KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Verzió	Dátum	Módosította/létrehozta	Módosítás
1.0	2014.06.02.	Arnold Andrea	első verzió
2.0	2018.06.01.	Arnold Andrea	ASP követelmények rögzítése

TARTALOMJEGYZÉK

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Szabályzat célja
2. Szabályzat hatálya
2.1. Szervezeti-személyi hatály
2.2. Tárgyi hatály
3. IBSZ általános követelményei
4. IBSZ felülvizsgálata

II. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

5. A hivatal információs rendszereinek Biztonsági osztályba sorolása
6. A hivatal Biztonsági szintbe sorolása
7. Kockázatelemzés és kezelés
8. Rendszer és szolgáltatás beszerzés- beszerzési eljárásrend
8.1. Erőforrás igény felmérés
8.2. Beszerzések
8.3. Az elektronikus információs rendszer védelmi szempontjainak érvényesítése a beszerzés során
9. Elektronikus információs rendszerek ügymenet folytonosságának tervezése
9.1. Ügymenet folytonosságra vonatkozó eljárásrend
9.2. Kritikus rendszerelemek meghatározása
9.3. Folyamatos működésre felkészítő képzés
9.4. Az elektronikus információs rendszer mentései
9.5. Infokommunikációs szolgáltatások
9.6. Az elektronikus információs rendszer helyreállítása és újraindítása.
10. Emberi tényezőket figyelembe vevő – személy – biztonság
10.1. Információbiztonsági tevékenységek
10.2. Információbiztonsági felelősségi rend meghatározása
10.3. A munkaköri felelősség és az alkalmazás feltételei
10.4. Munkakörök, feladatok biztonsági szempontú besorolása
10.5. A személyek ellenőrzése
10.6. Biztonsági események kezelése
10.7. Eljárás jogviszony megszűnésekor
10.8. Áthelyezések, átirányítások és kirendelések kezelése
10.9. Fegyelmi intézkedések
10.10. Belső egyeztetés
10.11. Viselkedési szabályok az interneten
10.12. Harmadik felekkel kapcsolatos előírások
11. Biztonság tudatosság képzés
11.1. Alapképzés
11.2. Belső fenyegetés
11.3. Szerepkör vagy feladat alapú biztonsági képzés
12. Az elektronikus információs rendszerek nyilvántartása

III. FIZIKAI VÉDELMI INTÉZKEDÉSEK

13. Fizikai védelmi eljárásrend
13.1. Az irodák, a helyiségek és az eszközök védelme
13.2. Az infokommunikációs eszközök elhelyezése és védelme
13.3. Tápáramellátás
13.4. Kábelezés biztonsága
13.5. Felhasználói szabályok
13.6. Felügyelet alól kikerülő eszközök

14. Fizikai belépési engedélyek
15. Fizikai belépés ellenőrzése
15.1. Fizikai belépések
15.2. Kulcsok megóvása
15.3. Hozzáférés az adatátviteli berendezésekhez és csatornákhoz
15.4. Tűz- és behatolás védelem

IV. LOGIKAI VÉDELMI INTÉZKEDÉSEK

16. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK
16.1. Elektronikus információs rendszer kapcsolódásai
17. TERVEZÉS- BIZTONSÁGTERVEZÉSI ELJÁRÁSREND
17.1. Rendszerbiztonsági terv
18. KONFIGURÁCIÓKEZELÉSI ELJÁRÁSREND
18.1. Alapkonfiguráció
18.2. Elektronikus információs rendszerelem leltár
18.3. Legszűkebb funkcionalitás
18.4. Duplikálás elleni védelem
18.5. A szoftverhasználat korlátozásai
18.6. A felhasználó által telepített szoftverek
19. KARBANTARTÁSI ELJÁRÁSREND
20. ADATHORDOZÓK VÉDELMÉRE VONATKOZÓ ELJÁRÁSREND
20.1. Hozzáférés az adathordozókhoz, adathordozók használata
20.2. Adathordozók tárolása
20.3. Adathordozók szállítása
20.4. Kriptográfiai védelem
20.5. Adathordozók törlése
20.6. Ismeretlen tulajdonos
20.7. Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása
21. AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁSREND
21.1. Azonosítás, hitelesítés és azonosítókezelés
21.2. Birtoklás alapú hitelesítés
21.3. A felhasználó felelősségi köre a jelszó használat során
22. HOZZÁFÉRÉS ELLENŐRZÉSI ELJÁRÁSREND
22.1. Felhasználói fiókok kezelése
22.2. Kiemelt jogosultságok kezelése
22.3. Hozzáférési jogok igénylésének eljárásrendje
22.4. Jogosult hozzáférés a biztonsági funkciókhoz
22.5. Munkaszakasz zárolása, képernyőtakarás
22.6. Vezeték nélküli hozzáférés
22.7. Mobil eszközök hozzáférése
22.8. Külső elektronikus információs rendszerek használata
22.9. Információ megosztás, nyilvánosan elérhető tartalom
23. RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉG
23.1. Rendszer és információ sértetlenségére vonatkozó eljárásrend, hibajavítás
23.2. Kártékony kódok elleni védelem
23.3. Vírusriadó
23.4. Az elektronikus információs rendszer felügyelete
23.5. Biztonsági riasztások és tájékoztatások
23.6. Bemeneti információ ellenőrzés
23.7. Kimeneti információ kezelése és megőrzése
24. NAPLÓZÁSI ELJÁRÁSREND
25. RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELMI ELJÁRÁSREND

V. ZÁRÓ RENDELKEZÉSEK

Mellékletek:

1. sz. melléklet: Értelmező rendelkezések

2. sz. melléklet: Informatikai biztonsági házirend

3. sz. melléklet: Felhasználói nyilatkozat

4. sz. melléklet: Oktatási nyilatkozat

5. sz. melléklet: Hozzáférési jogok igénylése, módosítása, megszüntetése

6. sz. melléklet: Biztonsági események jelentése

7. sz. melléklet: Kockázatelemzési és kezelési módszertan

8. sz. melléklet: A Hivatal elektronikus információs rendszereinek besorolása

9. sz. melléklet: Információbiztonsági tájékoztatás

10. sz. melléklet: Szerverszoba belépési napló

11. sz. melléklet: Karbantartási napló

12. sz. melléklet: Titoktartási nyilatkozat

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 15.§ (1) bekezdés d) pontjában, valamint a törvényben meghatározott technológiai biztonsági, a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII.15.) BM rendelete, az önkormányzati ASP rendszerről szóló 257/2016. (VIII.31.) Korm. rendelete, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24.§ (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. 30.§ (1) bekezdésében kapott felhatalmazás alapján a Komlói Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) informatikai biztonsági szabályzatát az alábbiakban határozom meg:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

A szabályzat célja, hogy biztosítsa a Hivatal és intézményei, alkalmazottai által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IT alkalmazása során biztosítsa a Hivatalnál az alábbiakat:

- titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást, az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- munkaállomásokon (USER) lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését, a számítógépes rendszerek zavartalan üzemeltetését, 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.

Jelen IBSZ a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát.

Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.

2. A SZABÁLYZAT HATÁLYA

2.1. Szervezeti-személyi hatálya kiterjed:

- A Komlói Közös Önkormányzati Hivatal és Mánfa Község Önkormányzat minden olyan munkatársára, illetve a hivatallal polgári jogi jogviszonyban álló személyre, aki a munkavégzés, feladatellátás az információ technológiai (továbbiakban: IT) eszközökkel, valamint az általuk kezelt adatokkal kapcsolatba kerül, ezekkel az eszközökkel, adatokkal munkát végez.

- A Komlói Közös Önkormányzati Hivatal és Mánfa Község Önkormányzat informatikai rendszerével, szolgáltatásaival polgári jogi jogviszony alapján vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre a velük kötött szerződésben rögzített mértékben, illetve titoktartási (*12.sz.melléklet*) nyilatkozat alapján.

2.2. Tárgyi hatálya kiterjed:

- a Hivatal tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre,
- a rendszer- és felhasználói programokra;
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók tárolására, felhasználására;
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

A szabályzat előírásait alkalmazni kell a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások illetőleg dokumentumok esetében. A tárgyi hatály kiterjed az önkormányzati ASP központ által nyújtott szakrendszerek felhasználó oldali komponenseire (munkaállomások, azokon futó szoftverek, kártyaolvasó, e-személyi). A nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

3. AZ IBSZ ÁLTALÁNOS KÖVETELMÉNYEI

Az IBSZ és a jelen IBSZ *2. sz. melléklete* (továbbiakban: FIBH) előírásainak alkalmazása, betartása kötelező.

Az információbiztonsági előírások betartása megvédi a Hivatalt, felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

A felhasználók részére a FIBH, a Hivatal vezető tisztségviselői, a rendszergazda, az adatgazdák részére a teljes IBSZ előírásai a mérvadók.

A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. Az IBSZ és a FIBH el nem olvasása nem mentesít a felelősség alól.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák a FIBH előírásait.

A Hivatal elektronikus információs rendszereit csak az IBSZ *3.sz. mellékletében* található nyilatkozat aláírása után lehet használatba venni.

4. IBSZ FELÜLVIZSGÁLATA

Az IBSZ módosítására van szükség, ha a Hivatal elektronikus információs rendszereinek működésében, vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben jelentős változások következnek be.

Az IBSZ-t legalább évente egy alkalommal felül kell vizsgálni.

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a jegyző hatásköre.

II. Adminisztratív védelmi intézkedések

5. A HIVATAL ELEKTRONIKUS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

Az állami és önkormányzati szervek elektronikus információbiztonságról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervezeteket biztonsági szintbe kell sorolni. A szervezet adatkezelésével érintett elektronikus információs rendszereinek biztonsági osztályba sorolását a 41/2015. (VII. 15.) BM rendelet 1. melléklete alapján kell elvégezni. A szervezet besorolási szintje az informatikai rendszerek legmagasabb biztonsági osztályával azonos besorolású, de legalább az Ibtv.9.§ (2) bekezdésében meghatározott 2. biztonsági szintű.

A biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adat bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer sértetlenségének és rendelkezésre állásának sérülése esetén bekövetkező kár mértéke alapján kell elvégezni.
A Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását *a 8. sz. melléklet* tartalmazza.

Az önkormányzati ASP rendszer szakrendszereit az ASP működtetője sorolja biztonsági osztályba. Az önkormányzat oldali szükséges védelmi intézkedéseket a csatlakozási szerződésben megfogalmazottak szerint kell végrehajtani.

A biztonsági osztályba sorolást mindig kockázatelemzéssel együtt kell végezni.

A biztonsági osztályba sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be Hivatal szervezeti felépítésében;
b) az elektronikus információs rendszerben kezelt adatok bővülnek vagy az adatok köre változik;
c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

Ha nem történik lényegi változás, a biztonsági osztályba sorolást háromévente felül kell vizsgálni.

A biztonsági osztályba sorolást a jegyző hagyja jóvá.

A felhasználóknak az információ kezelése során tisztában kell lennie az adott információ védelmi igényével és ennek megfelelően kell kezelniük azt.

6. A HIVATAL BIZTONSÁGI SZINTBE SOROLÁSA

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint. A szervezet besorolási szintje az informatikai rendszerek legmagasabb biztonsági osztályával azonos besorolású, de legalább az Ibtv.9.§ (2) bekezdésében meghatározott 2. biztonsági szintű.

Az elvégzett kockázatelemzés, kárérték becslés és az informatikai rendszerek osztályba sorolása alapján **a Hivatal biztonsági szintje 2.**

7. KOCKÁZATELEMZÉS ÉS KEZELÉS

Az információbiztonsági kockázatelemzés célja, hogy feltárja a Hivatal elektronikus információs rendszereire és az azokban kezelt adatokra ható fenyegető tényezőket, veszélyforrásokat (fenyegetettség elemzés), vizsgálja az elektronikus információs rendszer gyenge pontjait (sérülékenység vizsgálat), elemezze a veszélyforrások által a gyenge pontokon keresztül bekövetkező sikeres támadások bekövetkezési valószínűségét és az általuk okozott kár nagyságát (kockázatelemzés), valamint kezelje a Hivatal által el nem fogadható kockázatokat (kockázatkezelés).

A kockázatarányos védelem kialakításához rendszeres és tervszerű informatikai kockázatkezelésre van szükség. Annak érdekében, hogy a kockázatkezelési folyamata a Hivatal számára jól követhető, megismételhető és ellenőrizhető legyen, írásos kockázatkezelési módszertanra van szükség, mely mind a kockázatelemzés, mind a kockázatkezelés területén lefekteti az alapvető végrehajtási módszereket.

A kockázatelemzési és kezelési módszertant jelen IBSZ *7. sz. melléklete* tartalmazza.

A kockázatelemzést soron kívül el kell végezni, hogy ha

a) változás áll be az elektronikus információs rendszerben vagy annak működési környezetében (beleértve az új fenyegetések és sebezhetőségek megjelenését),

b) olyan körülmények következnek be, amelyek befolyásolják az elektronikus információs rendszer biztonsági állapotát.

A kockázatok kezelésére, az ügymenet folytonossági és informatikai katasztrófa-elhárítási tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős és határidő megjelölésével.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az informatikai biztonsági felelős, a rendszergazda, a jegyző, valamint a jegyző által írásban kijelölt személyek jogosultak.

8. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS – BESZERZÉSI ELJÁRÁSREND

A Hivatalnak a jelen fejezetben foglalt követelmények alapján kell az elektronikus információs rendszereire vonatkozó beszerzéseit elvégeznie.

8.1. Erőforrás igény felmérés

Az éves költségvetési tervezési folyamatban ki kell térni az elektronikus információs rendszerek biztonsági beruházásainak tervezésére, oly módon, hogy az a Hivatal költségvetésében elkülönítetten szerepeljen.

A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok alapján kell elkészíteni.

Az informatikai igények tervezési dokumentumot az információbiztonsági felelős készíti el a hivatalvezetővel együttműködve.

Az információbiztonsági beruházások tervezését tartalmazó igényfelmérést az információbiztonsági felelős terjeszti be a Jegyzőnek jóváhagyás céljából.

8.2. Beszerzések

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

- a funkcionális biztonsági követelményeket,
- a garanciális biztonsági követelményeket,
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

8.3. Elektronikus információs rendszer védelmi szempontjainak érvényesítése a beszerzés során

A szállítónak a következő dokumentumokat kell elkészítenie az átadás-átvétel előtt:

- a szállítandó termék/fejlesztés biztonsági intézkedéseinek funkcionális biztonsági leírása;
- adminisztrátori dokumentáció;
- felhasználói dokumentáció.

A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

Gondoskodni kell a biztonsággal kapcsolatos dokumentumok illetéktelenek elleni védelméről az EIR teljes életciklusa (létrehozás, módosítás, megsemmisítés) alatt.

Fejlesztési szerződések biztonsági követelményei

A fejlesztést végző külső féllel megkötendő szerződésnek a következőket kell tartalmaznia:

Minden egyes, a Hivatal elektronikus információs rendszerével kapcsolatba kerülő fejlesztési vagy bővítési projektnél figyelembe kell venni a Hivatal érvényben lévő, vonatkozó szabályzatait, különös tekintettel az IBSZ-re, annak tudomásul vételét és elfogadását a szerződésben rögzíteni kell.

Fejlesztett komponensek esetében a szerződésben rögzíteni kell, hogy a leszállított szoftver megfelelően biztonságos környezetben, auditálható körülmények között készült, így nem tartalmaz kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Hivatalnak bármilyen kára keletkezne, akkor azért a Szállító felelősséggel tartozik.

Rendszerkövetés (támogatás)

Az infokommunikációs rendszerhez a szállítónak szerződésben rögzített feltételek mellett az alábbi területeket magába foglaló támogatást kell nyújtania:

- az infokommunikációs rendszerben felmerülő hibák javítása,
- a Hivatal fejlesztési igényeinek ellátása,
- az infokommunikációs rendszer futtató környezetének (operációs rendszer, adatbázis rendszerek) frissítése.

A szerződésben rögzíteni kell a támogatás körülményeit (határidők, rendelkezésre állás, helyszíni vagy telefonos támogatás) is a megfelelő szolgáltatási szint biztosítására. A paraméterek pontos értékének meghatározása az infokommunikációs rendszer adatgazdájának és az informatikai üzemeltetésért felelős vezető feladata.

Az elektronikus információs rendszerre vonatkozó dokumentáció

A szállítónak következő dokumentációkat kell készítenie a fejlesztés során:

Adminisztrátori dokumentáció

Az adminisztrátori dokumentációnak tartalmaznia kell:

- a technikai környezet ismertetését,
- a kapacitástervezési leírást,
- az alkalmazott portok, szolgáltatások, és protokollok részletes ismertetése,
- a kommunikációs környezet ismertetését,
- a szerepköröket és hozzájuk tartozó feladatok ismertetését,
- a jogosultsági rendszer részletes ismertetését,
- a feldolgozások részletes ismertetését üzemeltetési szempontból,
- a mentés, archiválás, monitorozás ismertetését,
- az időszaki teendők ismertetését,
- a hibaüzenetek, hibaelhárítással kapcsolatos feladatok ismertetését,
- rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
- a biztonsági funkciók hatékony alkalmazását és fenntartását,
- a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

Felhasználói dokumentáció

A felhasználói dokumentáció tartalmazza:

- a funkciók felhasználói leírása képekkel illusztrálva,
- a kezelési felületek, menürendszer ismertetését,
- az interfész leírásokat,
- a funkcióleírásokat, a funkciójegyzéket,
- a kapcsolódó rendszerelemek pontos hivatkozását,
- az ellenőrzési és hibakezelési eljárásokat / hibajegyzéket,
- logikai kontrollok ismertetése.

A fejlesztett termék csak a sikeres átadás-átvételt követően illeszthető be a Hivatal informatikai rendszerébe.

A sikeres átadás-átvétel feltétele a jelen IBSZ-ben meghatározott dokumentációk Hivatal általi elfogadása, a funkcionális biztonsági követelmények IBF általi, tesztrendszerben történő ellenőrzése.

9. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK, ÜGYMENET FOLYTONOSSÁGÁNAK TERVEZÉSE

A Hivatal elektronikus információs rendszereinek folyamatos működésének biztosítása érdekében, valamint a katasztrófa-helyzetek bekövetkezte során a jelen fejezetben foglaltak szerint kell eljárni.

9.1. Ügymenet folytonosságra vonatkozó eljárásrend

Az IBF-nek az érintett területek bevonásával ki kell dolgoznia és jóvá kell hagyatnia az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet (továbbiakban: ÜFT).

A folyamatos működés tervezésére vonatkozó tevékenységeket össze kell hangolni a biztonsági események és vészhelyzeti/katasztrófa helyzetek kezelésével.

A tervezés során meg kell határozni a Hivatal által biztosítandó szolgáltatásokat és alapfunkciókat, valamint az ezekhez kapcsolódó és a Hivatal részéről elvárt vészhelyzeti követelményeket.

Meg kell határozni az elektronikus információs rendszer kiesése esetére a helyreállítási feladatokat, a helyreállítási prioritásokat és azok mértékét.

Ki kell jelölni a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket.

Az ügymenet-folytonosságot úgy kell kialakítani, hogy az biztosítsa a Hivatal által előzetesen definiált alapszolgáltatások fenntartását, még az elektronikus információs rendszer összeomlása vagy hibája ellenére is.

Ki kell dolgozni a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

ÜFT felülvizsgálata

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

- az elektronikus információs rendszer vagy a működtetési környezet jelentős változása,
- az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén.

Az Ügymenet-folytonossági terv változásairól képzés formájában tájékoztatni kell a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

Az ÜFT kezelése

Az Ügymenet-folytonossági terv jóváhagyott példányának páncélszekrényben történő őrzéséről a rendszergazda gondoskodik.

Az Ügymenet-folytonossági terv bizalmas dokumentumnak tekinthető, ezért csak az abban megjelölt személyek számára hozzáférhető, illetékteleneknek nem adhatják tovább.

9.2. Kritikus rendszerelemek meghatározása

Az ÜFT-ben meg kell határozni a Hivatal elektronikus információs rendszereinek alapfunkcióit támogató kritikus rendszerelemeket.

9.3. Folyamatos működésre felkészítő képzés

A felhasználókat folyamatosan képezni kell az ÜFT-ben megfogalmazott működési feltételek biztosítása érdekében.

9.4. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jog-szabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárás-rendet kell kidolgozni a következők figyelembevételével:

Rendszeres mentéseket kell készíteni a legalább 2-es biztonsági osztályba sorolt elektronikus információs rendszerekről és az azokban kezelt adatokról. A mentések során a következő adat-fajták mentését kell biztosítani:

- felhasználói szintű adatok (ügyviteli adatok)
- rendszerszintű információk
- naplóinformációk
- a rendszerrel kapcsolatos dokumentációk.

Biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a lényeges adatok és szoftverek esetleges adathordozó hiba, az elektronikus információs rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

A mentési eljárásrendet úgy kell kialakítani, hogy az egyrészt megfeleljen az üzembiztonsági elvárásoknak, másrészt minél biztonságosabb védelmet nyújtson az esetlegesen előforduló hibák ellen.

Az EIR-ek fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az ügymenet folytonosság fenntartása érdekében a mentéseket tartalmazó adathordozókat szerverhelyiségtől elkülönítve, páncélszekrényben kell tárolni.

9.5. Infokommunikációs szolgáltatások

Ha lehetséges tartalék internet vonalat kell biztosítani az önkormányzati ASP rendszer folyamatos elérése érdekében. Amennyiben az elsődleges vonal nem áll rendelkezésre, úgy a rendszergazdának gondoskodnia kell a tartalék vonal beüzemeléséről. Olyan tartalék szolgáltatást kell biztosítani, mely az éles vonaltól elkülönülő vonalon biztosítja az internetelérést.

Az internet szolgáltatókkal kötött szerződéseknek tartalmazniuk kell az elvárt

- szolgáltatási időszakot,
- szolgáltatási szintet,
- helyreállítási időket.

9.6. Az elektronikus információs rendszer helyreállítása és újraindítása

Az ügymenet-folytonosság tervezése során ki kell dolgozni az elektronikus információs rendszerek helyreállítási terveit, melyek a katasztrófahelyzetek kezelésére vonatkozóan a következőket kell tartalmaznia:

- katasztrófát követő helyreállítandó célállapotot;
- a katasztrófa eseményeket;
- a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;
- a helyreállítási terv hatókörét;
- a megelőzés érdekében végzett tevékenységeket;
- felkészülés a katasztrófa elhárítására;
- katasztrófa esetén végrehajtandó tevékenységek;
- elektronikus információs rendszerek vészleállításának és újraindításának folyamatát;
- a helyreállítási terv tesztelését, karbantartását.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

A rendszergazdának - mindezeken túl - gondoskodnia kell az elektronikus információs rendszer helyreállításához szükséges mentések meglétéről, elérhetőségéről.

10. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ – SZEMÉLY BIZTONSÁG

10.1. Információbiztonsági tevékenységek

A Hivatalban a következő információbiztonsági tevékenységeket kell ellátni:

- informatikai kockázatelemzés és kezelés,
- elektronikus információs rendszerek biztonsági felügyelete,
- új elektronikus információs rendszerek információbiztonsági véleményezése és elfogadása,
- szervezetek közötti információbiztonsági együttműködés,
- az információbiztonság független felülvizsgálata.

10.2. Az információbiztonsági felelősségi rend meghatározása

Az információbiztonság megvalósítását, fenntartását és ellenőrzését a Hivatal a feladatok és felelősség szempontjából egymástól elhatárolt szervezeti keretek között valósítja meg.

A Hivatal információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

- a szervezet vezetője (jegyző),
- az információbiztonsági felelős, rendszergazda,
- az adatgazdák,

- a szervezeti egység vezetője,
- önkormányzati ASP adminisztrátor,
- önkormányzat szakrendszeri adminisztrátor,
- a felhasználók.

A jegyző az Ibtv. alapján gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

- biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
- biztosítja a Hivatalra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
- meghatározza a Hivatal elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az információbiztonsági szabályzatot,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a Hivatal munkatársai információbiztonsági ismereteinek szinten tartásáról,
- gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,
- biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,
- ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a jelen IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek,
- felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,
- megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket,
- biztosítja a jogszabályokban meghatározott hatóságok részére az ellenőrzés lefolytatásához és a biztonsági incidensek kivizsgálásához szükséges feltételeket.

Az IBF, rendszergazda:

- gondoskodik a Hivatal elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

- felelős az elektronikus információs rendszerek IBSZ-ben foglaltak szerinti üzemeltetéséért,
- előkészíti a Hivatal elektronikus információs rendszereire vonatkozó információbiztonsági politikát, információbiztonsági stratégiát és az információbiztonsági szabályzatot,
- előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a Hivatal biztonsági szintbe történő besorolását,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit,
- kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal,
- biztosítja a jogszabályokban meghatározott követelmények teljesülését,
- közreműködik a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában,
- felel a Hivatalnál üzemelő informatikai rendszerek, infrastruktúrák működtetésével, kialakításával és felügyeletével kapcsolatos feladatok ellátásáért,
- ellenőrzi a Hivatal informatikai biztonsági állapotának fenntartását szolgáló és garantáló műszaki-technikai, fizikai és adminisztratív területet érintő belső szabályok betartását,
- a Hivatallal köztisztviselői vagy munkavégzésre irányuló egyéb jogviszonyban állók és más személyek a Hivatal területén vagy a Hivatallal kapcsolatba hozható módon veszélyeztető, jogsértő magatartása megelőzése, felderítése, folytatásának megakadályozása érdekében elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására,
- biztosítja az informatikai rendszerek használatához szükséges hálózati- és erőforrás-hozzáférési jogokat a felhasználók részére,
- a hálózati felhasználók üzemeltetési feladatainak szakmai irányítása,
- ellenőrzi az SZMSZ rendelkezései és a munkaköri leírások alapján az informatikai rendszer szereplőinek jogosultsági szintjét,
- nyomon követi a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, szükség esetén belső riasztást és figyelmeztetést ad ki,
- felügyeli a Hivatalon belüli informatikai helyiségeket, eszközöket és infrastruktúrát érintő karbantartási terveket.

Adatgazda

Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését vagy nyilvántartás vezetését elrendeli.

Az adatgazdák a jelen IBSZ *8.sz. mellékletében* kerültek kijelölésre.

Az adatgazda meghatározza az adatokhoz/tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges.

Az adatgazda felelős a hatáskörébe tartozó elektronikus információs rendszerek hozzáférési jogosultságainak - a lehetőségek szerint - a „szükséges, minimális jogosultságok” elve alapján történő engedélyezéséért.

A szervezeti egység vezetője

A szervezeti egység vezetőjének feladata és felelőssége, hogy az általa irányított szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági előírásokat.

Önkormányzati ASP adminisztrátor

Az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat) szintű felhasználó kezelés, azaz

- az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása;
- az adott tenant felhasználók tanúsítványkezelése, e-szig, hozzárendelése, adminisztrációja és karbantartása.

Önkormányzat szakrendszeri adminisztrátor

Az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

A felhasználó

A Hivatal felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

A felhasználó jogosult:

a) a számára biztosított infokommunikációs eszközök, szoftverek üzemszerű használatára,

b) a beállított jogosultságának megfelelően, a munkájához szükséges adatállományok elérésére,

c) információbiztonsági képzésre,

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftverek használatához támogatást kérni,

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

A felhasználó kötelessége

Az információk védelmét azok keletkezésének, feldolgozásának, szétosztásának, tárolásának és selejtezésének teljes folyamata, életciklusa során biztosítani kell.

Valamennyi felhasználó köteles azonnal értesíteni felettesét a következő eseményekről, körülményekről:

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása,

b) ha olyan adatokhoz fér hozzá, melynek kezelésében nem illetékes,

c) információbiztonsági esemény.

Az munkahelyi vezetőnek jeleznie kell a tapasztaltakat a rendszergazda részére, aki információbiztonsági incidens esetén értesíti az IBF-et.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, kulcsot, vagy bárminemű egyéb, a Hivatal erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló felülvizsgálatokban a felhasználó köteles együttműködni a kivizsgálókkal.

A felhasználó számára büntetőjogi, illetve munkajogi felelősségre vonás terhe mellett tilos illetéktelenül más felhasználó jogosultságainak használata, a hálózat monitorozása, felderítése, jelszavak kipróbálása, illetve ezek kísérlete is.

A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a jelen IBSZ *2. sz.mellékletének* megismeréséért és az abban foglalt szabályok betartásáért,

b) az önkormányzati ASP központ működtetője által közzétett felhasználói biztonsági követelmények betartásáért,

c) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért,

d) a személyre szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért,

e) az elektronikus információs rendszerben végzett műveletekért,

f) a Hivatal elektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

10.3. A munkaköri felelősség és az alkalmazás feltételei

A munkaköri leírásokban meg kell határozni az általános és az adott munkakörhöz tartozó információbiztonsági feladatokat és felelősségeket.

A Hivatalnak tájékoztatnia kell a dolgozókat arról, hogy milyen jogi felelősségük és kötelezettségük van az információbiztonsági előírások betartására vonatkozóan. A dolgozók információbiztonsági felelőssége arra az esetre is vonatkozik, ha nem a Hivatalban (pl. otthon), illetve a normál munkaidőn kívül dolgozik.

A munkahelyi vezető közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az IBSZ előírásait.

A Hivatal elektronikus információs rendszereit csak a jelen IBSZ 3*.sz.mellékletben* található nyilatkozat és az ASP titoktartási nyilatkozat aláírása után lehet használatba venni.

10.4. Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatalban nincsenek nemzetbiztonsági ellenőrzés alá eső munkakörök és feladatok.

A jelen fejezetben foglaltakat az IBSZ éves felülvizsgálatával párhuzamosan felül kell vizsgálni.

10.5. A személyek ellenőrzése

A Hivatal személyügyekért felelős vezetőjének a feladata, hogy az elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személy a feltételeknek megfelel-e. A vizsgálat magában foglalja az alábbiakat:

- referenciák ellenőrzése,
- a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,
- a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,
- nyelvtudást igazoló okiratok ellenőrzése,
- hatóság által kibocsátott azonosító irat ellenőrzése,
- erkölcsi bizonyítvány ellenőrzése.

10.6. Biztonsági események kezelése

Biztonsági incidensnek számít minden, az informatikával kapcsolatba hozható rendellenes működés, fenyegetés, amely az adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását veszélyezteti.

A Hivatal az elektronikus információs rendszerek biztonsági eseményeinek kezelésekor a következők szerint jár el:

- Dokumentált eljárást kell kialakítani a biztonsági eseményekről szóló jelentések elkészítésére, a visszajelzések kezelésére.

- A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát.
- A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *6.sz. mellékletében* található űrlapot kell használni.
- Biztonsági esemény esetén az IBF látja el a biztonságiesemény-kezelési megbízott feladatait.
- Hivatali kapun keresztül haladéktalanul jelentenie kell a biztonsági eseményt a Kormányzati Eseménykezelő Központ (továbbiakban: GovCert) részére. Amennyiben a biztonsági esemény érinti az önkormányzati ASP rendszert, úgy a biztonsági eseményt az önkormányzati ASP rendszer működtetőjének is jelenteni kell.
- a bejelentéshez csatolni kell a biztonsági eseményhez kapcsolódó valamennyi bizonyítékot.
- a Hivatalnak együtt kell működnie a GovCert-tel a biztonsági esemény kezelésében és a GovCert által javasolt intézkedéseket végre kell hajtania.
- kivizsgálást kell kezdeményezni a beérkezett jelentés alapján és javaslatot kell tennie a jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.
- Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy javaslatot kell tennie a jegyző részére a fegyelmi eljárások lefolytatása érdekében.

Jelentés a biztonság gyenge oldalairól

A rendszergazda köteles azonnal jelenteni az IBF-nek, amennyiben munkája során biztonsági veszélyeket, vagy az elektronikus információs rendszerben valamilyen gyenge pontot fedeztek fel.

Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

- fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet is,
- be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből. A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Okulás a biztonsági eseményekből

Az IBF-nek a bejelentett biztonsági eseményekről, veszélyes helyzetekről, illetve a működési zavarokról, azok előfordulási gyakoriságáról, és kezelésükre tett intézkedések eredményéről jelentést kell készítenie jegyző számára.

Az IBF feladata a biztonsági események kezelése során nyert tapasztalatok felhasználásával a meglévő biztonsági rendszer – így a szabályozó elemek és technikai megoldások felülvizsgálata és szükség esetén tökéletesítése.

Szükség esetén (nagy kár, vagy várható jelentős potenciális kár, illetve gyorsan szaporodó előfordulás esetén) az egyes eseményeket, illetve esemény típusokat az IBF-nek soron kívül jelentenie kell a jegyző részére.

10.7. Eljárás jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

- Jogosultságok megszüntetése, úgy hogy a régi állapot mentésre vagy dokumentálásra kerül.
- A felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról.
- Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve ha szükséges a megadott idő után törölni a rendszerből.

A fenti feladatok végrehajtásáért a rendszergazda a felelős.

Vagyontárgyak visszaszolgáltatása

Valamennyi felhasználónak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia a Hivatal valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

A rendszergazdának az eszköz leadásakor ellenőriznie kell, hogy a felhasználó az átvételi elismervényben rögzített hardver-, szoftver specifikációval adja-e vissza a munkaállomást.

Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár.

A fentiektől eltérni a jegyző írásos engedélyével lehetséges.

A feladatok végrehajtásáért a rendszergazda a felelős.

Információbiztonsági kötelmek a jogviszony megszűnése után

A személyügyi referensnek a jelen IBSZ *9. sz.mellékletében* foglaltak szerint tájékoztatnia kell a dolgozót arról, hogy a jelen IBSZ-ben foglalt kötelezettségei a jogviszony megszűnése után is fennállnak, az abban foglaltak megsértése jogi következményeket von maga után.

10.8. Áthelyezések, átirányítások és kirendelések kezelése

Az áthelyezés során, szükség esetén el kell végezni az érintett munkatárs ellenőrzését a jelen IBSZ **Hiba! A hivatkozási forrás nem található.** „**Hiba! A hivatkozási forrás nem található.**” pontjában foglaltak alapján.

Az érintett munkatárs részére az elektronikus információs rendszerhez történő logikai és fizikai hozzáférések engedélyezését a jelen IBSZ „22.3. Hozzáférési jogok igénylésének eljárásrendje” pontjában foglaltaknak megfelelően kell elvégezni.

Szükség esetén el kell végezni az áthelyezés miatt megváltozott hozzáférési engedélyek módosítását vagy megszüntetését.

A jogviszony megváltozásáról a jegyző értesíti a munkatárs régi, valamint új vezetőjét.

10.9. Fegyelmi intézkedések

A jelen IBSZ-ben előírt szabályok megszegéséről az észlelő haladéktalanul köteles tájékoztatni az IBF-et. Az IBF a tudomására jutott események súlyosságát mérlegeli, és szükség esetén jelenti a jegyzőnek.

A biztonsági előírások megsértőivel szemben fegyelmi felelősségre vonásra kerülhet sor, amelyet az IBF által felterjesztett jelentés alapján a jegyző kezdeményez. Az eljárás a jogszabályok és a Hivatal belső szabályai szerint történik.

Külső szerződő fél által elkövetett szabályszegés esetében a szerződésben foglaltak szerint, illetve a vonatkozó jogszabályok alapján kell eljárni.

10.10. Belső egyeztetés

A Hivatalnak terveznie kell az elektronikus információs rendszerei biztonságát érintő tevékenységeit, annak érdekében, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

10.11. Viselkedési szabályok az interneten

A Hivatal által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai.

A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja.

A nem munkavégzést szolgáló hálózati sávszélesség foglalása (pl. nagyméretű állományok letöltése), és adatok kiszolgálón történő tárolása esetén a felhasználó figyelmeztetésben részesül. Ismételt előfordulás esetén az rendszergazda jelentést tesz a jegyző felé.

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, kiiktatása. Ebbe a körbe tartoznak a vírusellenőrző és Internet böngésző kontrollok is.

Tilos internetes vagy más jellegű szolgáltatást nyújtó külső féllel hálózati kapcsolat kialakítása.

Tilos az elektronikus információs rendszerek használata a Hivatali értékekkel összhangban nem álló célokra, vagyis pl. szexuális jellegű fájlok fogadására, küldésére, fenyegetésre vagy megfélemlítésre, megkülönböztetésre, gyűlölködésre, fegyverekkel és illegális drogokkal való kereskedésre, erőszakra, internetes- illetve szerencsejátékokra, bármilyen kereskedelmi illetve jogellenes tevékenységre.

Tilos hivatali adatok tárolására külföldi felhő-alapú tárhely-szolgáltatást igénybe venni. Amennyiben külföldi felhő-alapú tárhely-szolgáltatás igénybe vételére van szükség, úgy előzetesen engedélyeztetni kell a Nemzeti Elektronikus Információbiztonsági Hatósággal, de ebben az esetben is csak EGT tagállamon belüli adatkezelés, illetve adatfeldolgozás lehetséges.

Az internetről csak Hivatali célból lehet fájlokat letölteni. Tilos fájlletöltő szolgáltatások használata. Különösen tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!

Tilos az interneten nem nyilvános hivatali információt közzétenni.

Az internetes oldalak elérése monitorozásra és naplózásra kerülhet, a munkával összefüggésbe nem hozható oldalak elérhetőségét az informatikai üzemeltetés jogosult korlátozni.

E-mail használat

A Hivatal által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag társasági munkavégzés céljára biztosított, ezért a felhasználóknak tilos a Hivatali e-mail címüket nem társasági minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra stb.)!

A Hivatal által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az e-mail a munkavégzéssel kapcsolatos levelezést szolgálja, ahol az egy felhasználóra eső tárterület korlátozott, és ennek túllépése esetén a rendszer figyelmeztetést küld, további figyelmeztetési határok átlépése esetén pedig megszűnhet a további levelezési lehetőség.

Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

Elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására.

A felhasználók alapértelmezésben a levelezés során csak a saját postaládájukat tudják kezelni, mások postaládáit nem látják.

Zavaró, félreinformáló levelek, spam-ek küldése, jogtalan megrendelések elindítása tilos, és eljárást vonhat maga után.

Ismeretlen helyről származó e-mail-t megnyitni nem szabad, mert maga a levél vagy annak csatolmánya vírus lehet, ezért ezeket olvasatlanul törölni kell.

A Hivatali hálózat és hálózatában résztvevő eszközök távoli elérésének szabályozása

A szabályozás célja, hogy meghatározza a Hivatal belső hálózatához való távoli gépről történő csatlakozás szabályait. A cél a hivatal hálózatának és hálózatán tárolt adatok védelme, a hálózati eszközök sebezhetőségének csökkentése. A károk magukban foglalják az érzékeny adatok elvesztését, a hivatal anyagi károsodását és az eszközök rendelkezésre állását. A távoli hozzáférést a jegyző engedélyezi.

- A távoli elérésnek VPN (Virtuális magánhálózati) kapcsolaton keresztül kell megvalósulnia.
- A rendszerbe való belépéshez szükséges a felhasználó azonosítására szolgáló felhasználói név jelszó megadása.
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni szigorúan TILOS!

10.12. Harmadik felekkel kapcsolatos előírások

Harmadik fél csak egyedi esetben, meghatározott időre és meghatározott feladat ellátásához látható el jogosultsággal, amit szerződésben kell dokumentálni. A hozzáférést az elektronikus információs rendszer adatgazdájának kell engedélyezni.

A Hivatal és szerződéses partnerei megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

A harmadik félnek a Hivatal elektronikus információs rendszereihez történő hozzáférése esetében - figyelembe véve a szükséges hozzáférési típusokat, az információ értékét, a harmadik fél által alkalmazott biztosítékokat, valamint a hozzáférés mélységét - törekedni kell a kockázatok minimalizálására.

Azokban az esetekben, amelyekben az információ feldolgozása vagy kezelése kiszervezéssel történik, a harmadik féllel kötött szerződésnek a betartandó biztonsági követelményeket is tartalmaznia kell.

Harmadik fél hozzáférése a Hivatal adataihoz és információihoz, a munkájához elengedhetetlenül szükséges minimum szintre kell korlátozni. A hozzáférések feltételeit szerződésben kell részletezni. A szerződés csak a Hivatal jelen IBSZ-évl összhangban lévő követelményeket tartalmazhat.

A szerződésnek tartalmaznia kell továbbá a bizalmasságra, a szellemi tulajdonjogokra, a szerzői jogok átruházására és minden közösen végzett munkálatok védelmére vonatkozó nem nyilvános garanciákat is.

A szerződésben elő kell írni, hogy a Hivatal információs vagyonelemei a szerződés lejártát követően kerüljenek vissza a Hivatal birtokába, a szerződött félnél - valamint annak partnereinél, alvállalkozóinál - pedig kerüljenek megsemmisítésre.

A szerződéses partnernek a Hivatallal egyeztetnie kell a számára nyújtott szolgáltatásokkal kapcsolatos minden részdöntést.

A szerződésben a Hivatal számára jogot kell biztosítani arra, hogy a már kölcsönösen elfogadott szerződéses felelősséget felülvizsgálja, szükség esetén harmadik féllel felülvizsgáltassa.

Harmadik fél a Hivatal adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen IBSZ *12. sz. mellékletében* található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, szükség szerint az alábbiakat kell előírni:

- a külső szervezetnek meg kell határoznia a Hivatallal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;
- meg kell követelni, hogy a szerződő fél feleljen meg a Hivatal által meghatározott személybiztonsági követelményeknek;
- meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;
- elő kell írni, 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 értesítést a Hivatalnak;
- az informatikai biztonság fő szabályait;
- az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;
- az információk másolásának és nyilvánosságra hozatalának feltételeit;
- a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;
- a felek felelősségének meghatározását;
- a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;
- a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;
- a felmerülő problémák kezelését;
- a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;
- világos és egyértelmű jelentéskészítési struktúrát és rendszert;
- a változáskezelések egyértelmű és meghatározott folyamatát;
- óvintézkedések meghatározását a kártékony kódok ellen;
- biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;
- az alvállalkozók bevonására vonatkozó szabályokat.

Abban az esetben, ha a feladat elvégzésére a harmadik fél alvállalkozót is igénybe vesz, a szerződésben pontosan meg kell nevezni az alvállalkozót, s meg kell határozni a rá vonatkozó hozzáférési jogosultságokat. A titoktartási kötelezettség a harmadik fél alvállalkozójára is vonatkozik, és a szerződésnek titoktartási nyilatkozat részt is kell tartalmaznia.

11. BIZTONSÁG TUDATOSSÁG KÉPZÉS

Rendszeres belső oktatásokkal gondoskodni kell arról, hogy a felhasználókban tudatosodjanak az alapvető információbiztonsági fogalmak, illetve ismerjék meg a munkájuk során felmerülő információbiztonsági fenyegetettségeket. Gondoskodni kell arról is, hogy a napi feladatok végzése során a felhasználók kellőképpen felkészültek legyenek a jelen IBSZ-ben foglaltak betartására.

11.1. Alapképzés

Minden felhasználó részére alap biztonság tudatosság képzéseket kell tartani. A képzésen a következő témaköröket kell érinteni:

- információbiztonságra vonatkozó jogszabályok;
- információbiztonsági alapfogalmak;
- felhasználók napi munkavégzése során jelentkező fenyegetettségek, azokkal szembeni védekezési lehetőségek;
- Hivatal információbiztonsági szabályozó rendszerének ismertetése.

Új dolgozó munkába lépésekor a dolgozóval a munkába állás előtt az információbiztonsági előírásokat meg kell ismertetni. A dolgozók információbiztonsági tudatosságának fenntartása érdekében évente frissítő oktatást kell szervezni.

Az információbiztonsági oktatások és továbbképzések tematikájának kidolgozása, a szükséges szakirodalom és tájékoztató anyagok biztosítása, valamint a képzés megtartása az IBF feladata.

Az oktatáson, illetve továbbképzésen való részvétel az elektronikus információs rendszerrel kapcsolatba kerülő személyek számára kötelező és a megjelenést a résztvevők aláírásukkal kötelesek tanúsítani (*4.sz. melléklet*).

11.2. Belső fenyegetés

A biztonsági képzések tematikáját úgy kell kidolgozni, hogy a felhasználó képes legyen felismerni a belső fenyegetéseket és legyen tudatában annak, hogy jelentenie kell a szabálysértéseket és egyéb belső fenyegetésből fakadó biztonsági incidenseket.

11.3. Szerepkör vagy feladat alapú biztonsági képzés

Az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy kijelölt feladat végrehajtását megelőzően és az elektronikus információs rendszerben bekövetkezett változás esetén a biztonsági képzés el kell végezni.

12. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

A rendszergazdának nyilvántartást kell vezetni a működtetett valamennyi elektronikus információs rendszerről. A nyilvántartásnak minden elektronikus információs rendszerre nézve a következőket kell tartalmaznia:

- annak alapfeladatait;
- a rendszerek által biztosítandó szolgáltatásokat;
- az érintett rendszerekhez tartozó licenc számot;
- 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.

III. FIZIKAI VÉDELMI INTÉZKEDÉSEK

13. FIZIKAI VÉDELMI ELJÁRÁSREND

Az elektronikus információs rendszer fizikai környezetének kialakítása, működtetése és használata során az általános biztonsági előírások szerint kell eljárni, az alábbiak szerint:

- az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani;
- a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell;
- a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről gondoskodni kell;
- a Hivatal közös használatú helyiségei és folyosóin infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása jegyzői engedéllyel történhet;
- valamennyi iroda és tárgyaló helyiség védett terület, a területek elhagyása esetén a bejárati ajtót zárva kell tartani;
- a Hivatal szerverszobája, a strukturált kábelezés rendező központja kiemelten védett terület, a helyiséget kiemelt belépési rendszerrel kell ellátni.

13.1. Az irodák, a helyiségek és az eszközök védelme

A Hivatalnak az irodák, a szobák és a számítógépterem védelmét az alábbiak szerint kell szabályozni:

- a kulcsokat nem szabad nyilvános, idegenek számára is könnyen hozzáférhető helyen tárolni;

- a védett és érzékeny helyiségek átlagos kinézetűek legyenek, ne hívják fel magukra a figyelmet, ne legyen rajtuk olyan jelzés, amelyből kiderül a funkciójuk;
- a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni. Amennyiben ez nem megvalósítható, úgy pin kódos védelmet kell megvalósítani.
- a dokumentumok tárolása védett területen történjen;
- azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat zárva kell tartani.

13.2. Az infokommunikációs eszközök elhelyezése és védelme

Az információs vagyon - lopás, veszélyeztetés, egyéb károsodás elleni - védelmének és a működési folyamatok folytonosságának biztosítása érdekében a Hivatal infokommunikációs eszközeit, azok megfelelő fizikai elhelyezésével és kezelésével is biztosítani kell.

Az infokommunikációs eszközöket úgy kell elhelyezni, és védelmüket úgy kell kialakítani, hogy minimálisra csökkenjenek a környezeti hatások következtében megjelenő kockázatok, és minimálisra csökkenjen az illetéktelen hozzáférések lehetősége, de a munkavégzés hatékonysága ne romoljon.

A védelmi intézkedések biztosítsák, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek, ezért

- be kell tartani a tűzvédelmi előírásokat;
- a Hivatal területére a normál háztartási vegyi anyagokon, tisztítószereken túl vegyi anyagot, robbanóanyagot behozni tilos;
- a monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen leolvasását;

Különös figyelmet kell fordítani az önkormányzati ASP rendszert elérő munkaállomások elhelyezésére, gondoskodni kell az illetéktelen hozzáférések megakadályozásáról.

13.3. Tápáramellátás

A kritikus infokommunikációs eszközök (kiszolgáló, tűzfal, router, switch) működését szünetmentes áramforrásról kell biztosítani. Intézkedéseket kell foganatosítani, hogy a kiszolgálók az áthidalási időn belül szabályosan leállíthatók legyenek.

13.4. A kábelezés biztonsága

Biztosítani kell az elektromos és adatvezetékek megszakadás és a rongálások elleni megfelelő védelmét.

A hálózati zavarok okozta hibák elkerülése érdekében az erősáramú vezetékeket el kell különíteni a kommunikációs hálózattól. A kábelstruktúra legyen érzéketlen az elektromos hálózati zavarokra.

13.4. Felhasználói szabályok

Az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen pontban leírtakat:

- a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az ügyfelek számára;
- a munkafázis végeztével, ill. az iroda hosszabb idejű elhagyása esetén ki kell jelentkezni az alkalmazásokból;
- a felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;
- ügyfelet irodában felügyelet nélkül hagyni tilos.

13.6. Felügyelet alól kikerülő eszközök

Szerviz részére eszközt csak a rendszergazda adhat át. Szervizbe történő szállítás esetén a szerviz által adott szállítólevelet a rendszergazda őrzi meg.

Szervizbe történő szállításkor vagy garanciális javítás esetén - jegyzőkönyv felvétele mellett – a rendszergazdának gondoskodnia kell az adatokat tartalmazó adathordozók törléséről.

A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) a Hivatalnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki- és beszállíthatják.

Minden más esetben eszközt kiszállítani csak a rendszergazda írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése a rendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállítása tilos. Az információbiztonsági tudatosság fokozását célzó oktatások keretében a felhasználókat tájékoztatni kell az ezzel kapcsolatos ellenőrzési feladatokról és jogokról.

14. FIZIKAI BELÉPÉSI ENGEDÉLYEK

El kell készíteni és napra készen kell tartani az elektronikus információs rendszereknek helyt adó helyiségekbe belépésre jogosultak listáját. A belépésre jogosultak listája egyben a jogosultságot igazoló dokumentumként is szolgál. A belépésre jogosultak listáját a Hivatal Titkárságán kell tárolni.

15. FIZIKAI BELÉPÉS ELLENŐRZÉSE

15.1. Fizikai belépések

Az elektronikus információs rendszerek felhasználóinak a Hivatalba történő fizikai be- és kilépések tényét jelenléti íven rögzíteni kell. Naplózni kell a munkában töltött időt, valamint a távolléteket.

A jelenléti ívek megfelelő vezetését ellenőrizni kell. Az átvizsgálást a személyügyi referens végzi, aki megteszi a szükséges intézkedéseket a jegyző felé, amennyiben a naplók vezetése nem megfelelő.

Ügyfélfogadási időn kívül a Hivatal földszinti bejárati ajtaját zárva kell tartani. Hivatalba érkező vendégek, ügyfelek kíséretét annak a munkatársnak kell biztosítani, akihez a vendég érkezik. A Hivatalba történő be-és kilépések felügyeletét munkaidőben a portaszolgálatot teljesítő személy végzi.

15.2. Kulcsok megóvása

Gondoskodni kell a védett munkaterületek ajtóinak kulcsainak megőrzéséről. Amennyiben a kulcsot a birtokosa elveszti, azonnal jelentenie kell, majd gondoskodni kell az ajtó zárjának a cseréjéről.

15.3. Hozzáférés az adatátviteli berendezésekhez és csatornákhoz

A kiemelten védett területre (szerver szoba) belépés csak hivatalos célból, ellenőrzötten és kísérővel történhet. Az ajtókat zárva kell tartani. A szerverszoba kulcsát a rendszergazda tárolja, onnan csak az arra feljogosítottak vehetik fel. A jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni. (*10.sz. melléklet*). A szerverszoba áramtalanításáért a rendszergazda felelős

15.4. Tűz-, behatolásvédelem

A szerverszoba tűz- és villámvédelmi rendszerrel felszerelt helyiség lehet. A szerverhelyiségben független áramellátással ellátott tűzjelző készüléket, valamint elektromos tüzek oltására alkalmas tűzoltó készüléket kell alkalmazni. A szerverszobát behatolás védelmi rendszerrel kell ellátni

IV. LOGIKAI VÉDELMI INTÉZKEDÉSEK

16. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

A Hivatalnak úgy kell kialakítania az általános védelmi intézkedéseit, hogy biztosított legyen

- az elektronikus információs rendszer és annak környezete biztonsági állapotának felügyelete,
- meghatározásra kerüljenek az információbiztonsággal összefüggő szerepkörök és felelősségi körök,
- kijelölésre kerüljenek az ezeket betöltő személyek,
- az elektronikus információbiztonsági engedélyezési folyamatok kerüljenek integrálásra a társasági szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.
- az elektronikus információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden, a Hivatal tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi szintre és folyamatra.

16.1. Elektronikus információs rendszer kapcsolódásai

A Hivatal csak a felügyelete alatt álló informatikai rendszer felett gyakorol kontrollt, a rendszer felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett.

Az összekapcsolást mind a jegyzőnek, mind a rendszergazdának jóvá kell hagynia.

Dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

17. TERVEZÉS - BIZTONSÁGTERVEZÉSI ELJÁRÁSREND

17.1. Rendszerbiztonsági terv

A Hivatal az elektronikus információs rendszeréhez rendszerbiztonsági tervet készít, amely:

- meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;
- meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;
- meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;
- a vonatkozó rendszerdokumentáció keretébe foglalja az elektronikus információs rendszer biztonsági követelményeit;
- meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;
- gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);
- frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;
- elvégzi a szükséges belső egyeztetéseket;
- gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Ha egy adott információs rendszer jelentősége nem indokolja, vagy a jog, szabályozási, üzemeltetési körülmények nem teszik lehetővé, a Jegyző eltekinthet az adott rendszerre vonatkozó rendszerbiztonsági terv készítésétől.

18.KONFIGURÁCIÓKEZELÉSI ELJÁRÁSREND

18.1. Alap konfiguráció

A Hivatal valamennyi elektronikus információs rendszeréhez elkészíti az alapkonfigurációt, amelyet dokumentált formában, biztonságos helyen szükséges tárolni.

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia:

- Hardver elemek;
- Szoftverek;
- Egyes szoftverkomponensek alapkonfigurációi.

Az egyes elektronikus információs rendszerek alapkonfigurációját a rendszergazda évente felülvizsgálja, és a módosításokat átvezeti.

18.2. Elektronikus információs rendszerelem leltár

Az elektronikus információs rendszerek valamennyi hardver/szoftver eleméről a rendszergazdának nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a kiszolgálók és munkaállomások pontos és naprakész hardver konfigurációját, az elhelyezkedésüket, a működő alkalmazások egyedi beállításait és az értük felelős személy nevét.

18.3.Legszűkebb funkcionalitás

A Hivatal elektronikus információs rendszereiben csak a szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Az önkormányzati ASP rendszert elérő munkaállomásokon tilos olyan alkalmazást futtatni, amely a munkaállomást harmadik féllel köti össze, és amelynek segítségével lehetőség van távoli támogatásra, vezérlésre, képernyő átvételére.

18.4.Duplikálás elleni védelem

A Hivatalnak ellenőriznie kell, hogy az elektronikus információs rendszer hatókörén belüli elemek nincsenek-e felvéve más elektronikus információs rendszerek leltárában.

18.5.A szoftver használat korlátozásai

Szoftverek beszerzése

A Hivatalban kizárólag a jegyző által engedélyezett, jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni.

Ezen célok biztosítása érdekében új szoftverek beszerzése kizárólag a rendszergazda véleménye után lehetséges.

Szabad vagy nyílt forráskódú szoftverek használatbavételét a jegyző engedélyezi. Ezen szoftvereket használatba vétel előtt biztonságos körülmények között tesztelni kell.

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.

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 felhasználókhoz való installálásra is.

Jogvédelem

A Hivatal rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtiszta szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtiszta szoftverek tarthatóak. Ennek központi ellenőrzéséről a rendszergazda gondoskodik.

Szoftverek üzemeltetése

A szoftverek üzemeltetési feladatait a rendszergazda látja el. Ez folyamatos tevékenységet igénylő feladat, mind a szoftverkövetés, rendszeres mentés, mind pedig a rendszerhasználat felügyelete, ellenőrzése.

A rendszergazda feladata a felhasználók rendelkezésére állás azok szoftver kezelési, szoftver működési problémáival kapcsolatban. A szoftverek kezelési problémáira helyszíni vagy telefonos segítségnyújtással, dokumentációkkal adhat megoldást.

A felhasználók problémáik megoldását a rendszergazdától közvetlenül kérhetik. A rendszerfelügyelet célja a rendeltetésszerű használat ellenőrzése, biztosítása.

Ebbe beletartozik az illegális szoftver-, ill. rendszerhasználatok kiderítése és megakadályozása, a vírusfertőzések ellenőrzése, jelentése és megszüntetése éppúgy, mint a nem használt szoftverelemek behatárolása, kivonásukra vagy kiváltásukra történő javaslattétel.

A másolatok és szétosztások ellenőrzése érdekében a telepítőkészleteket és a licenceket tartalmazó dokumentumokat zárható szekrényben kell tárolni és a hozzáféréseket ellenőrizni kell.

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

18.6.A felhasználó által telepített szoftverek

A felhasználók semmilyen alkalmazást nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak a rendszergazda végezheti el.

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

19. KARBANTARTÁSI ELJÁRÁSREND

A folyamatos működés érdekében a Hivatal elektronikus információs rendszereit a gyártó ajánlása alapján rendszeresen karban kell tartani. A karbantartások ütemezése, végrehajtása és az ellenőrzés megszervezése a rendszergazda feladata.

A számítógépek, perifériák, nyomtatók meghibásodása vagy felhasználó váltása estén, illetve 1 év folyamatos üzemelés után az alapvető karbantartást el kell végezni (felület tisztítása, az eszköz belsejéből a por eltávolítása, érintkezők tisztítása).
Az informatikai rendszereket kiszolgáló szerverek karbantartását évente el kell végezni (tisztítás, portalanítás stb.).
A működéshez szükséges hálózati kiszolgáló eszközök (switch, router) meghibásodása esetén azokat a tartalék készletből azonnal pótolni kell.

Szoftverek karbantartása

- a rendszergazda köteles a használt szoftverek frissítéseit figyelemmel kísérni, a kritikus frissítéseket haladéktalanul telepíteni,
- az üzemeltetett informatikai rendszerek verzióváltásait annak rendelkezésre állása után azonnal telepíteni kell,
- rendszergazda folyamatosan ellenőrzi, hogy minden használt szoftver üzemeltetési feltételei biztosítottak-e.

A tervezett karbantartásokat a jegyző engedélyezi. Amennyiben ez az elektronikus információs rendszerek leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges.
Az elvégzett karbantartási munkákat a karbantartási naplóban rögzíteni kell. (*11.sz.melléklet*)

A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

Karbantartók

Abban az esetben, ha saját erőből a karbantartás nem végezhető el, akkor a rendszergazda kezdeményezi a jegyzőnél külső fél (alvállalkozó) megbízását.

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

A karbantartást végző külső felekről nyilvántartást kell vezetni, melynek minimálisan a következőket tartalmaznia:

- szervezet megnevezése,
- szerződésszám,
- szerződés időtartama,
- szerződéses kapcsolattartó neve, elérhetősége,
- szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

Külsős szerződő fél munkavégzése esetén a rendszergazda biztosítja a folyamatos felügyeletet a karbantartás során.

Adathordozók ellenőrzése

A karbantartás során igénybe vett adathordozókat használatba vétel előtt kártékony kód elleni ellenőrzésnek kell alávetni.

Távoli karbantartás

Távoli karbantartást csak a rendszergazda végezhet. Az önkormányzati ASP rendszert használó munkaállomásokon távoli képernyő átvétel nem engedélyezett.

A távoli hozzáférések során VPN kapcsolatot kell alkalmazni, mely megfelelő erősségű titkosítással, ismert sérülékenységet nem tartalmazó kriptográfiai algoritmussal épül fel.

Távoli hozzáféréseket csak olyan eszközről lehet kezdeményezni, melyen

- naprakész, memóriában rezidens kártékony kód elleni védelem fut,
- naprakész, gyártó által támogatott operációs rendszer és alkalmazások futnak.

20. ADATHORDOZÓK VÉDELMÉRE VONATKOZÓ ELJÁRÁSREND

20.1. Hozzáférés az adathordozókhoz, adathordozók használata

A Hivatalban csak a Hivatal tulajdonában lévő adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

Otthoni munkavégzés és bármilyen más célból CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pen drive) adatot kijuttatni csak az Adatgazda vagy a szervezeti egység vezetőjének engedélyével lehet.

Az adatok kivitelét a Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

20.2. Adathordozók tárolása

A Hivatal elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A felhasználók részére kiosztott mobil adathordozókat használaton kívül zárható irodabútorban kell tárolni.

20.3. Adathordozók szállítása

A felhasználók részére biztosított mobil adathordozók a felhasználók részéről korlátozás nélkül szállíthatóak.

A kiszolgáló oldali adathordozók szállítására a rendszergazda jogosult. Ebben az esetben a szállítást dokumentálni kell.

20.4. Kriptográfiai védelem

Szállítás során biztosítani kell az adathordozókon tárolt adatok bizalmasságát és sértetlenségét. Ennek érdekében a felhasználók részére kiosztott mobil adathordozókon tárolt adatokat szabványos, ismert sérülékenységektől mentes kriptográfiai módszerrel titkosítani kell.

20.5. Adathordozók törlése

Az adathordozókat leselejtezés előtt a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal törölni kell.

20.6. Ismeretlen tulajdonos

A Hivatal elektronikus információs rendszereiben tilos nem a hivatal tulajdonát képező adathordozót csatlakoztatni.

20.7. Az infokommunikációs eszközök biztonságos újrahasznosítása vagy mások rendelkezésére bocsátása

Az infokommunikációs eszközök újrahasznosítása vagy mások rendelkezésre bocsátása előtt minden esetben gondoskodni kell arról, hogy az infokommunikációs eszközökön tárolt információk visszaállíthatatlanul eltávolításra kerüljenek. Ennek érdekében

- a rajtuk tárolt adatokat helyreállíthatatlanságot garantáló technikával törölni kell;
- a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;
- garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az adatok megfelelő módon történő eltávolításáért az adatgazda a felelős. Az adatok eltávolítását a rendszergazda végzi.

A hordozható infokommunikációs eszközök védelme

A hordozható infokommunikációs eszközök használata során a munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

- mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;
- cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;
- a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában;
- a mobil infokommunikációs eszközök ellopása esetén az ellopás tényét a lehető leggyorsabban jelenteni kell az IBF-nek.

Infokommunikációs eszköz elvesztése

Bármely infokommunikációs eszköz eltűnését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek és az IBF-nek, valamint tájékoztatni kell őket arról, hogy az eszköz tartalmaz-e bárminemű érzékeny információt. (Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve.)

21. AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁSREND

21.1. Azonosítás és hitelesítés, azonosító kezelés

Valamennyi elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie a Hivatal valamennyi felhasználóját és a felhasználók által végzett tevékenységeket.

Ennek érdekében egyénre szóló felhasználói azonosítókat kell képezni, a csoportos azonosítók használata nem engedélyezett.

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos.

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

- a jelszó legalább nyolc karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;
- az előző jelszavak újra használatát kerülni kell;
- zárolás esetén előre beállított időtartam eltelte után engedélyezze vissza a felhasználói fiókot.

A Hivatalban csak olyan azonosítási rendszert lehet alkalmazni, mely nem tárolja a jelszót nyílt formában.

21.2. Birtoklás alapú hitelesítés

Az önkormányzati ASP rendszer csak e-személyi használatával és jelszó alapú azonosítás és hitelesítés után érhető el. Az e-személyi tartalmazza a birtokláshoz szükséges adatokat (magán kulcs és egyéb azonosító adatok).

Kiemelt figyelmet kell fordítani az e-személyi megőrzésére.

21.3. A felhasználó felelősségi köre a jelszó használat során

A Hivatal elektronikus információs rendszereiben a jelszavak használatának és képzésének részletes szabályai a következők:

- a felhasználó a jelszavát köteles titokban tartani,

- a jelszószabályok betartása minden felhasználónak jól felfogott érdeke;

- a felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el;

- a felhasználói jelszót TILOS leírni;

- ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal értesíteni kell a rendszergazdát;

- nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé, pl. makróra, vagy funkció billentyűre;

- a jelszó könnyen megjegyezhető, és nehezen kitalálható legyen;

- semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja, ilyenek a nevek, telefonszámok, születési dátumok, stb.;

- ne legyen a gépnévre vagy a felhasználói névre utaló;

- ne legyen sorozat.

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét a rendszergazdának kell beállítani.

A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben.

22. HOZZÁFÉRÉS ELLENŐRZÉSI ELJÁRÁSREND

22.1. Felhasználói fiókok kezelése

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

A jogosultságok és a hozzáférés menedzselésekor az alábbi alapelveket kell figyelembe venni:

- A meghatározott jogosultságok alkalmazásával minimalizálható legyen a rosszindulatú vagy egyéb jogosulatlan hozzáférés kockázata.

- Az elektronikus információs rendszerrel kapcsolatba kerülő személyeknek a munkájuk ellátásához szükséges minimális jogosultságokat kell biztosítani, a munkavégzésük időtartamára.

- Az azonos tevékenységet ellátó felhasználók jogosultságai szerepkörök szintjén legyenek kialakítva, és a felhasználók a kialakított szerepkörökbe kerüljenek besorolásra.

- Az összeférhetetlenségi szabályokat figyelembe kell venni.

- Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

- Törekedni kell arra, hogy a jogosultságok automatizált módon kerüljenek nyilvántartásba, szükség esetén, papír alapon kell a nyilvántartást vezetni.

- Minden egyes elektronikus információs rendszerhez, csak a megfelelő adminisztrálást követően lehet felhasználói jogosultságot adni, módosítani, és felfüggeszteni, illetve visszavonni.

- Az éles elektronikus információs rendszerekben a fejlesztők hozzáférési jogosultságokkal nem rendelkezhetnek.

A felhasználók nyilvántartásba vételi szabályainak és a követendő eljárásrend kidolgozásakor a következőket kell figyelembe venni:

- A felhasználói tevékenység ellenőrizhetősége és nyomon követhetősége érdekében a felhasználók elektronikus információs rendszerekben történő azonosítására egyedi felhasználó azonosítókat kell alkalmazni.

- A csoportos felhasználó azonosítók használatát tiltani kell.

- A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:
    - a felhasználó munkakörét és az azzal kapcsolatos feladatait;
    - a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;
    - a felhasználó jogviszonyát;
    - a felhasználó munkahelyét.

- A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:
    - a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;
    - annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;
    - azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;
    - annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

- a munkahelyi vezető aláírását.

22.2. Kiemelt jogosultságok kezelése

A felhasználói jogosultságok kiadási folyamatánál szigorúbban kell kezelni a kiemelt jogokat biztosító adminisztrátori jogok megadását.

Az elektronikus információs rendszereknél a jogosultságok kiadásának engedélyezési eljárása során az alábbiakat kell figyelembe venni:

- pontosan meg kell határozni azokat a rendszerelemeket, - pl. operációs rendszereket, adatbázis kezelő rendszert, valamint az alkalmazásokat - és az alkalmazotti kategóriát, amelyhez az adminisztrátori jogosultságokat kell hozzá rendelni;

- az adminisztrátori jogosultságokat a „feltétlenül szükséges” és az „eseményenkénti” használat elve alapján kell kiadni;

- az adminisztrátori jogot kizárólag a jegyző engedélyezheti.

Az üzemeltetők csak az elektronikus információs rendszer, illetve alkalmazás üzemeltetéséhez szükséges információkhoz férhetnek hozzá, a részükre biztosított adminisztrátori jogosultság birtokában csak a felhasználó külön engedélyével és jelenlétében, kifejezetten a hiba elhárítása érdekében vagy a felhasználói igény kielégítése érdekében férhetnek hozzá a felhasználók által kezelt információkhoz.

22.3. Hozzáférési jogok igénylésének eljárásrendje

Az új hozzáférési jogok igénylését, a jogosultságok módosítását és a jogosultságok visszavonását a jelen fejezetben leírtak szerint kell elvégezni.

Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *5.sz. mellékletében* található űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

Az űrlapon meg kell jelölni az igényelt jogosultság szintjét, azt az időszakot, amelyre a jogosultságot biztosítani kell, illetve a jogosultságigénylés indoklását.

A kitöltött űrlapot alá kell írattatni a munkahelyi vezetővel, aki igazolja, hogy a feladatellátáshoz szükséges a jogosultság biztosítása.

A jogosultság beállításáról a rendszergazda intézkedik.

Hozzáférési jog módosítása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *5.sz. mellékletében* található űrlapot.

Az eljárásrend megegyezik az új hozzáférésben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

Hozzáférési jog visszavonása

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jelen IBSZ *5. sz. mellékletében* található űrlapon kell kezdeményezni.

Az űrlapot ezután el kell küldeni a rendszergazda részére, aki intézkedik a jogosultság visszavonásáról.

ASP szakrendszerek hozzáférése

Az ASP szakrendszerekhez történő hozzáférés feltétele, hogy a felhasználó rendelkezzen E-személyivel, melyet az okmányirodákban és a kormányablakokban igényelhet.

ASP szakrendszerekhez történő hozzáférések esetében az új felhasználó létrehozását az önkormányzati ASP adminisztrátornak kell jelezni az igényelt szakrendszer és a szakrendszeri szerepkör megadásával, aki a szükséges hozzáférés birtokában létrehozza a felhasználót az ASP rendszerben, illetve hozzárendeli a szakrendszeri szerepkörökhöz.

A kilépő felhasználókról a személyügyi ügyintézőnek értesítenie kell az önkormányzati ASP adminisztrátort, aki visszavonja a kilépő felhasználó jogosultságait.

A kiosztott jogosultságokat az önkormányzati ASP adminisztrátor évente felülvizsgálja és - az adatgazdákkal egyeztetve - a nem szükséges jogosultságokat visszavonja.

22.4. Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal elektronikus információs rendszereiben a jelen IBSZ-ben megfogalmazott logikai védelmi intézkedések végrehajtása érdekében a következő biztonsági funkciók kerülnek megállapításra:

- tűzfalak, behatolás-detektáló rendszerek üzemeltetése, konfigurálása
- kártékony kód elleni védelem üzemeltetése, konfigurálása
- operációs rendszerek üzemeltetése, konfigurálása
- EIR-ek adminisztrálása
- mentési rendszer üzemeltetése, konfigurálása

A biztonsági funkciók eléréséhez kifejezetten erre a célra létrehozott, egyedi azonosítóval lehet hozzáférni, melyet a napi munkavégzéshez tilos felhasználni. Ezen meghatározott biztonsági funkciók elérésére a rendszergazda jogosult.

22.5. A munkaszakasz zárolása, képernyőtakarás

A felhasználónak a már végzett munkafolyamat után az alkalmazásból ki kell lépnie. A képernyőt úgy kell elhelyezni, hogy az azon lévő adatokat illetéktelen személy ne lássa. A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

22.6. Vezeték nélküli hozzáférés

A Hivatalban csak az IBF által jóváhagyott vezeték nélküli (továbbiakban: Wi-Fi) hozzáférési pont létesíthető. A Hivatalban ad-hoc Wi-Fi hálózat nem létesíthető.

Valamennyi hozzáférési pontot a Hivatal által biztosított eszközön kell létrehozni. Biztosítani kell a hozzáférési pontok felügyeletét.

Minden hozzáférési pont részére külön VLAN-t kell létrehozni, úgy hogy a hálózatok között nem lehet átjárás és az egy hálózatban lévő eszközök sem érhetik el egymást. Az internet és a belső hálózat elérése a központi tűzfalon keresztül történhet.

Valamennyi hozzáférési pont esetében szabványos, ismert sérülékenységektől mentes kriptográfiai megoldással támogatott azonosítást és hitelesítést kell alkalmazni.

22.7. Mobil eszközök hozzáférése

A Hivatal elektronikus információs rendszereihez csak a jegyző engedélyével, a hitelesítés szabályait alkalmazva lehet hozzáférni. A biztonságos hozzáférést a rendszergazda biztosítja.

22.8. Külső elektronikus információs rendszerek használata

A Hivatal belső elektronikus információs rendszereinek külső hozzáférése során ismert sérülékenységektől mentes titkosítású VPN kapcsolatot kell alkalmazni, melynek során egyedileg kell azonosítani a felhasználót. A munka befejeztével bontani kell a VPN kapcsolatot.

A Hivatal belső elektronikus információs rendszereinek külső hozzáféréséhez csak olyan biztonságos infokommunikációs eszköz használható, amely megfelel a következő követelményeknek:

- Az eszközökön a felhasználóknak rendszergazdai jog nem adható.
- Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.
- Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.
- Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

A felhasználók képzésénél kiemelt figyelmet kell fordítani ezen eszközök biztonságos kezelésére.

A felhasználókat egyedileg kell azonosítani és a hálózati kapcsolatot szabványos kriptográfiai módszerrel titkosítani kell.

22.9. Információ megosztás, nyilvánosan elérhető tartalom

A Hivatal elektronikus információs rendszereiben kezelt adatok külső fél részére történő továbbítása előtt az érintett felhasználónak meg kell vizsgálnia, hogy a vonatkozó szerződés vagy jogszabály alapján az adat átadható-e. Különös figyelmet kell fordítani a jogszabály által védett adatok továbbítására.

Az információ megosztással kapcsolatos követelményeket az adott terület vezetőjének ismertetnie kell a felhasználókkal.

Az információk közzétételével kapcsolatban a Hivatal a jogszabályokat, a vonatkozó belső szabályzatát és az erkölcsi normákat követi.

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

- Jegyzői utasításban ki kell jelölni azokat a személyeket, akik jogosultak a Hivatal honlapján a Hivatal és annak működésével kapcsolatos bármely információ közzétételére.

- A kijelölt személyeket képzésben kell részesíteni annak biztosítása érdekében, hogy a nyilvánosan hozzáférhető információk ne tartalmazzanak nem nyilvános (pl.: személyes adatokat, üzleti titkokat) információkat.

- Gondoskodni kell arról, hogy közzététel előtt átvizsgálásra kerüljenek a publikálandó tartalmak.

- Időszakosan át kell vizsgálni a Hivatal honlapját a nem nyilvános információk tekintetében, és gondoskodni kell azok eltávolításáról.

23. A RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉG

23.1. Rendszer és információ sértetlenségre vonatkozó eljárásrend, hibajavítás

Az elektronikus információs rendszerek, illetve az adatok sértetlenségére vonatkozóan a következő eljárásrendet kell alkalmazni:

A rendszerprogramokkal kapcsolatos bármely konfigurálási, hangolási műveletet csak a rendszergazda végezhet. Az alkalmazáson végzendő, annak bármely funkcióját megváltoztató művelethez – beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - a jegyző engedélye szükséges.

A rendszergazdának biztosítania kell, hogy a rendszerszoftver naprakész állapotban legyen, és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az üzemeltetők számára.

Az alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni.

A felhasználói adatok és alkalmazások védelme érdekében a szoftverek módosítása (frissítés, verzióváltás) folyamán az alkalmazáshoz és az adatokhoz történő illetéktelen hozzáférést és az illetéktelen próbálkozást meg kell akadályozni. Gondoskodni kell arról, hogy a telepített alkalmazások, fájlok ne károsodjanak, és a követelményeknek megfelelően működjenek.

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

Gondoskodni kell arról, hogy a munkaállomásokon telepített operációs rendszerek és egyéb segédprogramok naprakészek legyenek.

A Microsoft termékek biztonsági frissítéseinek a telepítéséről a megjelenésüktől számított 1 héten belül gondoskodni kell. A biztonsági frissítéseket a rendszergazdának előzetesen tesztelni kell.

A nem Microsoft termékek frissítését a gyártói ajánlások figyelembe vételével kell elvégezni. A biztonsági frissítések telepítése a rendszergazda feladata.

23.2. Kártékony kódok elleni védelem

A Hivatalnak meg kell őriznie az elektronikus információs rendszerek és az információ bizalmasságát, sértetlenségét és rendelkezésre állását a kártékony kódok és a kéretlen üzenetek támadásaival szemben.

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

- Munkaállomások és kiszolgálók esetében memóriában rezidens kártékony kód elleni megoldásokat kell alkalmazni.

- Kártékony kód elleni megoldás nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem üzemeltethető.

- Egyéb infokommunikációs eszközök tekintetében a gyártói ajánlások és a lehetőségek figyelembe vételével törekedni kell a kártékony kódok elleni védekezésre.

- A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

- A kártékony kód elleni alkalmazásnak az email-ek csatolmányát ellenőriznie kell, a futtatható állományok szűrését be kell kapcsolni.

- A hordozható számítógépek esetében az üzemeltetőnek gondoskodnia kell a kártékony kód elleni alkalmazás adatbázisának automatikus frissítéséről, közvetlenül a hordozható számítógép bekapcsolása után.

- A külső forrásból származó a cserélhető adathordozókat használatba vétel előtt automatikus kártékony kód ellenőrzés alá kell vetni.

- A felhasználókat meg kell ismertetni a kártékony kód felmerülésének esetében követendő előírásokkal.

- A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell.

- Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani a hivatali hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.

- A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

23.3. Vírusriadó

A vírusriadót a Rendszergazda javaslatára a Jegyző rendelheti el.

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, és a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót

nem szükséges elrendelni. A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását. Ha ez nem sikerül, akkor vírusriadót kell elrendelni.

Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:

- ha a szokásosnál sokkal több vírusincidens történt;

- a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója;

- ugyanaz a vírus fordul elő egyszerre kettőnél több gépen, különböző állományokban;

- valamely számítógépen aktivizálódik a vírus romboló rutinja, vagy a vírus valamilyen effektust (videó, hang stb.) produkál annak ellenére, hogy a vírusadatbázis frissített, a víruskereső motor működött;

- adatátvitel során, egy számítógépen jelentkező szokványostól eltérő működés, átkerül más számítógépekre is;

- szerver oldali vírusfertőzés esetén.

A vírusriadó idején a vírus mentesítés szakmai felügyeletét a rendszergazda látja el.

23.4. Az elektronikus információs rendszer felügyelete

Az elektronikus információs rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén az eszközök javítását végzők bevonása.

Az elektronikus információs rendszerek felügyelete az alkalmazások, az adatbázisok, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

A fenti feladatok végrehajtása a rendszergazda feladata.

A rendszergazdának ismernie kell a Hivatal rendszereszközeinek, elektronikus információs rendszereinek működését és azok figyelmeztető és hibaüzeneteit. A szükséges reagálásokat tartalmazó leírást tudniuk kell alkalmazni.

A rendszergazdának rendszeresen el kell végeznie azokat a tevékenységeket, amelyek alapján meggyőződhet arról, hogy az elektronikus információs rendszer üzemszerűen működik.

Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolni kell, valamint az operációs rendszer beállításait rendszeresen menteni kell.

23.5. Biztonsági riasztások és tájékoztatások

A Hivatalnak folyamatosan figyelemmel kell kísérnie a Kormányzati Eseménykezelő Központ által kiadott riasztásokat, valamint a Nemzeti Elektronikus Információbiztonsági Hatóság által közzétett értesítéseket.

Az IBF-nek meg kell vizsgálnia, hogy az adott riasztás vagy értesítés érinti-e a Hivatalt, illetve annak elektronikus információs rendszereit és szükség esetén belső riasztást kell kiadnia az érintett szerepkörök részére.

23.6. Bemeneti információ ellenőrzés

Az önkormányzati ASP rendszer esetében meg kell határoznia a jegyzőnek, hogy mely Hivatali munkaállomásról jogosult a felhasználó elérni az önkormányzati ASP rendszert. A működtető által kiadott kliens oldali tanúsítvány telepítésével biztosítható a bemeneti információ belépési pontok érvényessége.

23.7. A kimeneti információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban a Hivatal Iratkezelési Szabályzatával összhangban a következők az előírások:

- gondoskodni kell a kimeneti információ tartalmi ellenőrzéséről,
- gondoskodni kell arról, hogy a kimeneti információhoz történő fizikai és logikai hozzáférés csak az arra jogosított személyekre korlátozódik,
- gondoskodni kell arról, hogy a jogosult személyek időben megkapják az elkészült kimeneti információkat,
- biztosítani kell, hogy a megsemmisítési eljárások során az kimeneti információk tartalma helyreállíthatatlanul megsemmisüljön.

24. NAPLÓZÁSI ELJÁRÁSREND

Naplózható események

- Az informatikai rendszerek naplózási rendszerének kialakítása (Windows naplófájlok, adatbázis 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.

- Az esetleges illetéktelen hozzáférést, jogosultságokkal való visszaéléseket - melyek szankciókat vonnak maguk után - jegyzőkönyvben rögzíteni kell.

- A visszaélés tényét a hivatal vezetője felé azonnal jelezni kell.

Időbélyegek

Az elektronikus információs rendszereknek a naplóbejegyzésekhez készített időbélyegeket a rendszer belső órái alapján kell elkészítenie.

A Hivatalnak szinkronizálnia kell a rendszer belső rendszer órákat a belső, illetve a külső időszolgáltatóval.

A napló információk védelme

Az elektronikus információs rendszereknek a jelen IBSZ-ben foglaltaknak megfelelően meg kell védenie a napló információkat és a napló eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

A naplóbejegyzések megőrzése

A biztonsági események utólagos kivizsgálása érdekében a naplóbejegyzéseket 1 évig meg kell őrizni.

25. RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELMI ELJÁRÁSREND

Az elektronikus információs rendszerek és a kommunikáció védelmére vonatkozóan a következő eljárásrendet kell alkalmazni.

A határok védelme

Mind a belső, mind a külső hálózati szolgáltatókhoz történő hozzáférést a következő módon kell ellenőrizni:

- Csak a szükséges adatfogalom engedélyezése.
- A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.
- Levelet továbbítani csak a levelező szerveren keresztül szabad.
- Megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között.
- A felhasználókat jelszóval megfelelően hitelesíteni kell.
- Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.
- A Hivatal belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.
- Biztosítani kell, hogy a Hivatal elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.
- A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználónak az Internet használata során tilos:

-a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele,

- az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni,

- fájlcserélő alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni,

- hivatali email címmel nyilvános levelezőlistákra, hírlevelekre feliratkozni.

- A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

A hálózati szolgáltatások belső használatának szabályozása

A Hivatal elektronikus információs rendszerében a felhasználók csak azokhoz a hálózati szolgáltatásokhoz férhetnek hozzá, amelyek használata a munkavégzésükhöz feltétlenül szükségesek.

A hálózatokkal és a hálózati szolgáltatásokkal kapcsolatosan az alábbiakat kell figyelembe venni:

- a felhasználókkal meg kell ismertetni azoknak a hálózatoknak és hálózati szolgáltatásoknak a felsorolását, amelyeket igénybe vehetnek;

- a hálózati kapcsolatokhoz és szolgáltatásokhoz való hozzáférés védelmére szolgáló óvintézkedések és eljárások tartalmazzanak bejelentkezési védelmet vagy más, az alkalmazások jogosításának ellenőrzésére szolgáló védelmet;

- a hálózati szolgáltatások használatával kapcsolatos szabályozást összhangban kell tartani a hozzáféréseket meghatározó követelményekkel.

- a Hivatal elektronikus információs rendszerében TILOS modemet csatlakoztatni.

- a Hivatal hálózatában csak olyan Wi-Fi hozzáférési pont létesíthető, amely minimum WPA2 titkosítást alkalmaz.

- A kiosztott kulcsok hossza minimum 8 karakter, tartalmazzon kisbetűt, nagybetűt, számot vagy speciális karaktert.

A felhasználó hitelesítése külső összeköttetésekhez

A felhasználókat jelszóval hitelesíteni kell és ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

Hálózat szegmentálás

A Hivatal hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell.

A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom szűrésére, a lehetőségek korlátozására tűzfalak, tartalomszűrők, illetve meghatározott címekkel a kapcsolat tiltását biztosító megoldások szolgáljanak.

A hálózati összeköttetések ellenőrzése

A hálózatok hozzáférését szabályozni, a felhasználók felkapcsolódási lehetőségeit korlátozni kell.

Az Internet és a Hivatal elektronikus információs rendszere közötti hálózati forgalom ellenőrzésére a tűzfalak naplói szolgáljanak.

Kriptográfiai védelem

A Hivatalnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére szabványos, a vonatkozó jogszabályokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

Kriptográfiai megoldások alkalmazásának feltételei

A Hivatal elektronikus információs rendszereiben csak olyan kriptográfiai megoldások alkalmazhatók, amelyek a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

V. Záró rendelkezések

A szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Jelen szabályzatban nem szabályozott adatvédelemre és adatbiztonságra vonatkozó előírásokat a Komlói Közös Önkormányzati Hivatal adatvédelmi és adatbiztonsági szabályzata tartalmazza.

Jelen szabályzat 2018. június 1. napján lép hatályba. Ezzel egyidejűleg a 2014. július 2. napján kelt Informatikai Biztonsági Szabályzat hatályát veszti.

Komló, 2018. 06. 01.

KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL JEGYZŐJE 1.

dr. Vaskó Ernő
címzetes főjegyző