. szerinti kritikus szervezet ellenálló képességéért felelős vezetővel, valamint a Vbő. szerinti ellenálló képességért felelős vezetővel.
- ◊ o) feladatait alapvető szervezeteknél legalább kéthavonta egy napon, fontos szervezeteknél legalább háromhavonta egy napon – dokumentált módon – az érintett szervezetnél való fizikai jelenlét mellett köteles ellátni.

Az elektronikus információs rendszer biztonságáért felelős személy jogosult a Hivatal tevékenységeihez köthető közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében valamennyi adatot, illetve az

elektronikus információs rendszerek biztonságában keletkeztetett 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 Hivatal vezetője felé.

A rendszergazda (informatikai rendszerek felügyeletével, kezelésével megbízott személy vagy szervezet): a Jegyző iránymutatásával a szerződésben leírtaknak és e Szabályzatnak megfelelően végzi feladatait. Szorosan együttműködik az elektronikus információs rendszer biztonságáért felelős személlyel az informatikabiztonsági követelmények kialakításában és végrehajtásában. A védelem helyi operatív végrehajtásáért 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.
- az 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 Hivatal 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 Hivatal elektronikus információs rendszereinek nyilvántartása, beleértve a hardver-, szoftver- és licenccnyilvántartás elkészítését
- részvétel az informatikabiztonsági stratégia felülvizsgálatában, megvalósításában
- új elektronikus információs rendszer bevezetése esetén a felhasználók oktatása
- a Hivatal elektronikus információs rendszereivel kapcsolatos nyilvántartásainak évenkénti felülvizsgálata
- a saját feladatkörébe tartozó rendszerek felügyelete
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és azok karbantartásáért
- gondoskodik a rendszer kritikus részeinek meghatározásáért és újraindíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról
- a védelmi eszközök működésének folyamatos ellenőrzése
- felelős a Hivatali rendszerek hardver eszközeinek karbantartásáért
- gondoskodik a folyamatos vírusvédelem fenntartásáról
- folyamatosan figyelemmel kíséri és vizsgálja a rendszerek működése és biztonsága szempontjából lényeges paraméterek alakulását, kritikus eseményekkor jelzi a Jegyzőnek, 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 Hivatal minden munkavállalója, alvállalkozója, foglalkoztatási formától függetlenül, aki az informatikai rendszerekhez jogosultságot kap és azt használja. A felhasználók kötelezettsége a Szabályzatban szereplő, illetve a Jegyző 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 Hivatali szerepköröket a Hivatal a munkaköri leírásokban, a Hivatal *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 Jegyzőnek;
- 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 a Jegyzőnél,
- 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 rendszergazdának,
- 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 megóvjá. 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 vétkezen – szándékosan vagy gondatlanul – megszegi és személyével kapcsolatosan fegyelmi vétség gyanúja merül fel, a rendszergazda a kötelezettségszegésről és annak körülményeiről haladéktalanul írásban tájékoztatja a Hivatal vezetőjét, aki dönt a fegyelmi eljárás megindításáról.

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

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

Harmadik fél szolgáltatásainak igénybe vétele előtt a Jegyző 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 Jegyző jogosult és köteles a Hivatal 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 Hivatal a tv.-ben meghatározott alaptevékenységét a *Szervezeti és Működési Szabályzatban*, alapító okiratban, vagy más hivatalos dokumentumban rögzítette.

2. HIVATAL RENDSZEREINEK BESOROLÁSI NYILATKOZATA

SELLYEI KÖZÖS ÖNKORMÁNYZATI HIVATAL nyilatkozatban rögzíti, hogy a „7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről” alapján és lefolytatott értékelés eredményeként a Hivatal EIR-jeinek és ezzel együtt a Hivatalnak a biztonsági szintje

„alap” besorolású.

Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel:

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

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

A Hivatalra vonatkozóan meghatározza és dokumentumban rögzíti

- az elektronikus információs rendszerei védelmével kapcsolatos szerepköröket, felelőségeiket, feladataikat és az ehhez szükséges hatásköröket;
- a kockázatmenedzsment stratégiáját, amely leírja, hogy a Hivatal 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 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 Hivatali architektúrában, amennyiben a Hivatal rendelkezik vele;

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

- az Informatikabiztonsági Szabályzatot a Hivatalra érvényes rendelkezések szerint az erre jogosult vezető hagyja jóvá;
- az Informatikabiztonsági Szabályzat tartalmazza az információbiztonság felügyeleti rendszerét, az információbiztonsággal kapcsolatos kötelezettségeket és felelősségeket;
- a Hivatal az Informatikabiztonsági Szabályzat be nem tartását fegyelmi ill. jogi eljárás keretében szankcionálja;
- a Hivatal biztonsági kontrollfolyamatai eljárásrendben szabályozottak; melyek 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 Hivatal 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 Hivatal úgy dokumentálja, hogy abból az elvégzett kontroll tevékenység - ideértve annak egyes jellemzőit, így különösen mélységét, érintett személyi és tárgyi köre - megállapítható legyen.

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 Hivatal 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 Informatikabiztonsági 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 jelszóházi rend 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.

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

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

3. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

3.1 Programmenedzsment

Informatikabiztonsági szabályzat

A Jegyző megfogalmazza, dokumentálja, jóvá hagyja, valamint kihirdeti a Hivatal Informatikabiztonsági Szabályzatát.

Az Informatikabiztonsági Szabályzatot szükség szerint, de legalább két évente egyszer az informatika biztonsági rendszer felülvizsgálata során a Jegyző az IB felelőssel együtt, felülvizsgálja, szükség szerint módosítja. Az informatikabiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor az Informatikabiztonsági Szabályzatot felülvizsgálja, szükség szerinti módosítja. A Jegyző az IBSZ-ben rögzíti a Hivatal 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 Hivatal által működtetett, vagy bevezetni kívánt védelmi intézkedésekről. Meghatározza a célkitűzéseket, a ható- és szerepköröket, a felelőségeket, a vezetői elkötelezettséget, a Hivatalon belüli együttműködés kereteit és a megfelelőségi kritériumokat. Leírja az információbiztonságért felelős és a szervezeti egységek közötti együttműködést. E dokumentum szerint a Jegyző elszámoltatható a Hivatali műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a Hivatali eszközök, személyek, más a szervezet szempontjából számottevőnek tartott kockázatokért. Gondoskodik arról, hogy az információbiztonsági Szabályzat jogszabályok számára ne legyen megismerhető, módosítható.

Az elektronikus információs rendszerek biztonságáért felelős személy

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

Információbiztonságot érintő erőforrások

A Hivatal 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. Gondoskodik arról, hogy a szükséges dokumentáció összhangban legyen a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. A Jegyző biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez tervezett forrásokat.

Intézkedési terv és mérföldkövei

A Jegyző *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 rendszerre vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosságot állapítanak meg, vagy a meghatározott biztonsági szint alacsonyabb, mint az érintett Hivatalra érvényes szint, akkor a Jegyző a vizsgálatot követő 90 napon belül felülvizsgálatot készít (aktualizálja a cselekvési tervet) a hiányosság megszüntetése érdekében.

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

A szervezet vezetője biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó Hivatali elektronikus információs rendszerek intézkedési tervei

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

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

Az elektronikus információs rendszerek nyilvántartása

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

- a rendszerek alapadatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot (amennyiben azok az érintett Hivatal kezelésében vannak);
- a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;
- a rendszert szállító, fejlesztő és karbantartó Szervezetek azonosító és elérhetőségi adatait, valamint ezen Szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait;
- követi Hivatal 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 Jegyző az elektronikus rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban (*Elektronikus Információs Rendszerelem Leltár*) kezeli.

Biztonsági teljesítmény mérése

A Hivatal 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 Hivatal reakcióideje
 - átlagos biztonsági esemény reagálási idő,
 - sérülékenységek felfedése utáni frissítési és hibakezelési eljárási idő,
 - rendelkezésre állás monitoring.
- e) az üzletmenet-folytonosság vonatkozásában
 - az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tesztelés végrehajtási ideje és annak hatékonysága.

Szervezeti architektúra

A Hivatal kifejleszti és fenntartja azt a szervezeti rendszert (architektúrát), amely tekintettel van mindazon kockázatokra, amelyek hatással lehetnek a Hivatali működésre, az eszközökre, az egyénekre és más szervezetekre, annak érdekében, hogy a biztonsági követelmények és védelmi intézkedések integrálása az architektúrába segítsen, annak biztosításában, hogy a biztonsági megfontolások a rendszerfejlesztési életciklus során mindvégig érvényesüljenek, és kifejezetten kapcsolódjanak a szervezet működési céljaihoz és folyamataihoz. A Biztonsági Architektúra követelmény az alábbi intézkedések során valósul meg:

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

A Hivatal működése szempontjából kritikus infrastruktúra biztonsági terve

A Hivatal 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 Hivatal 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 Hivatal működése szempontjából kritikus infrastruktúrák és erőforrások védelmének stratégiáit.

Kockázatmenedzsment stratégia

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

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

Engedélyezési folyamatok meghatározása

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

Beilleszti az engedélyezési folyamatot a Hivatal egészét átfogó kockázatkezelési keretrendszerbe.

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

Hivatali működés és üzleti folyamatok meghatározása

A Hivatal meghatározza a Hivatali célokat és folyamatokat, figyelembe véve az információbiztonságot, valamint a Hivatali működésre, eszközökre, személyekre gyakorolt kockázatokat. Meghatározza a célokból, folyamatokból adódó

információvédelmi igényeket. Évente a pénzügyi tervezéskor, felülvizsgálja és szükség szerint módosítja a célokat és folyamatokat.

Biztonsági személyzet képzése

A Hivatal 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 képzettség 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 lépésre és a nagyobb felelősséggel járó pozíciók betöltésére. E program keretében a Hivatal

- 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 lépésre és a nagyobb felelősséggel járó pozíciók betöltésére,
- a munkaerőprogramokat összehangolja a Hivatal biztonsági tudatosság és képzési programjaival,
- dokumentálja a programban részt vevők előrehaladásáról és fejlődését.

Tesztelés, képzés és felügyelet

A Hivatal bevezet egy folyamatot, amely biztosítja, hogy a Hivatali EIR-ekhez kapcsolódó biztonsági tesztek, képzések és felügyeleti tevékenységek elvégzésére vonatkozó tervek megfelelő fejlesztés és karbantartás mellett folyamatosan végrehajtásra kerüljenek. Felülvizsgálja és összehangolja a terveket a kockázatmenedzsment stratégiával és a kockázatkezelési intézkedésekre vonatkozó, az egész Hivatalra 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 Hivatal kapcsolatokat alakít ki szakmai csoportokkal és közösségekkel annak érdekében, hogy

- elősegítse a Hivatalhoz köthető személyek folyamatos biztonsági oktatását és képzését;
- naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén;
- 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 Hivatalokban dolgozó biztonsági szakemberek csoportjai. Ezen szakmai csoportokkal való kapcsolatot a munkaköri leírásban és vagy megbízásban rögzíti.

Fenyegetettség tudatosító program

A Hivatal a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot vezet be, ami magában foglalja a fenyegetések felderítését és azokról szóló információk megosztását a Hivatalon belül és más Hivatalokkal. 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 kommunikáció)

Kockázatmenedzsment keretrendszer

A Hivatal 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 Hivatal által meghatározott személyekkel. A Hivatalban és az EIR-ben történő változásokkor mindig, de legalább évente elvégzi a kockázatmenedzsment keretrendszer szempontrendszerének felülvizsgálatát és frissítését.

Kockázatkezelésért felelős szerepek

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

Ellátási lánc kockázatmenedzsment stratégiája

A kockázatkezelésen belül kidolgoz egy a Hivatal 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 Hivatali folyamatok szintjén hajtja végre, valamint az ellátási lánc kockázatkezelési terveit, pedig az EIR-ek szintjén. A változások lekövetése általános kockázatkezelési követés szerint történik.

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

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

Folyamatos felügyeleti stratégia

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

- a felügyeleti tevékenységek gyakoriságát és módszereit, valamint a mérőszámokat,
- fenntart 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 Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Fiókkezelés

A Jegyző:

- 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 Jegyző 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 Hivatalban 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 Hivatalunk megfelelő körülményekkel járunk el, figyelembe véve a speciális fióktípusokkal együtt járó kockázatokat.

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 Hivatal 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 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 megjegyző funkcióját.
- Jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni 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 **Jegyző** 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.

Sikertelen bejelentkezési kísérletek

A Hivatal korlátot alkalmaz a felhasználó meghatározott időtartamon belüli 5 egymást követő sikertelen bejelentkezési kísérleteire. Ezt túllépve az EIR 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 Hivatalra vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint és a következőket tartalmazza:

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

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

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 Hivatalban csak biztonságos távoli hozzáférés engedélyezett, amely az érintett Hivatal EIR-éhez kapcsolódik és amely külső hálózatokon, például az interneten keresztül kommunikál. A Hivatal jellemzően titkosított virtuális magánhálózatokat (VPN-eket) használ a távoli kapcsolatok bizalmasságának és integritásának megőrzése érdekében.

Vezeték nélküli hozzáférés

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

Hivatali 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 Jegyző

- 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.

Mobil eszközök hozzáférés ellenőrzése

A Jegyző 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.

Külső elektronikus információs rendszerek használata

A Jegyző 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 Hivatal által ellenőrzött információkat.
- c) külső szolgáltató a Hivatali rendszeren, azonosítatlan és engedéllyel nem rendelkező tevékenységet nem végezhet.

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

Nyilvánosan elérhető tartalom

A Jegyző

- a) kijelöli a Hivatal vezető beosztású munkatársát, aki jogosult a nyilvánosan hozzáférhető elektronikus információs rendszeren az érintett Hivatallal kapcsolatos bármely információ közzétételére. A Hivatalban csak a Jegyző 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 Jegyző nyilvánosan elérhető rendszerként definiálja például a Hivatal publikus weboldalát;
- f) a publikus felületeken való közzétételt és a médiával való kommunikációt a Jegyző szabályozza, a Hivatal külső kommunikációjáért a Jegyző a felelős.
- g) a Hivatali honlap (www.agfalva.hu) tartalommenedzsmentjét egy külsős megbízott, megbízási szerződés keretében végzheti;
- h) a Hivatali ügyintézésrel kapcsolatos dokumentációk, határozatok, rendeletek a Jegyző jóváhagyását követően kerülnek nyilvánosságra;
- i) a publikált információk csak nyilvános adatokat és információkat tartalmazhatnak.

A Jegyző legalább évente áttekinti a honlapot és nem nyilvános adat kikerülése esetén eltávolítja azt.

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

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

3.3 Tudatosság és képzés

A Jegyző biztosítja

- hogy a felhasználók rendelkezzenek a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel;
- a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását, mely képzés magában foglalja a biztonsági követelményeket, a jogi felelősséget, az óvintézkedéseket, valamint az informatikai eszközök helyes használatát, az informatikabiztonsági előírtaakat;

- hogy a felhasználók ismerjék a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is minimálisra csökkentsék a lehetséges biztonsági kockázatokat, és alá kell írniuk az erről szóló nyilatkozatot;
- hogy minden felhasználó tudatában legyen annak, hogy a biztonsági szabályok megsértése szankciókkal jár.

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a képzéssel kapcsolatos eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Szerepkörök, felelősségek, szabályzat és eljárásrendek

A Jegyző 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 Hivatalba újonnan belépő munkavállalókat a lehető leghamarabb alapképzésben részesítik. Rendkívüli oktatást tart a Hivatal rendszereiben történő jelentős változás vagy a Hivatal rendszereiben történő incidens után.

A Jegyző:

- a) felelős a képzési kritériumok meghatározásáért;
- b) biztosítja a képzéshez a szükséges erőforrásokat;
- c) gondoskodik a képzések fontosságának tudatosításáról a teljes Hivatalban.

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 Jegyző felelőssége, hogy a Hivatal 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. A képzést legalább évente meg kell ismételni, illetve minden olyan EIR-ben vagy munkakörben történő változás esetén, mely ezt indokolttá teszi.

A képzés

- felhívja a munkatársak figyelmét az Informatikabiztonsági 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 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 Hivatal informatikai rendszereihez hozzáférők számára, amely jelenlétet az oktatás végén szükség szerint a jelenléti ív aláírásával igazolnak.

Biztonságtudatossági képzés – Belső fenyegetés

A Jegyző 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 Jegyzőnek.

Szerepkör alapú biztonsági képzés

A Hivatal 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 szerepkör alapú 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 adminisztrátorai; 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 Jegyző felelőssége a felhasználók oktatásának biztosítása. Az új rendszerhez hozzáférés csak azoknak a felhasználóknak adható, akik részesültek a képzésben és ezt aláírásukkal igazolták.

A biztonsági képzésre vonatkozó dokumentációk

A Hivatal dokumentálja és egyúttal nyomon követi 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 Hivatal 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 elszámoltathatóság szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a naplózással kapcsolatos eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Naplózható események

A Hivatal 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 Jegyző 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 Hivatali 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 informatikabiztonsági eseményekről helyi naplóállományt generál;
- e) felelősséget vállal, hogy a kialakított naplózási rendszer szükséges mértékben biztosítsa a számon kérhetőséget 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, a Jegyző tájékoztatása mellett. A naplóállományokat meghibásodás vagy biztonsági incidens esetén, eseti jelleggel vizsgálhatja. 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;
- mi volt az eseménynek a kimenetele, valamint
- az eseményhez kapcsolódó személyek, alanyok, objektumok.

Naplózás tárkapacitása

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

Naplózási hiba kezelése

A Hivatal 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 Hivatal által meghatározott időn belül, szükség szerint további meghatározott intézkedéseket hajt végre.

Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

A Hivatal felülvizsgálja, elemzi és jelentést készít a Hivatal 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 Jegyző és szükség szerint az IBF vizsgálja.

Időbélyegek

A Jegyző a Hivatal által üzemeltetett rendszereknél és hálózaton belül a rendszerórát követeli meg a naplóbejegyzések időbélyegeinek előállításához. Időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz (úgynevezett UTC) vagy a Greenwichi középidejűhöz (úgynevezett GMT) rendelhető módon, megfelelően a Hivatal által meghatározott időmérési pontosságnak.

Naplóinformációk védelme

A Jegyző a Hivatal által üzemeltetett rendszereknél fizikai és logikai követelmények támasztásával, megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

Naplóbejegyzések megőrzése

A Jegyző a Hivatal által üzemeltetett rendszereknél a naplóbejegyzéseket meghatározott – a jogszabályi és az érintett Hivatalon belüli információ megőrzési követelményeknek megfelelő – időtartamig a biztonsági események utólagos kivizsgálásának biztosítása érdekében a naplótárhelyek kapacitásával összhangban őrzi meg.

Naplóbejegyzések létrehozása

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

3.5 Értékelés, engedélyezés és monitorozás

Biztonságértékelési szabályok, szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti az értékelés, monitorozás ellenőrzési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

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

Biztonsági értékelések

A Jegyző 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 védelmi intézkedések értékelésének elvégzéséhez. Így pl. a kockázatkezelési koncepciók és megközelítések általános ismerete, valamint a hardver, szoftver és firmware rendszerelemek átfogó ismerete és tapasztalata.

Információcsere

A Jegyző 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 Hivatalon belüli és a Hivatalon 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 intézkedési terv és mérföldkövei

A Jegyző és az IBF olyan intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására. Így a Hivatal 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 Jegyző maga látja el (esetként átruházza) az engedélyezési feladatokat, aki az EIR-ért felel. Maga látja el azt a felelősi feladatot, aki a Hivatali 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 Jegyző kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a Hivatali szintű stratégiával összhangban. A folyamatos felügyelet eredményeként az IBF kockázatkezelésben értékeli a problémás védelmi intézkedéseket a problémát kiváltó okok elemzésével.

Folyamatos felügyelet – Kockázatmonitorozás

A Jegyző 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.

Belső rendszerkapcsolatok

A Jegyző engedélyezi a Hivatal 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 Hivatal a belső rendszerkapcsolatokat nem különálló esetenként

hagyja jóvá, hanem közös jellemzőkkel és/vagy konfigurációval, valamint interfésszel rendelkező kategóriákkal dolgozik, beleértve a meghatározott feldolgozási, továbbítási 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 kísérése és karbantartása. A szolgáltatásokról, a szoftver és hardver konfigurációkról és azok dokumentációjáról központonként tárol információkat, így segíti az incidensfelügyeletet, problémakezelést, változáskezelést és a verziókövetést.

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a konfigurációkezelési eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő;

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

Alapkonfiguráció

A Hivatal által használt desktopok, laptopok és szerverek esetében egy alapkonfigurációs nyilvántartást készítünk el, és azt folyamatosan aktualizáljuk. 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;
- alapértelmezetten alkalmazott policy beállítások;
- alkalmazandó biztonsági beállítások;

Változások esetén azonnal, de legalább évente szükséges a nyilvántartás felülvizsgálata.

Biztonsági hatásvizsgálatok

A Hivatal rendszereiben csak az végezhet biztonsági hatásvizsgálatokat, akik 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 Hivatal ellátási láncában érintett partnereivel és az egyéb érdekelt felekkel.

A változtatásokra vonatkozó hozzáférés korlátozások

A Jegyző, 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).

Konfigurációs beállítások

A Hivatal meghatározza a Hivatali szintű, egységes konfigurációs elvárásokat, melyeket a *Konfigurációkezelési Szabályzatban* dokumentált. A Hivatal a Hivatali 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 Jegyző felelőssége, 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 Jegyző az EIR-kezeléséért felelőst megbízza, hogy szükséges mértékben azonosítsa, dokumentálja, majd fogadja el a meghatározott rendszerelemek konfigurációs beállításaiban a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.

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

Legszűkebb funkcionalitás

A Hivatal 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.

Rendszerelem leltár

Az elektronikus információs rendszerelem leltár a Hivatal 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 licenccnyilvántartására, külön rögzítve;
- a megvásárolt licencekre;
- a Hivatal megrendelésére fejlesztett termékek licenceire.

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 elektronikus formában is megőrizhető, ha biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos olvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

A szoftverhasználat korlátozásai

A Jegyző

- a) kizárólag olyan szoftvereket és kapcsolódó dokumentációt engedélyez, amelyek megfelelnek a rájuk 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 Hivatal 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 Hivatal informatikai eszközeire TILOS illegális és/vagy nem jogtiszt szoftvert telepíteni!;
- e) engedélyével a Hivatal informatikai eszközeire szoftvereket a felhasználó is telepíthet, de tudatában kell lennie annak a informatikabiztonsági 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 két évente) ellenőrizni automatikus, vagy manuális módszerekkel a Hivatali szoftverhasználat jogtisztaságát, illetve szerzői jogvédett tartalmak (pl. zene, film, dokumentumok) jogosulatlan megosztását a Hivatal informatikai rendszerein;
- h) illegális szoftverek használata, illetve a Hivatal által nem engedélyezett szerzői jogvédett tartalmak tárolása esetén a használatban és megosztásban érintett felhasználóval szemben, felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indíthat, 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 vezetni a változtatásokat
- 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

Programok megőrzése, nyilvántartása

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

A programokról szóló nyilvántartásnak az alábbi adatokat kell tartalmaznia:

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

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 naprakész 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 Hivatalban dolgozók felhasználói jogosultságát és annak körét a rendszergazda a *Felhasználó nyilvántartásban* vezeti. A nyilvántartás vezetése és folyamatos aktualizálása a rendszergazda feladata.

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

Felhasználó által telepített szoftver

A Jegyző a dolgozóinak, felhasználóinak sem hardveresen, sem szoftveresen nem korlátozza a telepítési és módosítási jogosultságokat. A Jegyző a Hivatal által használt EIR-ek felhasználói számára az informatikai eszközöket és erőforrásokat a Hivatali 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.

3.7 Készenléti tervezés

A Jegyző megfogalmazza, és az érintett Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a készenléti tervezésre vonatkozó eljárásrendet.

A Hivatal az elektronikus információbiztonsággal kapcsolatos egyéb szabályokat egy külön dokumentumban (*Üzletmenet-folytonosság Szabályzat*) kezeli.

Üzletmenet-folytonossági szabályzat és eljárásrendek

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

- a) biztosítja, hogy a kockázatok esetleges bekövetkezésekor a szolgáltatás kiesés ne legyen nagyobb a tervezettnél (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 Hivatal 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 Jegyző 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, felelőségeket, 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 Hivatal működésének folytonosságával kapcsolatos feladatok tervezése, irányítása, koordinálása, a szükséges erőforrások rendelkezésre állásának biztosítása a Jegyző feladata. A feladat keretében a Jegyző alapvetően biztosítja, hogy informatikai szolgáltatás kiesésével járó rendkívüli esemény esetén

- az informatikai szolgáltatás elfogadható időn belül és elfogadható adatvesztés 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 Hivatal működését érintő rendkívüli esemény esetén a Hivatal 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 Hivatal 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 Hivatal feladatait, illetve az azok

alapján az érintett ügyviteli folyamatokra levezethető rendelkezésre állási követelményeket.

A fenti követelmények érdekében számba veszi a Hivatal működését támogató informatikai szolgáltatásokat, a szolgáltatások rendelkezésre állását veszélyeztető lehetséges rendkívüli eseményeket és meghatározza, hogy milyen preventív, detektív, illetve korrektív intézkedések bevezetésével csökkenthetők 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 Hivatal 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 Jegyző felelőssége meghatározni a Hivatal 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).

A folyamatos működésre felkészítő képzés

A Jegyző az EIR-rel kapcsolatban saját működtetésű elektronikus információs rendszerek folyamatos működésére felkészítő képzést tartat az Informatikabiztonsági felelős révén a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül (az Informatikabiztonsági vezető ajánlása, de legkésőbb az éves oktatás során);
- 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.

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.
- Archiválendő 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 Jegyző feladata biztosítani a Hivatal működése szempontjából kritikus adatok, szoftverek, konfigurációs beállítások megfelelő tartalékolását. A Hivatal 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 Jegyző 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 Hivatal elektronikus formában tárolja, a mentéseknek alkalmasnak kell lennie az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A Hivatalban 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 Jegyzőnek 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 biztonsági mentést végeznek, hogy a sikertelen frissítés esetén vissza lehessen állítani a korábbi állapotot. Ezeket a funkciókat nem tekintjük a Hivatal időszakos mentési politikája részének.

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

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

- napi mentések: hétfőtől - péntekig; változás mentés 00.00-01.00 között
- heti mentések: szombatonként automatizált módon;
- éves mentések: tárgy év utolsó munkanapját követő nap.

A tárgy év utolsó mentésének (az éves mentés) megtörténte után a NAS adattároló eszköz tükör merevlemeze cserélődik, egy új merevlemezre. A mentést tartalmazó HDD a Jegyzői titkárságon páncélszekrényben kerül elhelyezésre.

Az adatok mentése, az adathordozók biztonsága

A **napi adatmentés** a következő módon történik:

- (1) Az adatvédelmi felelős által meghatározott fájlokat naponta, a munka befejezésével AES- 256 erősségű jelszóval védett *.zip* fájlba tömörítve az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba (vagy feltöltheti az erre a célra létrehozott FTP tárhelyre).
- (2) A külső, biztonságos másolatokat tartalmazó merevlemez csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből, és az adatvédelmi felelős által kijelölt helyre kell elzárni (FTP tárhelyre való feltöltés esetén ez úgy módosul, hogy csak a feltöltés idejére szabad az FTP kapcsolatot élővé tenni, adatfeltöltés után a kapcsolatot meg kell szakítani).
- (3) A korábbi adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan a 14 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 13 frissebb adatmentés az állományokról.

A **heti adatmentés** a következő módon történik:

- (1) Az adatvédelmi felelős által meghatározott, de általánosságban elmondható, hogy a merevlemezen lévő összes fájlról hetente egyszer teljes körű biztonsági másolatot kell készíteni. Az adathalmazok méretének megfelelően vagy a napi mentésnél már szokásos AES-256 erősségű jelszóval védett *.zip* fájlba tömörítve, vagy az eredeti állapotban; az adatmentés helyének kijelölt külső merevlemezre kell másolni, az aznapi dátumra utaló megnevezéssel ellátott, új, erre a célra létrehozott könyvtárba, a könyvtár nevében utalva arra, hogy heti és teljes körű, minden adatot érintő biztonsági másolatról van szó.

- (2) A külső, biztonsági másolatokat tartalmazó merevlemezt csak az adatmentés idejére szabad üzembe állítani, az adatmentés befejeztével szabályszerűen el kell távolítani a rendszerből és az adatvédelmi felelős által kijelölt helyre el kell zárni.
- (3) A korábbi, heti, teljeskörű adatmentéseket csak az adatvédelmi felelős írásbeli utasítására szabad törölni, általánosan az 1 hónapnál régebbi biztonsági mentést tartalmazó könyvtárak kerülhetnek törlésre, de csak abban az esetben, ha már létezik 3 frissebb adatmentés az állományokról.

Az éves adatmentés a következő módon történik:

A tárgy év utolsó teljeskörű biztonsági mentésének megtörténte után, az adatmentés helyének kijelölt külső adattároló eszköz tükör merevlemeze cserélődik egy új merevlemezre. A mentést tartalmazó merevlemez páncélszekrényben kerül elhelyezésre.

Adatvesztés, elemi kár, bármilyen, adatokat érintő probléma esetén követendő eljárás

- (1) Az adatkezelő munkatárs az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az adatvédelmi felelőst.
- (2) Az adatkezelő munkatárs a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az adatvédelmi felelős további utasításáig nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.
- (3) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és az adatkezelő munkatárs jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.
- (4) Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) haladéktalanul értesíti a Hivatal rendszergazdáját.
- (5) A rendszergazda kiérkezéséig az adatvédelmi felelős biztosítja az érintett számítástechnikai eszközök elkülönítését (senki nem nyúlhat hozzá, még az adatvédelmi felelős sem).

Adatok visszatöltése, adatmentési pontok visszaállítása

A napi és heti rendszerességgel mentett adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni.

Feladatok és felelősségek

A Jegyző által meghatározott követelményeknek megfelelő mentési megoldás kialakítása és a mentések elkészítésével és ellenőrzésével kapcsolatos feladatok szükséges gyakorisággal történő végrehajtása az adott eszköz üzemeltetési feladataival megbízott feladata.

A felhasználó felelőssége, hogy az általa használt eszközön (munkaállomáson, laptopon) tárolt azon adatokról, állományokról, amelyek sérülése, elvesztése jelentősen hátráltatná a napi munkavégzést, illetve amelyek pótlása utólag nem lehetséges, vagy túl nagy terhet jelentene a Hivatalra nézve valamiféle mentés készüljön (Word, Excel). Az adott eszköz üzemeltetési feladatainak ellátásáért felelős feladata tájékoztatni a felhasználót, hogy mit kell tennie az állományok mentése érdekében (pl. külső adathordozóra írás, hálózati megosztásra történő másolás stb.).

A szervezeten tárolt adatok mentéséért a rendszergazda a felelős.

A Jegyző joga a mentési feladatok végrehajtásának ellenőrzése, számon kérése.

Az elektronikus információs rendszer archiválása

A Hivatal tevékenységéből adódóan, ha saját rendszerein személyes, védendő adatokat kezel és dolgoz fel és ebből következően archiválási folyamatot tart fenn az elektronikus dokumentumok hosszú távú, biztonságos megőrzése, archiválása céljából, akkor a Hivatal az archiválási tevékenységét a rendeletnek megfelelő *Archiválási Szabályzata* szerint hajtja végre.

Egyéb esetben a Hivatal maga határozza meg az archiválandó adatok körét és módját.

Az elektronikus információs rendszer helyreállítása és újraindítása

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

3.8 Azonosítás és hitelesítés

Szabályzat és eljárásrendek

A Jegyző megfogalmazza, és az érintett Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti az azonosításra és hitelesítésre vonatkozó eljárásrendet, mely az *Azonosítási hitelesítési Szabályzat* és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Ebben dokumentálja, kiadja és megismerteti a Hivatal 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 Hivatalon belüli együttműködés kereteit és a megfelelési kritériumokat, továbbá összhangban van a Hivatalra vonatkozó hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

Azonosítás és hitelesítés

Fő szabály szerint a Hivatal 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 illet, akkor a Hivatal többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

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

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

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Azonosító kezelés

A Jegyző megköveteli, hogy az egyéni-, csoport-, szerepkör- és eszközazonosítók a Hivatal által meghatározott személyek vagy szerepkörökhöz jogosultságokhoz legyenek kötve. Az így kiosztott jogokat a felhasználók kötelesek használni, attól nem térhetnek el. Ez az azonosító lehet például MAC cím, IP cím, vagy eszköz-specifikus token. Az azonosítót hozzá kell rendelni 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 rendelhetők.

A hitelesítésre szolgáló eszközök kezelése

A Jegyző 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, 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 Jegyző az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvényen 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, 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 Hivatal 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. A rendelkezésre állás folyamatos biztosítása érdekében a Jegyző gondoskodik ezek 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 tárolni 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!

Hitelesítési információk visszajelzésének elrejtése

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

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

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.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Azonosítás és hitelesítés (Hivatalon kívüli felhasználók)

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti az érintett Hivatalon kívüli felhasználókat és tevékenységüket. A Jegyző az *Engedélyezési és jogosultsági Szabályzatban* leírtak szerint biztosíthat távoli hozzáférést a rendszereihez, melyről külön nyilvántartást kell vezetni. A Hivatal jelenleg egyik rendszeréhez sem biztosít hozzáférést külső felhasználók számára, csak a hálózatának elemeihez.

A Hivatal 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 (Hivatalon kívüli felhasználók) – Meghatározott azonosítási profilok használata

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

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Újrahitelesítés

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

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

3.9 Biztonsági események kezelése

Hitelesítésszolgáltatók tanúsítványának elfogadása

A Jegyző – 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 kiesése (pl.: olyan hibajelenség előfordulásakor, amely helyben – esetleg távoli segítségnyújtás igénybevételével – kezelhető, mint például egy eszköz újraindítása);
- az informatikai erőforrások széles körét vagy egészét érintő (véssz helyzet) esetén a rendeletben előírt működés nem teljesülését okozó esemény, amely a tartalék intézkedések, illetve helyreállító tevékenységek végrehajtásának elrendelését indokolja.

Biztonsági esemény kezelése szabályzat és eljárásrendek

A Jegyző megfogalmazza, és az érintett Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a biztonsági események kezelésével kapcsolatos szabályokat.

A Hivatal az elektronikus információbiztonsággal kapcsolatos egyéb biztonsági események kezelésének szabályait egy külön dokumentumban (*Biztonsági eseménykezelési szabályzat*) kezeli.

Ebben dokumentálja, kiadja és megismerteti a Hivatal által meghatározott személyekkel szerepkörük szerint a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó *Biztonsági eseménykezelési szabályzatot*, amely meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a Hivatalon belüli együttműködés kereteit és a megfelelési kritériumokat, továbbá összhangban van a Hivatalra vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

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

Amennyiben a bekövetkezett esemény hatására a Hivatal 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 a 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 Hivatal 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 Jegyző 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 IBF feladata az indokolt új, illetve meglévő védelmi intézkedések módosítására vonatkozó javaslat elkészítése, s a Jegyző részére történő megküldése.

Képzés a biztonsági események kezelésére

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

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 Hivatal 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.

A biztonsági események nyomon követése

A Hivatal által használt EIR-ekhez hozzáféréssel rendelkező munkatársak és a Hivatal 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 eskalációs 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 jelentése

A Jegyző megköveteli, hogy a használt EIR-ek bármely szerelemének, 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 Hivatal vezetőjét.

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

Segítségnyújtás a biztonsági események kezeléséhez

A Hivatal támogatást biztosít (helpdesk, oktatás stb.) 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 Jegyző - amennyiben releváns - automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségét és a támogatást.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Biztonsági eseménykezelési terv

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

- a terv struktúráját,
- a bejelentésköteles biztonsági eseményeket,
- szükség szerint a metrikákat a belső mérésre,
- az erőforrásokat,
- az információ-megosztás módját,
- a szerepköröket, felelősöket.

3.10 Karbantartás

Karbantartási szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a rendszer karbantartási eljárásrendet, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Szabályozott karbantartás

A Jegyző,

- a) a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentáltatja és felülvizsgáltatja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a Hivatal 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 Hivatali létesítményből;
- d) az elszállítás előtt minden adatot és információt – mentést követően – töröltet a berendezésekről;
- e) ellenőrzeti, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat;
- f) megköveteli, hogy csatolják a meghatározott, karbantartással kapcsolatos információkat a karbantartási a számítástechnikai eszközökön javítást, módosítását végzők, illetve új eszközök telepítését csak a rendszergazdák, vagy az általuk megbízott és ellenőrzött külső vállalkozó végezzenek;
- g) számítógépek esetében, megköveteli, hogy ha a javítás külső helyszínen történik, az esetleges adattartalmat törölni, az el- és visszaszállítást pedig dokumentálni kell;
- h) megköveteli azt, hogy a nem javítható eszközöket a leírtaknak megfelelően selejtezni, esetleges adattartalmukat pedig – szükség esetén véglegesen és helyreállíthatatlanul – törölni kell;
- i) elvárja, hogy a tervezett karbantartások mértéke és gyakorisága felel meg a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer elvégzésre kerül;
- j) elvárja, hogy a karbantartás minél nagyobb mértékben járuljon hozzá a kockázatok (a működési szabályok betartásával) csökkentéséhez, a helyes és rendszeres karbantartottság révén.

Távoli karbantartás

A Jegyző 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 Informatikabiztonsági Szabályzattal, és dokumentálva van az elektronikus információs rendszer *Rendszerezésbiztonsági 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.

Karbantartó személyek

A Jegyző kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére, és nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó szervezetekről vagy személyekről. Ellenőriztetni az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait, szükség szerint kíséretet rendel a karbantartók mellé. Kijelöli a Hivatalhoz tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyeket

arra, hogy felügyeljük a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

3.11 Adathordozók védelme

Adathordozók védelme szabályzat és eljárásrendek

A Jegyző megfogalmazza, és az érintett Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti az adathordozók védelmével kapcsolatos szabályokat.

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

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti az adathordozók védelmével kapcsolatos szabályokat, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A jegyző megköveteli az adathordozónak minősülő eszközök (pl. floppy, CD, USB eszközök, külső merevlemezek, stb.) kezelésének a Hivatalban használatos szabályok betartását. Így,

- 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 adathordozókat a használat után a tárolási helyre kell visszatenni;
- f) munkaidőben a munkaasztalon, csak az aktuális adatfeldolgozáshoz szükséges adathordozók lehetnek;
- g) adathordozót az arra nem jogosult személynek, csak a Jegyző utasítására lehet átadni.

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 Jegyző 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 adattárolókat minden felhasználónak kötelessége rendeltetésszerűen használni. A Hivatal adathordozóin csak munkavégzéshez szükséges adatok tárolhatók.

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

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 kell törölni, így védve az adatok bizalmasságát. A biztonságos törlés eredményességét a rendszergazdának minden esetben ellenőrizni kell. Azokat az adathordozókat, amelyeket nem lehet biztonságosan törölni, tilos újrafelhasználni, azokat meg kell semmisíteni.

Adathordozók használata

A Jegyző 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 Hivatali EIR-ekben, ha azoknak nincs azonosítható, vagy engedélyezett tulajdonosa.

3.12 Fizikai és környezeti védelem

Fizikai környezet védelme szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon belül kihirdeti a fizikai védelemmel kapcsolatos szabályokat, mely jelen Szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

Alapvető normák, üzemeltetési szabályok

A felhasználók kötelesek betartani a Jegyző 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 Hivatal épületeinek minden oldalról zárható határfelülettel kell rendelkeznie. Minden munkatárs köteles ellenőrizni a felügyelete alatt álló Hivatali 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 Jegyző felé.

A Hivatal 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 Hivatal ügyintézésre használt helyiségeiben ügyfelek, továbbá a Hivatal egyéb, ügyfelek elől elzárt területeire - köztük a Hivatal által használt információs rendszerek elemeinek helyt adó helyiségeiben - a látogatók és munkavégzés céljából a Hivatallal 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 Jegyző által ezzel megbízott munkavállaló feladata.

Amennyiben a Hivatal 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 Jegyző 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 Hivatal tűzvédelmi Szabályzata” tartalmazza.

Vagyonvédelem, fizikai biztonság

- a szerverszobát, irodákat biztonsági zárral kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;
- a szerverszoba kulcsát a rendszergazda 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 Jegyzőnek 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 rendszergazda, valamint az informatikai rendszer üzemeltetését végző gazdálkodó szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a Jegyző engedélyezheti.
- Hivatali időn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát a rendszergazda tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben. A szerverszoba áramtalanításáért a rendszergazda felelős.
- Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért a rendszergazda 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 rendszergazda felügyelete mellett, legalább havonta egyszer, a kijelölt személyek végezhetik.
- A berendezések belsejébe nyúlni TILOS! Bármilyen, nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda 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 rendszergazda 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 használatot, a szakszerűséget, a vonatkozó érintésvédelmi szabályokat 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 az adatvédelmi felelős 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 mentést 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 külön, az épületen kívül, egy tűzbiztos helyen kell tárolni.

Felhasználókra vonatkozó szabályok

Felhasználó lehet a Hivatal képviselője, a Hivatal 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 Jegyző engedélyével. Egyéb személy felhasználói jogot csak Jegyző engedélyével szerezhet.

Általános felhasználói szabályok

- A Hivatal 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 felhasználásból történő kizárást vonhatja maga után.

A Hivatal épületén kívül

Az alábbi szabályok érvényesek minden olyan helyiségre, ami nem a Hivatal 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 Hivatali tulajdonú informatikai eszközt tárolni, használni:

- Utcán, tömegközlekedési eszközön és egyéb nyilvános helyen a Hivatal 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 kialakításra kerül egy titkosított partíció az érzékeny adatok tárolására).

Tiszta asztal tiszta képernyő 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 maradjon;
- kötelesek minden esetben a harmadik felek felügyeletéről gondoskodni, annak érdekében, 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 Jegyző személyre, eszközre, munkafolyamatra vonatkozó felmentést adhat, ha ez szakmailag indokolt.
- a Hivatal épületén belül, Hivatali 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 elől.
- kizárólag az aktuális ügyintézéshez szükséges alkalmazások, programablakok lehetnek megnyitva a képernyőn (amennyiben az ügyfél rálát a képernyőre).

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 szervizelést 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 Szabályzat*nak és a Hivatali Iratkezelési Szabályzatnak megfelelően kell lefolytatni. Az adathordozókat a *Leltározási Szabályzat*nak 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 adatok bevitelénél elv, hogy azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti
- az adatrögzítési dokumentumok:
 - adatrögzítési utasítások
 - ellenőrzési utasítások
 - programok kezelési utasításai
 - megőrzési és archiválási utasítás
 - 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 háttértáiról 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 elemeket és vezetékeket, csatlakozókat és egyéb átviteli elemeket mindennemű sérüléstől óvni kell. Ezek illetéktelen megbontása tilos.

A Hivatal azon helyiségeibe, ahol információs rendszerek (pl. szerverek, adatmentések, telefonközpontok, stb.) vagy rendszerelemek (pl. számítógépek) található, 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 Hivatal 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 Hivatal a végpont fizikai megszüntetéséről, illetve az eszköz zárt területre történő áthelyezéséről köteles gondoskodni.

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

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

Nyitvatartási időn kívül a Hivatal épületeiben ügyfél, látogató vagy a Hivatal számára munkát végző, szerződött partner kizárólag a Jegyző 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 Jegyzőt minden esetben előzetesen tájékoztatni kell.

Minden munkatárs kötelessége, hogy a Hivatalban 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 Jegyző felé, ha a védelmi rendszerek működésében rendellenességet vagy hibát észlel.

Őrzés, védelem szempontjai

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

a *Cselekvési terv*nek. A Hivatal a jegyzőkönyvet az EIR *Szolgáltatási szerződés*ben megjelölt fél kérésére, illetve a Hatóság felszólítására betekintésre adja át.

A fizikai belépési engedélyek

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

A Jegyző

- 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 listában szereplők esetleges visszavonásáról

A fizikai belépés ellenőrzése

A Jegyző

- a) megköveteli, hogy kizárólag a Hivatal által meghatározott be-, és kilépési pontokon legyen biztosítva a belépésre jogosultak számára a fizikai belépés;
- b) megköveteli, hogy ellenőrzés alatt legyenek tartva a létesítményen belüli, belépésre jogosultak által elérhető helyiségek;
- c) gondoskodik a létesítmény információs eszközeinek helyt adó létesítményeibe, eseti jelleggel belépők kíséretéről és figyelemmel követi a tevékenységüket;
- d) megóvjá 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 Hivatal 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 Jegyző felelőssége biztosítani, hogy a Hivatal helyiségeinek kialakítása, illetve az informatikai eszközök elhelyezése során a helyi adottságokat figyelembe véve elfogadható szintre csökkentse az informatikai eszközök jogosulatlan fizikai hozzáféréseiből eredő kockázatokat, a lehetőségekhez képest legoptimálisabb módon biztosítottak legyenek az egyes informatikai rendszerek megbízható működéséhez szükséges környezeti és infrastrukturális körülmények.

A fizikai hozzáférések felügyelete

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

Látogatói hozzáférési naplók

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

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 szervezeti egységét.

Vészvilágítás

A Hivatal 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 Jegyző 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.

Környezeti védelmi intézkedések

A Jegyző, 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 Jegyző 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.

Be- és kiszállítás

A Jegyző mindig engedélyezi, vagy tiltja, továbbá figyelteti és ellenőrizteti a létesítménybe bevitt, onnan kivitt az EIR-rel kapcsolatban saját működtetésű elektronikus információs rendszerelemeket, és nyilvántartást vezet ezekről.

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

3.13 Tervezés

Biztonságtervezési szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint az érintett Hivatalon 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 rendszerelemre terjed ki, és tartalmazza a rendszer biztonsági követelményeinek áttekintését, valamint a követelmények teljesítéséhez kiválasztott intézkedéseket. A Jegyző a saját működtetésű elektronikus információs rendszereihez jelen dokumentumban rendszerbiztonsági tervet készít, amely

- a) összhangban áll a *Biztonságtervezési Eljárásrenddel*, valamint igazodik a Hivatal 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;

- i) frissíti a rendszerbiztonsági tervet az elektronikus információk 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.

Viselkedési szabályok

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon 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 Hivatal 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 Hivatalhoz köthető személy ezeket használja hivatalos feladatának ellátására vagy hivatalos ügyek intézésére, a közösségi médiával és a közösségi hálózatokkal kapcsolatos hálózati üzenetváltásban Hivatali információk vesznek részt, mert az adott személy(ek) a közösségi médiához és a webhelyekhez a Hivatali EIR-en keresztül fér(nek) hozzá.

Viselkedési szabályok az interneten

- a) tilos a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele
- b) tilosak az *Engedélyezési és jogosultsági Szabályzatban* meghatározott, interneten megvalósuló tevékenységeket (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, „sötét web” stb.) végezni
- c) a Hivatal a gépeken nem korlátozza a közösségi oldalak használatát, tiltja magánpostafiók elérését, és más, a Hivataltól idegen tevékenységet
- d) tilos a Hivatal informatikai eszközein tárolni, feldolgozni vagy továbbítani olyan anyagokat, melyek közízlést, vagy törvényt sértenek, mint például:
 - betiltott filmeket, publikációkat;
 - számítógépes játékok;
 - pornográfiát, pedofíliát, erőszakot hirdető cikkeket, publikációkat;
 - megbotránkoztató, a jó ízlés határait sértő anyagokat;
 - gyűlöletkeltésre alkalmas, vagy vallási és kisebbségi érzelmeket sértő anyagokat.

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

A Jegyző a 2011.évi CXII tv. (info tv) alapján szabályozza, illetve korlátozza az internet- és email használatot. Az internet és az IT rendszer kizárólag a Hivatali 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, Hivatali 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 betekinthez. Ugyanis, amennyiben a tájékoztatás ellenére a munkavállaló magáncélú 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 Hivatal érdekeit. Minden felhasználónak lehetősége van felhasználói *nev@hivatal.hu* című postafiókot igényelni, és ezt kizárólagosan Hivatali célra használni. A Hivatal e szabályokra figyelemmel monitorozhatja a hálózathoz küldött, illetve fogadott levelek tartalmát az adatvédelmi szabályok és ajánlások figyelembevételével.

- a) A Hivatal hálózatán keresztül küldött vagy fogadott leveleken központilag vírus- és kémprogram ellenőrzés történik, ami különböző védelmi és szűrő funkciókkal egészül ki.
- b) A Hivatal 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 Hivatali levelező rendszert e-mail személlyel (spam) terhelhetik meg.
- Tilos a Hivatali e-mail cím magánjellegű felhasználása.
- Tilos a Hivatali e-mail címet bármely weboldalon regisztrációhoz felhasználni.
- Tilos ismeretlen vagy gyanúsak 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 magáncélú használatát megtiltja, ezt követően a dolgozó teljes levelezése ellenőrizhetővé

válí. A Hivatal 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.

Biztonsági követelmények kiválasztása

Az érintett Hivatal 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 közzések.

Biztonsági követelmények testre szabása

A Hivatal testre szabja az így kiválasztott biztonsági követelményeket.

3.14 Személyi biztonság

Személyi biztonsági szabályzat és eljárásrendek

A Jegyző - amennyiben a Hivatali struktúra indokolja - megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-hez hozzáférési jogosultsággal rendelkező személyekkel, felhasználókkal szembeni személyi biztonsággal kapcsolatos elvárásokat.

Az EIR rendszereket használó Hivatal Jegyzőjének a felelőssége, hogy meghatározza az egyes, EIR szakrendszer munkakörökhöz tartozó felelősségeket és feladatokat.

Alkalmasság vizsgálatával kapcsolatos elvárások:

- A Hivatal 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, koncentrálóképeség stb.).
- Meggyőződik arról, hogy a foglalkoztatni kívánt személy rendelkezik a munka elvégzéséhez szükséges végzettséggel, tapasztalatokkal.
- A Hivatal vezetőjének felelőssége, hogy személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.
- A humánpolitikai szakterület vezetőjének a felelőssége, hogy a foglalkoztatás alkalmával a Hivatal munkaköri leírásban, a kockázatokkal arányosan rögzítse 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 Jegyző

- minden az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszerrel kapcsolatos Hivatali munkakört, vagy érintett Hivatalhoz 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.

Személyek háttérellenőrzése

A Jegyző:

- 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.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Személyek munkaviszonyának megszűnése

A Jegyző 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 Hivatal 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 Hivatali 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.

Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezés esetén a Jegyző 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 Jegyzőnek 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 Jegyző

- az EIR-rel kapcsolatban saját működtetésű elektronikus információs rendszereinél a külső szervezettel kötött megállapodásban, szerződésben megköveteli, hogy a külső szervezet határozza meg a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelőségekre vonatkozó elvárásokat is;
- szerződéses kötelezettségként megköveteli, hogy a szerződő fél feleljen meg a Jegyző 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 Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön írásos (pl. e-mail) értesítést a Jegyzőnek;
- folyamatosan ellenőrzi a szerződő féltől a személybiztonsági követelményeknek való megfelelést.

Fegyelmi intézkedések

Az informatikai rendszerek biztonságának gondatlan veszélyeztetése, az informatikabiztonsági szabályok megsértése, illetve a felhasználó súlyos mulasztása

esetén a Jegyzőnek felelőssége a szükséges fegyelmi eljárás lefolytatása. A Jegyző 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 Jegyző. A vizsgálatba a Jegyző 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 okozott vagy okozható kár becsült mértékét,
- a felelősségre vonás javasolt módját.

Amennyiben az információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, a Jegyzőnek 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 Jegyző. 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 Jegyző (vagy erre feljogosított személy) fegyelmi eljárást, polgári jogi pert is indíthat. Amennyiben az elkövetett cselekmény a Büntető Törvénykönyv szerint bűncselekménynek minősül, a Jegyző köteles a szabályszegővel szemben feljelentést tenni, és a rendelkezésre álló bizonyítékokat az eljáró hatóságok részére átadni.

Munkaköri leírások

A Hivatal belefoglalja a biztonsági szerepköröket és felelősségeket a Hivatali munkaköri leírásokba.

3.15 Kockázatkezelés

Kockázatkezelési szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-rel kapcsolatos kockázatkezelési elvárásokat.

A Hivatal a kockázatkezeléssel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Kockázatkezelési Szabályzat*) kezeli.

Biztonsági osztályba sorolás

A Jegyző 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 Jegyző az IBF-fel közösen rendszerszintű kockázatelemzést végez, melyben figyelembe veszi a fenyegetéseket, a sérülékenységeket, a káresemények bekövetkezésének valószínűségét, valamint a Hivatal működésére és eszközeire, az egyénekre, és a nemzetre gyakorolt hatásokat. Dokumentálják a kockázatelemzés eredményeit. 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 Jegyző az IBF-fel közösen a kockázatkezelés keretében felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.

Sérülékenységek ellenőrzése

A Hivatal a kockázatértékelésekor ellenőrzi az EIR sérülékenységeit, majd kijavítja a valós sérülékenységeket a meghatározott válaszdíőn belül, a kockázatkezelési eljárásoknak megfelelően. Ilyen tevékenységnek tekintendő az NBSZ NKI, a jelentős gyártók, valamint egyéb iparági szereplők által publikált sérülékenységek nyomkövetése, és a kiadott biztonsági frissítések, valamint új szoftver- és firmware verziók telepítése.

Sérülékenységhmenedzsment – Sérülékenységi információk fogadása

A Hivatal törekszik arra, hogy létrehozzon egy, vagy több csatornát, amelyen keresztül fogadhatja a Hivatali EIR-ekben és rendszerelemekben található sérülékenységekről szőő jelentéseket. Ez a csatorna lehet az NBSZ NKI által kiadott riasztások, figyelmeztetések.

Kockázatokra adott válasz

A Hivatal a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira. A kockázat megfelelő indoklással elfogadható, csökkenthető, megszüntethető vagy átadható, illetve megszüntethető.

Rendszerelemek kritikusságának elemzése

A Jegyző az IBF-el és rendszergazdával együtt azonosítja a Hivatal 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 Jegyző az informatikai eszközök és szoftverek beszerzésénél mindig a beszerzésekre vonatkozó Hivatali 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 Jegyzővel 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.

Hardver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Hivatal 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 Hivatal 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 Hivatal számítógépes rendszerében csak legális, jogtiszt szoftverek üzemeltethetők. 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 Hivatal költségvetése szabja meg. Az egyes szervezeti egységek igényeiket a Jegyző felé a költségvetés összeállítása előtt jelzik. A rendszergazda feladata a szükségszerű cserékről, frissítésekről a Jegyzővel 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 Jegyző 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 Hivatal rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtiszt szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtiszt szoftverek tarthatók. 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 rendszergazda feladata. Ezekből a kellékekből mindig akkora készlettel rendelkezik, amely biztosítja a folyamatos üzletmenetet, ügymenetet.

Beszerzési szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-rel kapcsolatos kockázatkezelési elvárásokat.

Erőforrások rendelkezésre állása

Az EIR-rel kapcsolatban saját hatókörben működtetett elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a Hivatal meghatározza, és dokumentálja, valamint biztosítja az elektronikus

információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat a beruházások tervezése részeként. Elkülönítetten kezeli az EIR-rel kapcsolatban saját működtetésű az elektronikus információs rendszerek biztonságát leíró dokumentumokat a beruházás tervezési dokumentációjában.

A rendszer fejlesztési életciklusa

A Jegyző a rendszergazda segítségével az elektronikus információs rendszereinek teljes életútján, azok minden életciklusában figyelemmel kíséri informatikabiztonsági helyzetüket.

A Jegyző a fejlesztési életciklus egészére meghatározza és dokumentáltatja az információbiztonsági szerepköröket és felelőségeket.

A Jegyző a saját működtetésű elektronikus információs rendszerhez meghatározza és a Hivatalra 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 Jegyző az EIR-rel 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 Jegyző védi az EIR-rel kapcsolatban saját működtetésű elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen.
- A Jegyző ugyancsak szerződéses követelményként határozza meg az EIR-rel 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 Jegyző - amennyiben ez alkalmazható - megköveteli a beszerzett EIR, rendszerelem vagy rendszerszolgáltatás fejlesztőtől, hogy adjon részletes leírást az alkalmazandó védelmi intézkedések funkcionális tulajdonságairól.

Az elektronikus információs rendszerre vonatkozó dokumentáció

A Hivatal 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 az EIR, rendszerelem vagy rendszerszolgáltatás **felhasználói** dokumentációját, amely tartalmazza:

- a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat, ezek hatékony használatának módját;
- a felhasználói interakció biztonságos módját;
- a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.

Biztonságtervezési elvek

A Jegyző - 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 Hivatal 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 Jegyző

- a) szerződéses kötelezettséggként követeli meg, hogy a szolgáltatási szerződés alapján igénybe vett elektronikus információs rendszerek szolgáltatásai megfeleljenek az érintett Hivatal elektronikus információbiztonsági követelményeinek;
- b) a vonatkozó rendelet szempontjai szerint a szerződésben meghatározza az érintett Hivatal felhasználóinak feladatait és kötelezettségeit a külső elektronikus információs rendszerek szolgáltatásával kapcsolatban, így
 - a külső szervezet határozza meg az érintett Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat is;
 - a szerződő fél feleljen meg az érintett Hivatal által meghatározott személybiztonsági követelményeknek;

- dokumentálja a személybiztonsági követelményeket;
 - ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az érintett Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az érintett Hivatalnak;
 - ha az elektronikus információbiztonsági szabályokat nem az érintett Hivatal 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.

Támogatással nem rendelkező rendszerelemek

A Jegyző 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 Hivatal által meghatározott külső szolgáltatók bevonásával valósít meg.

3.17 Rendszer- és kommunikációvédelem

Rendszer- és kommunikációvédelmi szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-rel kapcsolatos, rendszer és kommunikációvédelmi elvárásokat.

A Hivatal a rendszer és kommunikációvédelemmel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Rendszer- és kommunikációvédelmi Szabályzat*) kezeli.

A rendszer- és kommunikációvédelem megvalósítása során a Jegyző az IBSZ követelményei szerint jár el, valamint alkalmazza a *Biztonságtervezési eljárásrendben* foglaltakat.

A fentiekén túlmenően – de azokkal összhangban – a Hivatal az alábbi követelményeket fogalmazza meg a rendszer- és kommunikációvédelem érdekében:

A hálózat használatának szabályai

A Hivatal hálózata nem használható az alábbi tevékenységekre:

- a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű 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 azonosítójával kerül végrehajtásra.

A felhasználók jogai

- Minden Hivatali dolgozónak joga van saját felhasználói fiókhhoz, 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 Hivatal 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 Hivatal dolgozója, illetve az adott rendszer használatához már nincs joga. A törlést a Jegyző 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 Hivatal rendszeréhez tartoznak, de valamely feladat kapcsán a Hivatal vagy a Hivatal dolgozója hozzáférést igényelt, kapott ahhoz (pl pályázati rendszerhez történő hozzáférés, Cégkapuhoz történő hozzáférés). A nyilvántartásba vételt a Jegyző írásban kezdeményezi.

A határok védelme

A Jegyző 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 Hivatal belső hálózatától;
- c) csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészekon keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

Kriptográfiai kulcs előállítása és kezelése

A Jegyző - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Hivatal állítson elő és kezeljen kriptográfiai kulcsokat a Hivatal által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Kriptográfiai védelem

A Jegyző - amennyiben ez alkalmazható - meghatározza a kriptográfia Hivatalon belüli felhasználási területeit és megvalósítja az egyes kriptográfiai felhasználási területekhez szükséges kriptográfiai megoldásokat.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Együttműködésen alapuló számítástechnikai eszközök

A Jegyző - 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 Hivatal engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a személyeknek, akik fizikailag jelen vannak az eszköznél.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

A Jegyző - 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.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

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

A Jegyző - 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.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

A Jegyző - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Hivatal számára név- és címfeloldási szolgáltatást együttesen biztosító EIR-ek hibátűrő képességgel rendelkezzenek, és alkalmazzák a belső és a külső szerepkörök szétválasztását.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Folyamatok elkülönítése

A Jegyző - amennyiben ez alkalmazható - kötelezi az EIR működéséért felelős rendszergazdát, hogy a Hivatal elektronikus információs rendszereit egymástól elkülönítetten (végrehajtási tartományban tartja) működtesse 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 Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-rel kapcsolatos, rendszer és információsértetlenségi elvárásokat.

A Hivatal a rendszer- és információsértetlenséggel kapcsolatos egyéb szabályokat egy külön dokumentumban (*Rendszer- és információsértetlenségi Szabályzat*) kezeli.

Hibajavítás

A Jegyző 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 Hivatal feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
- c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepítse, vagy telepíttesse;
- d) építse be a hibajavítást a konfigurációkezelési folyamatba.

Hibajavítás – Automatizált hibaelhárítás állapota

A Jegyző 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 Jegyző, 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 Hivatal által meghatározott további személy(ek)e)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 Hivatal minden munkaállomásán és szerverén jogtisztta 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 a Hivatal informatikabiztonsági 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 Jegyzőnek, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a Hivatali egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

Az EIR monitorozása

A Jegyző 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.

Biztonsági riasztások és tájékoztatások

A Jegyző az EIR-vel kapcsolatban saját működtetésű elektronikus információs rendszereinél

- folyamatosan figyeli, illetve az informatikabiztonsági felelősön keresztül figyelteti a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
- folyamatosan figyelemmel kíséri, illetve az informatikabiztonsági 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 informatikabiztonsági felelősön keresztül tartat az érintett, külön jogszabályban meghatározott szervekkel;
- megfelelő ellenintézkedéseket és válaszlépéseket tesz, vagy intézkedik annak tételére a megbízott személyekkel, szervezetekkel.

Információ kezelése és megőrzése

A Jegyző 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.

3.19 Ellátási lánc kockázatkezelése

Ellátási láncok kockázata szabályzat és eljárásrendek

A Jegyző megfogalmazza és a Hivatalra érvényes követelmények szerint dokumentálja, valamint a Hivatalon belül kihirdeti az EIR-rel kapcsolatos ellátási lánc kockázatokat, elvárásokat.

Ellátási láncra vonatkozó kockázatmenedzsment szabályzat

A Jegyző 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 láncsal 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

Jegyző 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 Hivatal 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 Jegyző megköveteli, hogy az EIR-rel összefüggő szerződésekben szereplő információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződésai is tartalmazzák.

Beszerzési stratégiák, eszközök és módszerek

Általános szabályok

- a) A Jegyző az informatikai eszközök és szoftverek beszerzésénél mindig a beszerzésekre vonatkozó Hivatali és a törvényi szabályok szerint jár el. A beszerzett számítástechnikai eszközöket és szoftvereket nyilvántartásba veszi.
- b) A rendszergazda, az igénylő osztályok vezetőivel egyeztetve értékeli az igényeket, majd a Jegyzővel 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.

Hardver beszerzés

A rendszergazda a beszerzés és üzembe helyezés előtt a Hivatal 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 Hivatal 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 Hivatal számítógépes rendszerében csak legális, jogtiszt szoftverek üzemeltethetők. 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 Hivatal költségvetése szabja meg. Az egyesszervezeti egységek igényeiket a Jegyző felé a költségvetés összeállítása előtt jelzik. A rendszergazda feladata a szükséges cserékről, frissítésekről a Hivatal 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 Jegyző hatásköre.

Szoftver vásárlás

Szoftver vásárlása csak közvetlenül a szoftver gyártótól, 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 felhasználókhöz való installálásra is.

Jogvédelem

A Hivatal rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtisztá szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtisztá 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.

Értesítési megállapodások

A Jegyző szükség szerint megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel, cégekkel.

Rendszerek vagy rendszerelemek vizsgálata

A Jegyző - 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 Jegyző - 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 Hivatal által meghatározott külső szervezeteknek, illetve a Hivatal által meghatározott személyeknek vagy szerepköröknek.

Rendszerelem hitelessége – Hamisítás elleni képzés

A Jegyző - amennyiben ez alkalmazható - törekszik arra, hogy a Hivatal a meghatározott személyeknek vagy szerepköröknek képzést biztosítson a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésére.

(Az ebben a pontban foglaltak nem relevánsak az Intézményre nézve, azokat a saját belátása szerint nem vezeti be.)

Rendszerelem hitelessége – Konfigurációfelügyelet

A Jegyző - 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 Jegyző kötelezi az EIR működéséért felelős rendszergazdát, hogy meghatározott technikákkal és módszerekkel az adatok visszaállításának minimálisra csökkentésével, selejtezze a meghatározott adatokat, dokumentációkat, eszközöket és rendszerelemeket.

Dátum: 2025.06.20.

SZERZŐI JOGOK

EZ A DOKUMENTUM A HIVATAL TULAJDONA, MELYET A MAXENTROP KFT. KÉSZÍTETT EL SZÁMÁRA. ANNAK BÁRMILYEN RÉSZLETEIBEN VAGY EGÉSZÉBEN HARMADIK FELNEK VALÓ KIADÁSA A KÉSZÍTŐ ÍRÁSOS ENGEDÉLYE NÉLKÜL TILOS.