



TÉTI KÖZÖS ÖNKORMÁNYZATI HIVATAL
2018/..... SZÁMÚ JEGYZŐI UTASÍTÁS

TÉTI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes:

Jóváhagyta:

Bereczkiné dr. Kovács Piroska

jegyző

Készítette az E-Szoftverfejlesztő Kft. a Hivatal megbízásából. A szabályzat **szerzői jogvédelem alatt áll**, bármely részének felhasználása - a Hivatal kivételével - csak a jogtulajdonos E-Szoftverfejlesztő Kft. írásbeli engedélyével lehetséges. A szerzői jog nem korlátozza a Hivatalt a szabályzat módosításában, publikálásában a szerzői jogra való hivatkozás megtartása mellett.



TARTALOMJEGYZÉK

1	ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	8
1.1	SZERVEZETI SZINTŰ ALAPFELADATOK	8
1.1.1	Az Informatikai Biztonsági Szabályzat	8
1.1.2	Felülvizsgálat	8
1.1.3	Hatásköri és illetékességi szabályok	8
1.1.4	Célok	9
1.1.5	Hatály	9
1.1.6	Hivatalrendszer belső együttműködése	10
1.1.7	Szerepkörök, tevékenységek, felelőségek	11
1.1.8	Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje	17
1.1.9	Az elektronikus információs rendszerek biztonságáért felelős személy	18
1.1.10	Az intézkedési terv és mérföldkövei	19
1.1.11	Az elektronikus információs rendszerek nyilvántartása	20
1.1.12	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	20
1.2	KOCKÁZATELEMZÉS	22
1.2.1	Kockázatelemzési és kockázatkezelési eljárásrend	22
1.2.2	Biztonsági osztályba sorolás	22
1.2.3	Kockázatelemzés	23
1.3	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	23
1.3.1	Beszerzési eljárásrend	23
1.3.2	Erőforrás igény felmérés	24
1.3.3	Beszerzések	24
1.3.4	A védelem szempontjainak érvényesítése a beszerzés során	25
1.3.5	Külső elektronikus információs rendszerek szolgáltatásai	25
1.4	ÜZLETMENET- ÜGYMENET- FOLYTONOSSÁG TERVEZÉSE	26
1.4.1	Ügymenet-folytonosságra vonatkozó eljárásrend	26
1.4.2	Ügymenet-folytonossági terv informatikai erőforrás kiesésekre	27
1.4.3	Kritikus rendszerelemek meghatározása	28
1.4.4	A folyamatos működésre felkészítő képzés	28
1.4.5	Üzletmenet-folytonosság elérhetőség	29
1.4.6	Infokommunikációs szolgáltatások	29
1.4.7	Szolgáltatás prioritási rendelkezések	29
1.4.8	Az elektronikus információs rendszer mentései	29
1.4.9	Az elektronikus információs rendszer helyreállítása és újraindítása	30

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 2 / 89



1.5	A BIZTONSÁGI ESEMÉNYEK KEZELÉSE	31
1.5.1	Biztonsági eseménykezelési eljárásrend	31
1.5.2	Biztonsági esemény kezelése	31
1.5.3	A biztonsági események figyelése	31
1.5.4	A biztonsági események jelentése.....	32
1.5.5	Segítségnyújtás a biztonsági események kezeléséhez.....	32
1.5.6	Biztonsági eseménykezelési terv.....	33
1.5.7	Képzés a biztonsági események kezelésére.....	34
1.6	EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	34
1.6.1	Személybiztonsági eljárásrend	34
1.6.2	Munkakörök, feladatok biztonsági szempontú besorolása.....	34
1.6.3	A személyek ellenőrzése	35
1.6.4	Eljárás a jogviszony megszűnésekor.....	36
1.6.5	Az áthelyezések, átirányítások és kirendelések kezelése	37
1.6.6	A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	37
1.6.7	Fegyelmi intézkedések	38
1.6.8	Belső egyeztetés	38
1.6.9	Viselkedési szabályok az interneten.....	38
1.7	TUDATOSSÁG ÉS KÉPZÉS.....	41
1.7.1	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel	41
1.7.2	Képzési eljárásrend	42
1.7.3	Biztonság tudatosság képzés, belső fenyegetés.....	42
1.7.4	Szerepkör, vagy feladat alapú biztonsági képzés	43
1.7.5	A biztonsági képzésre vonatkozó dokumentációk	44
2	FIZIKAI VÉDELMI INTÉZKEDÉSEK.....	45
2.1	FIZIKAI ÉS KÖRNYEZETI VÉDELEM	45
2.1.1	Fizikai védelmi eljárásrend	45
2.1.2	Fizikai belépési engedélyek.....	45
2.1.3	A fizikai belépés ellenőrzése.....	47
2.1.4	Hozzáférés az adatátviteli eszközökhöz és csatornákhöz.....	47
2.1.5	A kimeneti eszközök hozzáférés ellenőrzése	48
2.1.6	A fizikai hozzáférések felügyelete	48
2.1.7	Behatolás riasztás, felügyeleti berendezések	48
2.1.8	A látogatók ellenőrzése	48
2.1.9	Áramellátó berendezések és kábelezés.....	49

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 3 / 89



2.1.10	Tűzvédelem	49
2.1.11	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	49
2.1.12	Be- és kiszállítás.....	49
2.1.13	Az elektronikus információs rendszer elemeinek elhelyezése	50
2.1.14	Karbantartók.....	50
2.1.15	Időben történő javítás	51
3	LOGIKAI VÉDELMI INTÉZKEDÉSEK	52
3.1	ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	52
3.1.1	Engedélyezés	52
3.1.2	Az elektronikus információs rendszer kapcsolódásai	52
3.1.3	Belső rendszerkapcsolatok	52
3.1.4	Külső kapcsolódásokra vonatkozó korlátozások.....	52
3.1.5	Személybiztonság.....	53
3.2	TERVEZÉS.....	53
3.2.1	Biztonságtervezési szabályzat	53
3.2.2	Rendszerbiztonsági terv	53
3.2.3	Cselekvési terv	54
3.2.4	Személyi biztonság.....	55
3.3	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	56
3.3.1	A rendszer fejlesztési életciklusa	56
3.4	KONFIGURÁCIÓKEZELÉS.....	56
3.4.1	Konfigurációkezelési eljárásrend	56
3.4.2	Alap konfiguráció.....	57
3.4.3	Legszűkebb funkcionalitás	57
3.4.4	Elektronikus információs rendszerelem leltár.....	57
3.4.5	Duplikálás elleni védelem	58
3.4.6	A szoftver használat korlátozásai	58
3.4.7	A felhasználó által telepített szoftverek	59
3.5	KARBANTARTÁS.....	60
3.5.1	Rendszer karbantartási eljárásrend.....	60
3.5.2	Rendszeres karbantartás	60
3.5.3	Adathordozó ellenőrzés	61
3.5.4	Távoli karbantartás	61
3.6	ADATHORDOZÓK VÉDELME	62
3.6.1	Adathordozók védelmére vonatkozó eljárásrend	62
3.6.2	Hozzáférés az adathordozókhoz.....	62
3.6.3	Adathordozók tárolása.....	63

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 4 / 89



3.6.4	Adathordozók szállítása	63
3.6.5	Kriptográfiai védelem	63
3.6.6	Adathordozók törlése	64
3.6.7	Adathordozók használata	64
3.6.8	Ismeretlen tulajdonos	64
3.7	AZONOSÍTÁS ÉS HITELESÍTÉS	65
3.7.1	Azonosítási és hitelesítési eljárásrend	65
3.7.2	Azonosítás és hitelesítés (Hivatalon belüli felhasználók)	65
3.7.3	Azonosító kezelés.....	65
3.7.4	A hitelesítésre szolgáló eszközök kezelése	66
3.7.5	Jelszó (tudás) alapú hitelesítés	66
3.7.6	Birtoklás alapú hitelesítés.....	67
3.7.7	Személyes vagy megbízható harmadik fél általi regisztráció	67
3.7.8	A hitelesítésre szolgáló eszköz visszacsatolása	67
3.7.9	Azonosítás és hitelesítés (hivatalon kívüli felhasználók).....	68
3.7.10	Hitelesítésszolgáltatók tanúsítványának elfogadása.....	68
3.8	HOZZÁFÉRÉS ELLENŐRZÉS.....	68
3.8.1	Hozzáférés ellenőrzési eljárásrend	68
3.8.2	Felhasználói fiókok kezelése.....	69
3.8.3	Hozzáférés ellenőrzés érvényesítése	70
3.8.4	A felelősségek szétválasztása.....	70
3.8.5	Legkisebb jogosultság elve	70
3.8.6	Jogosult hozzáférés a biztonsági funkciókhoz	71
3.8.7	Nem privilegizált hozzáférés a biztonsági funkciókhoz.....	71
3.8.8	Privilegizált fiókok.....	71
3.8.9	A munkaszakasz zárolása.....	71
3.8.10	Képernyőtakarás.....	72
3.8.11	A munkaszakasz lezárása	72
3.8.12	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek.....	72
3.8.13	Vezeték nélküli hozzáférés.....	72
3.8.14	Mobil eszközök hozzáférés ellenőrzése	72
3.8.15	Titkosítás	72
3.8.16	Külső elektronikus információs rendszerek használata	72
3.8.17	Korlátozott használat.....	73
3.8.18	Hordozható adattároló eszközök	73
3.8.19	Információ megosztás	73
3.8.20	Nyilvánosan elérhető tartalom	73

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 5 / 89



3.9	RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG	74
3.9.1	Rendszer- és információsértetlenségre vonatkozó eljárásrend.....	74
3.9.2	Hibajavítás.....	74
3.9.3	Kártékony kódok elleni védelem.....	75
3.9.4	Automatikus frissítés.....	76
3.9.5	Az elektronikus információs rendszer felügyelete	76
3.9.6	Biztonsági riasztások és tájékoztatások.....	76
3.9.7	Bemeneti információ ellenőrzés	77
3.9.8	A kimeneti információ kezelése és megőrzése	77
3.10	NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	77
3.10.1	Naplózási eljárásrend	77
3.10.2	Naplózható események.....	77
3.10.3	Naplóbejegyzések tartalma	78
3.10.4	Időbélyegek	78
3.10.5	A naplóinformációk védelme	78
3.10.6	A naplóbejegyzések megőrzése.....	78
3.10.7	Naplógenerálás	78
3.11	RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM	80
3.11.1	Rendszer- és kommunikáció védelmi eljárásrend.....	80
3.11.2	A határok védelme	81
3.11.3	Kriptográfiai kulcs előállítása és kezelése.....	81
3.11.4	Kriptográfiai védelem	81
3.11.5	Együttműködésen alapuló számítástechnikai eszközök.....	81
3.11.6	Elektronikus információs rendszeren keresztüli hangátvitel (ún. VoIP).....	81
3.11.7	A folyamatok elkülönítése	82
4	KAPCSOLÓDÓ MELLÉKLETEK	83
5	ALAPFOGALMAK	84

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 6 / 89



Verzió	Készült/módosult	Változás oka	Jóváhagyta	Hatálybalépés dátuma
1.0	2018.01.02.	Első verzió		



1 ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

1.1 SZERVEZETI SZINTŰ ALAPFELADATOK

1.1.1 Az Informatikai Biztonsági Szabályzat

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (Ibtv.) foglalt követelmények alapján a Téti Közös Önkormányzati Hivatal (továbbiakban: Hivatal) Informatikai Biztonsági Szabályzatában az alábbiakat határozza meg:

- a) meghatározza a célokat, a szabályzat tárgyi, személyi, területi és időbeni hatályát,
- b) az elektronikus információbiztonsággal kapcsolatos szerepköröket,
- c) a szerepkörhöz rendelt tevékenységet,
- d) a tevékenységhez kapcsolódó felelősséget,
- e) az információbiztonság hivatalrendszerének belső együttműködését,
- f) az elektronikus rendszerbiztonsággal kapcsolatos főbb területeket.

A szabályzatnak összhangban kell lenni a hatályos jogszabályokkal, köztük az alábbiakkal:

- a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel,
- b) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelettel,
- c) az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelettel.

1.1.2 Felülvizsgálat

A Hivatal az Informatikai Biztonsági Szabályzatot és hivatkozott eljárásrendjeit folyamatosan fejleszti és aktualizálja. A szabályzatot évente legalább egy alkalommal felül kell vizsgálni. A megfelelőségi vizsgálat kiterjed a szabályzat végrehajtásának, valamint a felmerülő informatikai, információbiztonsági és adatvédelmi eseményeknek és az ezekkel összefüggő biztonsági tevékenységeknek az ellenőrzésére.

A szabályzatot módosítani kell, ha a benne szereplő adatok megváltoztak, ha a Hivatal elektronikus információs rendszereinek működésében vagy a Hivatal elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben változások következnek be. Módosítani kell továbbá az elavult informatikai technológiai megoldások kivezetése, és az új technológiai újítások bevezetése során, új elektronikus információs rendszerek bevezetése és kivezetése alkalmával.

A szabályzat felülvizsgálatának, módosításának kezdeményezése és elvégzése az elektronikus információs rendszer biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Hivatal vezetőjének hatásköre.

1.1.3

1.1.4 Hatásköri és illetékességi szabályok

Az Informatikai Biztonsági Szabályzat a Hivatalon belüli nyilvános dokumentum, míg a hozzá kapcsolódó eljárások, tervek, módszertanok, nyilvántartások stb, a Hivatal bizalmas

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 8 / 89



dokumentumai, amelyeket a Hivatal elektronikus információs rendszerének felhasználói (a szabályzat személyi hatálya alá tartozók) a rájuk vonatkozó követelmény szerint megismerhetnek, de azokat illetékteleneknek nem adhatják tovább.

1.1.5 Célok

Az Informatikai Biztonsági Szabályzat célja (továbbiakban: IBSZ), hogy a Hivatal számára értéket képviselő információk védelméről történő gondoskodást szabályozza. Az információ védelmének a célja, hogy biztosítsa az információ;

- a) rendelkezésre állását (ahol, és amikor kell, az információ elérhető legyen),
- b) sértetlenségét (az információ legyen hiteles és autentikus),
- c) bizalmasságát (csak az arra jogosultak jussanak hozzá az információhoz).

A szabályzat meghatározza az információk védelméhez szükséges felelőségeket, feladatokat, folyamatokat és eljárásokat, valamint az általánosan betartandó informatikai üzemeltetési, információkezelési és viselkedési szabályokat.

Az IBSZ-ben szereplő követelményeket, rendelkezéseket és ajánlásokat a hatályos jogszabályok keretei között kell használni. A biztonsági szabályozás célja a következő:

- a) a jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit,
- b) a tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot,
- c) a megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

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 felelőséget, amelyekre a biztonságos információellátás érdekében szükség van. Megfogalmazza azokat a biztonsági követelményeket, amelyeket az önkormányzati ASP-hez való csatlakozással teljesíteni szükséges.

A Hivatal informatikai szolgáltatóival kötött szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

1.1.6 Hatály

Az IBSZ a Hivatal egészére vonatkozik. **A szabályzat tárgyi hatálya** kiterjed a Hivatal birtokában levő összes olyan eszközre (például: hardver, szoftver és hálózati elemek, dokumentációk), amelyek az alaprendeltetésből adódó, a Hivatal ügyviteli tevékenységével kapcsolatos feladatok ellátását biztosítják. A tárgyi hatály alá esnek mindazon eszközök is, amelyek harmadik személyek birtokában vannak ugyan, de a fenti tevékenységek ellátását biztosítják. E tárgyi hatályt a Hivatal szolgáltatói, vállalkozási vagy megbízási szerződések keretében érvényesítik. A szabályzat rendelkezik a Hivatal tevékenysége során feldolgozott, vagy azzal kapcsolatban keletkezett információk védelméről is, azok sértetlenségének, hitelességének és rendelkezésre állásának biztosításáról.

A tárgyi hatály kiterjed továbbá a központi szolgáltató rendszereinek használatához szükséges felhasználói munkaadásokra, szoftverekre, nyomatkészítő eszközökre,

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 9 / 89



kártyaolvasóra, E-személyire és minden olyan egyéb eszközre, amely a munkavégzéshez szükséges.

A szabályzat személyi hatálya kiterjed a Hivatal minden munkatársára, a Hivatal informatikai rendszeréhez hozzáféréssel rendelkező felhasználóra, szerződéses partnerére. Harmadik személyekkel szemben a Hivatal a személyi hatályt szolgáltatói, vállalkozási vagy megbízási szerződések keretében érvényesíti.

A szabályzat területi hatálya kiterjed a Téti Közös Önkormányzati Hivatalra, valamint a Téti Közös Önkormányzati Hivatal Rábaszentmihály és Rábacsécsény kirendeltségekre. Kiterjed továbbá a Hivatal informatikai erőforrásainak üzemelési helyszíneire, a külső szolgáltatók által a Hivatalnak nyújtott szolgáltatásban érintett helyszíneire.

Időbeni hatály: jelen IBSZ a kiadás napján lép hatályba, mellyel a korábbi Informatikai Biztonsági Szabályzat hatályát veszti.

Új elektronikus információs rendszer bevezetése (ASP) vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

1.1.7 Hivatalrendszer belső együttműködése

A Hivatal szervezeti szintű felépítését a *Szervezeti és Működési Szabályzatban* (SzMSz) rögzíti.

Az elektronikus információs rendszer biztonsága érdekében történő, a Hivatalon belüli együttműködés jelen szabályzat tételes előírásain túl az érintett személyek önkéntes, szabálykövető magatartásán és biztonságtudatos, proaktív viselkedésén is alapul.

Az egyes kontrollfolyamatokban kötelező együttműködési szabályokat az eljárásrendek vonatkozó előírásai részletezik. Általában minden érintett személy köteles:

- jelen szabályzat és kapcsolódó dokumentumok előírásait megismerni és magára nézve, nyilatkozat keretében kötelezőnek elismerni,
- az információbiztonsági tárgyú belső képzéseken részt venni,
- személyét érintő biztonsági ellenőrzéseket, auditokat tűrni, azokban az ellenőrző személyek kérése szerint részt venni,
- az általa biztonsági eseményként vélelmezett történéseket a felettes vezetőnek és/vagy a rendszergazda felé jelenteni.

Az IBSZ (és kapcsolódó dokumentumai) előírásainak betartása, betartatása, illetve a napi szintű munkavégzés során annak alkalmazása a dokumentum 1.1.5 *személyi hatálya* pontban megjelöltek számára kötelező.

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

A Hivatal vezetője közvetlenül felelős azért, hogy az ellenőrzése alá tartozó felhasználók betartsák az IBSZ előírásait.

A Hivatali munkavégzéshez szükséges elektronikus információs rendszereket csak a jelen IBSZ mellékletében található nyilatkozatok, illetve az önkormányzati ASP rendszer elemeit a szolgáltatási szerződéshez mellékelt titoktartási nyilatkozat aláírása után lehet használatba venni.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 10 / 89



1.1.8 Szerepkörök, tevékenységek, felelősségek

Az információbiztonság megvalósítása, fenntartása, fejlesztése és ellenőrzése érdekében a Hivatal a feladatok és felelősségek tekintetében az alábbi szerepköröket azonosítja:

Szerepkör	Főbb felelősségek, tevékenységek
elektronikus információs rendszerek védelméért felelős vezető (a Hivatal vezetője)	1. biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését, 2. biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését, 3. az elektronikus információs rendszer biztonságáért felelős személyt (információbiztonsági felelős, IBF) nevez ki vagy bíz meg, 4. meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot, 5. gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról, 6. rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak, 7. gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről, 8. 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, 9. ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 10. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 11. felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért, 12. megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket,



Szerepkör	Főbb felelősségek, tevékenységek
	13. a feladatokért a szervezet vezetője a 9. és 10. pontjában meghatározott esetben is felelős, kivéve azokat az esetköröket, amikor jogszabály által kijelölt központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni, 14. a jogszabály által kijelölt központi adatkezelő és adatfeldolgozó szolgáltató igénybevétele esetén a feltételek teljesítését a jogszabály által kijelölt központi adatkezelő és adatfeldolgozó szolgáltató úgy biztosítja, hogy közreműködik a szervezet és az elektronikus információs rendszer biztonságáért felelős személy (információbiztonsági felelős, IBF) feladatai ellátásában a jogkörébe tartozó tevékenységek tekintetében, a két szervezet közötti feladatmegosztást kétoldalú szolgáltatási szerződések biztosítják, amelyek a központi szolgáltató felett felügyeletet gyakorló miniszter vagy megbízottja ellenjegyzésével lépnek hatályba, 15. együttműködik a Hatósággal a Hatóság feladatainak elvégzésében, ennek során az Ibtv. 12. § alapján: a) az elektronikus információs rendszer biztonságáért felelős (információbiztonsági felelős, IBF) személyről tájékoztatást nyújt, b) a szervezet Informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a Hatóság részére.
elektronikus információs rendszer biztonságáért felelős személy (információbiztonsági felelős, IBF)	1. az IBF feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést, 2. az IBF felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, 3. gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, 4. elvégzi vagy irányítja a 3. pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését, 5. előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, eljárásrendeket, terveket, 6. előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását, 7. véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit, 8. kapcsolatot tart a Hatósággal és a Kormányzati Eseménykezelő Központtal,



Szerepkör	Főbb felelősségek, tevékenységek
	9. az IBF a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet, 10. az IBF biztosítja a törvényben meghatározott követelmények teljesülését; a) a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők, b) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők a törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén. 11. az IBF a törvény szerinti feladatai és felelőssége a 10. pont szerinti esetekben más személyre nem átruházható, 12. az IBF jogosult az 10. pont szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelés alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.
megbízott szervezeti egység vezető (osztály/irodavezetők)	1. együttműködik az információbiztonsági felelőssel az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárások, szabályok, felelősségek, kötelező vagy tiltott tevékenységek, viselkedési szabályok meghatározásában. 2. gondoskodik arról, hogy a felelőssége alá tartozó szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági követelményeket, szabályokat, 3. közreműködik az IBF által tartott előző pontban megjelölt követelmények teljesülésének ellenőrzése során, 4. saját és a felelőssége alá tartozó munkatársak információbiztonsági, informatikai fennakadásról tett észrevételeit jelenti a rendszergazdának.
adatgazda (megbízott szervezeti egység vezető)	1. meghatározza a hatókörébe tartozó elektronikus információs rendszerekhez, adatokhoz, tevékenységekhez hozzáférők körét, 2. engedélyezi a szükséges jogosultságokat a hatáskörébe tartozó elektronikus információs rendszerek, adatok, tevékenységek tekintetében (nyilatkoztatást követően), 3. tájékoztatja a rendszergazdát a felhasználói jogosultság



Szerepkör	Főbb felelősségek, tevékenységek
	visszavonásáról 4. közreműködik az információbiztonsági kockázatok elemzésében.
rendszergazda (külsős megbízott vállalkozó)	1. felelős az elektronikus információs rendszerek felügyeletéért, az alkalmazások, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások működésének folyamatos figyelemmel kíséréseért, az üzemeltetéshez szükséges dokumentációk kidolgozásáért, a törvényi előírásoknak megfelelő nyilvántartások vezetéséért és naprakészen tartásáért. Ennek értelmében: 2. elvégzi és felügyeli az informatikai hálózat, számítógépek, eszközök biztonsági beállításait (pl. operációs rendszer, router beállítások), 3. telepíti és felügyeli a Hivatal munkájához szükséges szoftvereket az IBSZ-ben megfogalmazott elveknek megfelelően, 4. biztosítja a rendszerfelügyeletet, a felhasználói fiókok felügyeletét, 5. felügyeli a fizikai belépést ellenőrző eszközöket, 6. az információbiztonsági felelőssel és az adatgazdákkal együttműködve kialakítja és működteti az adatokhoz, rendszerekhez való hozzáférési jogok rendszerét, 7. közreműködik az információbiztonsági felelőssel és az adatgazdákkal az információbiztonsági kockázatok elemzésében, 8. elvégzik a logok elemzését és jelentést készít róla az IBF felé, 9. információbiztonsági incidens észlelése esetén haladéktalanul jelentést tesz az IBF-nek, a biztonsági esemény elhárítását megkezdi, az eredményéről tájékoztatást nyújt az érintetteknek, 10. saját hatókörében rendszeres fizikai és logikai karbantartásokat végez és dokumentál (karbantartásnapló), 11. az információbiztonsági felelőssel közreműködve, meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket, 12. ellenőrzi az időszakos mentéseket, szükség szerinti helyreállításokat, visszaállítási teszteket és jegyzőkönyvezi azokat, 13. hiba esetén elvégzi vagy felügyeli az eszközök javítását (a szerződésnek/a jegyző utasításának megfelelően vagy vele egyeztetve), 14. közreműködik az információbiztonsági felelőssel a BCP/DRP tervek kidolgozásában, 15. kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat, 16. az információbiztonsági felelőssel egyeztetve vezeti az

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 14 / 89



Szerepkör	Főbb felelősségek, tevékenységek
	IBSZ-ben előírt nyilvántartásokat, mint például; a) hardver/ szoftver nyilvántartás, b) alapkonzfiguráció nyilvántartása, c) informatikai szolgáltatást nyújtó szerződött partnerek listája, d) jogosultságok nyilvántartása (eszközökhöz, rendszerekhez, felhasználói fiókok), e) belépésre jogosultak listája (irodákba, Hivatali helyiségekbe), f) nyilvántartja a fizikai belépést ellenőrző eszközöket, g) jogosultságigények nyilvántartása, h) hordozható eszközök listája, kiadott eszközök nyilvántartása, i) karbantartások naplózása, karbantartást végzők listája, j) szerverterembe történő belépés logolása, k) minden egyéb olyan nyilvántartás, amelyet a Hivatal információbiztonsági felelőse a hatáskörében előír.
felhasználók (az elektronikus információs rendszert igénybe vevők köre, a szabályzat személyi hatálya alá tartozók)	1. kötelesek az információbiztonsági szabályzatban rájuk vonatkozó szabályokat megismerni, elolvasni, 2. betartják, végrehajtják az elektronikus információbiztonsági szabályokat, utasításokat, magatartásukkal segítik a hatékony és biztonságos informatikai biztonság megteremtését, 3. együttműködnek a Hivatalt érintő információbiztonsági kérdéskörökben felettesükkel és az információbiztonsági felelőssel, 4. haladéktalanul jelentik felettesüknek vagy a rendszergazdának, ha az informatikai rendszerben fennakadást, leállást, zavart észlelnek, vagy, ha jogosulatlanul férnek hozzá adatokhoz, rendszerekhez, illetve, ha információbiztonsági eseményt/incidenst észlelnek, 5. információbiztonsági incidens esetén együtt kell működniük a kivizsgálásban, ha az személyüket érinti, vagy felettesük erre felkéri őket, 6. a felhasználóknak bizalmasan kell kezelniük felhasználói azonosítóikat, jelszavaikat, védett zónákba belépést biztosító kártyáikat, kódjaikat, 7. kötelesek részt venni a Hivatalon belül szervezett információbiztonsági oktatásokon, illetve a jegyző utasítása szerint más külső oktatásokon, 8. a birtokukban lévő, vagy tudomásukra jutott információkat bizalmasan kezelik, 9. felelősséggel tartoznak a munkavégzésük során az elektronikus információs rendszerben végzett feladatokért, a szakrendszerek szakszerű használatáért, 10. felelősséggel tartoznak a munkavégzésükhöz szükséges Hivatalból kiadott eszközök megfelelő fizikai, logikai



Szerepkör	Főbb felelősségek, tevékenységek
	védelméért, 11. az ASP központ működtetője által kiadott felhasználói biztonsági követelményeket kötelesek a felhasználók követni és betartani, 12. megtagadhatják az utasítást, ha annak végrehajtása jogszabályba, az informatikai biztonsággal kapcsolatos kiadott utasításba, szabályzatba ütközik, vagy megítélésük szerint veszélyeztetné az informatikai biztonságot, 13. a felhasználó köteles az utasítást adó figyelmét felhívni és egyben kérheti az utasítás írásba foglalását, ha az, vagy annak végrehajtása jogszabályba vagy a kiadott informatikai biztonsággal kapcsolatos utasításba ütközne, vagy teljesítése kárt idézhet elő, és a felhasználó a következményekkel számolhat, vagy az utasítás az érintettek jogos érdekeit sérti. Az utasítást adó felettes az utasítás írásba foglalását nem tagadhatja meg.
weblap fejlesztő, üzemeltető, tartalom felelős	weblap fejlesztő 1. mindenkori OWASP top 10-es sérülékenységek ellenőrzése, és nyilvánosságra hozott hibák kijavítása weblap motor / telepített modulok folyamatos ellenőrzése, frissítése. üzemeltető 1. védekezés külső (belső) támadás ellen, 2. használt szolgáltatások folyamatos frissítése karbantartása, 3. lehetőség szerint a szolgáltatások verziószámainak elrejtése. tartalom felelős 1. jogszabályi követelményeknek megfelelően a tartalom feltöltési és karbantartási feladatok ellátásáért a Hivatal által kijelölt munkatárs felelős, 2. a Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatokat közöl, a települést mutatja be, aktuális híreket és információkat közöl az állampolgárok számára, 3. a weboldalra szánt tartalmat előzetesen jóvá kell hagynia a Hivatal vezetőjének.
ASP adminisztrátor (tenant adminisztrátor)	1. az önkormányzati ASP adminisztrátor feladata a bérlő fiók, tenant (önkormányzat, intézmény, nemzetiségi önkormányzat) szintű felhasználó kezelés, azaz: a) az adott tenant felhasználóinak felvétele és szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása, b) intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele



Szerepkör	Főbb felelősségek, tevékenységek
	és felhasználók közötti kiosztása.
önkormányzat szakrendszerei adminisztrátor(ok)	1. feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszerei jogosultságok beállítása, adminisztrációja és karbantartása.

Az információbiztonsággal kapcsolatos felelősségeket, tevékenységeket a munkaköri leírásokkal összhangba kell hozni.

1.1.9 Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje

1. Biztonsági osztályba sorolás

A Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (1) bekezdésében foglaltak alapján, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 1. és 2. számú melléklete szerint biztonsági osztályba kell, hogy sorolja elektronikus információs rendszereit, illetve meg kell állapítania a Hivatal biztonsági szintjét.

Az információbiztonsági felelős feladata, hogy a Hivatal rendszereinek biztonsági osztályba sorolását az adatgazdákkal együttműködve elvégezze, a Hivatal biztonsági szintjét megállapítsa, osztályba és szintbe sorolás mellékletben, rendszerbiztonsági tervben vagy magában az IBSZ-ben rögzítse. Szükség esetén jelen IBSZ-t aktualizálja, a hatósági adatszolgáltatást előkészíti és a jegyző számára előterjeszti.

A biztonsági osztályba és szintbe sorolás eredményét új elektronikus információs rendszer be- és kivezetésekor, vagy az azzal összefüggő adatkezelési célok jelentős változása esetén, az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változásakor, de legalább 3 évente felül kell vizsgálni.

A Hivatalnak az elektronikus információs rendszerek osztályba sorolás eredményét a *NEIH-OVI Osztályba sorolás és védelmi intézkedés űrlap* (illetve XML állomány) kitöltésével a Nemzeti Elektronikus Információbiztonsági Hatóság részére meg kell küldenie.

Azokban az esetekben, amikor a Hivatal külső szolgáltatót, illetve jogszabály alapján kijelölt szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről a Hivatal tájékoztatást kell, hogy kérjen.

A Hivatalnak figyelembe kell vennie a külső szolgáltató, illetve jogszabály alapján kijelölt szolgáltató által meghatározott biztonsági osztály értékét, és a szolgáltatóval történő megállapodás (szerződés) értelmében, a reá vonatkozó biztonsági követelményeket kell teljesítenie. A Hatóság részére így, a *NEIH-OVI Osztályba sorolás és védelmi intézkedés űrlapot* annak megfelelően kell kitöltenie a Hivatalnak, ami a szolgáltatóval kötött megállapodás alapján rá nézve teljesítendő.

Osztályba sorolás eredménye: *Elektronikus információs rendszerek biztonsági osztálya – a Hivatal biztonsági szintje* 1. számú melléklet tartalmazza.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 17 / 89



2. Biztonsági szintbe sorolás

A 2013. évi L. törvény 9. § (4) bekezdésében foglaltak alapján a Hivatal biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint (41/2015. [VII. 15.] BM rendelet 2. melléklet).

A szintbe sorolás eredményét a *NEIH-SZVI Szintbe sorolás és védelmi intézkedés űrlap* (illetve XML állomány) kitöltésével a Hatóság részére szintén meg kell küldenie.

Szintbe sorolás eredménye: *Elektronikus információs rendszerek biztonsági osztálya – a Hivatal biztonsági szintje* 1. számú melléklet tartalmazza.

A besorolás alapján a 41/2015. (VII. 15.) BM rendeletben az elektronikus információs rendszerre érvényes biztonsági osztályhoz és a Hivatalra érvényes biztonsági szinthez rendelt követelményeket és azok megvalósításának módját a következő fejezet tartalmazza (adminisztratív, fizikai és logikai védelmi intézkedések). A dokumentum struktúrája a hatósági elvárásnak megfelelően leköveti a 41/2015 BM rendelet felépítését.

Külső szolgáltató, illetve jogszabály alapján kijelölt szolgáltató esetében az elektronikus információs rendszer nem tartozik a Hivatal saját hatókörébe, így az azzal kapcsolatos biztonsági követelmények megszlanak a Hivatal és a szolgáltató/üzemeltető között.

1.1.10 Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője a törvényi előírásnak megfelelően elektronikus információs rendszerek biztonságáért felelős személyt (információbiztonsági felelős, IBF) nevez ki vagy bíz meg, aki ellátja az állami és Hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat (Ibtv. 13. §).

A Hivatalnál csak olyan személy végezheti az információbiztonsági felelős feladatait, aki;

1. büntetlen előéletű

A büntetlen előélet követelményének való megfelelést az információbiztonsági felelős a Hivatallal fennálló jogviszonya keletkezését megelőzően köteles igazolni. A Hivatal az információbiztonsági felelőst kötelezheti, hogy a Hivatallal fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

2. rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel

Nemzeti Közzolgálati Egyetem elfogadható képesítése:

a) Elektronikus információbiztonsági vezető

Nem kell a fentebb jelölt képzettséget megszereznie annak a személynek, aki rendelkezik a külön jogszabályban meghatározott, akkreditált nemzetközi képzettséggel, vagy e szakterületen szerzett 5 év szakmai gyakorlattal, amelyet igazolni is tud.

ISACA elfogadható képesítései (külön jogszabályban meghatározott akkreditált nemzetközi képesítés):

- a) Certified Information Systems Auditor (CISA),
- b) Certified Information Security Manager (CISM),
- c) Certified in Risk and Information Systems Control (CRISC).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 18 / 89



(ISC)2 elfogadható képesítése:

- a) Certified Information Systems Security Professional (CISSP).

Releváns szakterületnek minősül (5 év szakmai gyakorlat, igazolni szükséges):

- a) információbiztonsági irányítási rendszer tervezése, kialakítása, működtetése,
- b) információbiztonsági ellenőrzés vagy felügyelet,
- c) információbiztonsági kockázatelemzés,
- d) információbiztonsági tanúsítás,
- e) információbiztonsági tesztelés (etikus hacker tevékenység).

Az információbiztonsági felelős és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt, az *Elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet* alapján.

A Hivatal vezetője a Hatóság (NEIH) számára, az Ibtv. 11. § (1) bekezdés c) pontjában meghatározott, információbiztonsági felelősről tájékoztatást nyújt.

1.1.11 Az intézkedési terv és mérőföldkövei

Az információbiztonsági felelős intézkedési tervet (cselekvési tervet) készít, amennyiben a meghatározott biztonsági osztálynál/szintnél hiányosságot állapít meg (tehát, ha valamely védelmi intézkedés nem valósul meg, vagy a bevezetett kontroll hibás/hiányos) és ezekhez mérőföldkövet rendel.

A feltárt hiányosságokat kockázatelemzést követően a kockázatokra adott válasz tevékenységek prioritása alapján teszi sorrendbe (jellemzően a nagy kockázattal járó hiányosságokat helyezi előtérbe).

Az intézkedési tervet (cselekvési tervet) a hiányosságok megállapítását követően kell elkészíteni:

- a. a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján,
- b. az elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál megállapított hiányosságot, a vizsgálatot követő 90 napon belül kell felülvizsgálni, a hiányosság(ok) megszüntetése érdekében,
- c. ha a meghatározott biztonsági szint alacsonyabb, mint a Hivatalra érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

Az intézkedési tervet (cselekvési tervet) folyamatosan aktualizálni kell.

Az intézkedési terv (cselekvési terv) legalább az alábbi pontokat tartalmazza:

- a. megvalósulatlan védelmi intézkedés (meghatározott biztonsági osztályhoz tartozó OVI-úrlapból a „nem valósult meg” sorok), bevezetett hibás/hiányos kontrollok, elektronikus információs rendszer ismert sérülékenységei, a kockázatelemzés eredményének sorrendjében,
- b. tervezett intézkedés,
- c. felelős,
- d. tervezett határidő,
- e. megvalósítás dátuma,
- f. intézkedés eredménye (teljesült/nem teljesült),

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 19 / 89



- g. ellenőrző személy megnevezése.

Mivel az intézkedési terv (cselekvési terv) bizalmas információkat tartalmaz, ezért ezt csak a jegyző, az információbiztonsági felelős, és az információbiztonsági felelős által kijelölt személyek ismerhetik meg.

1.1.12 Az elektronikus információs rendszerek nyilvántartása

Az információbiztonsági felelős az elektronikus információs rendszerekről nyilvántartást vezet, azt szükség szerint aktualizálja.

A nyilvántartás tartalmazza:

- a) az információs rendszer alapfeladatait,
- b) a rendszerek által biztosítandó szolgáltatásokat,
- c) az érintett rendszerekhez tartozó licenc számot (amennyiben azok a Hivatal kezelésében vannak),
- d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait,
- e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

Az elektronikus információs rendszerek nyilvántartását egy korlátozottan, csak az érintetteknek hozzáférhető belső dokumentumban, vagy elektronikus nyilvántartásban kell kezelni.

1.1.13 Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatókörébe tartozó:

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

1. A fizikai és logikai jogosultságok engedélyezése az alábbiakat foglalja magába:

- melyek a jogosultsággal rendelkező személyek felelősségei, velük szembeni szabályok, követelmények,
- hogyan történik az elektronikus információs rendszerhez való hozzáférés engedélyezése, jogosultság adás,
- melyek a rendszer jogosultsági szintjei (biztonsági zónák védelme, minimum jogosultság, privilegizált, stb), mit tartalmaznak az egyes jogosultsági szintek,
- melyek a legkisebb jogosultság elve alapján, a jogosultsági körök,
- kik az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek és milyen jogosultságaik vannak, kik rendelkeznek/rendelkezhetnek privilegizált jogosultsággal,
- melyek azok a tevékenységek, amelyek az elektronikus információs rendszer használata során engedélyezettek, illetve tiltottak,
- hogyan történik a jogosultsággal rendelkező személyek nyilatkoztatása (biztonsági szabályok és kötelezettségek megismerése),
- hogyan történik a jogosultság visszavonás.

Ezek az engedélyezések a *Fizikai védelmi intézkedések* és *Logikai védelmi intézkedések* fejezet alatt kerülnek részletezésre.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 20 / 89



Ha a kockázatkezelés keretében, vezetői feladatszabás következtében vagy egyéb igény nyomán az információbiztonsággal kapcsolatos folyamatok, eljárások és dokumentumok változtatása válik szükségessé, a módosítást kezdeményező személy a javaslatot az információbiztonsági felelős elé terjeszti, aki – a javaslatok mérlegelése és elfogadása után – átvezeti a módosításokat a dokumentumokon. Beszerzést, belső erőforrások átcsoportosítását igénylő, biztonsági osztályba és szintbe sorolás változását jelentő módosítások jóváhagyása a jegyző jogköre, ilyen esetekben az információbiztonsági felelős az előterjesztő.

Az egyes dokumentumok változásának követése céljából valamennyi irat elején fel kell tüntetni a változásokat nyilvántartó táblázatot a következő adattartalommal:

- a. verzió,
- b. készült (dátum),
- c. változás oka,
- d. jóváhagyta,
- e. hatálybalépés dátuma.

A táblázatban a szöveg valamennyi változását fel kell jegyezni.

2. Hatósági engedélyezés szükséges az alábbi esetekben:

- a) amennyiben a Hivatal az elektronikus információs rendszerre a jogszabályi alapértelmezettnél alacsonyabb biztonsági osztályt kíván megállapítani, a Hatóság felé írásbeli kérelmet kell benyújtania.

A kérelemhez csatolni kell:

- az eltérő biztonsági osztályba sorolás alapjául szolgáló kockázatelemzés dokumentációját,
- a kérelem tárgyát képező elektronikus információs rendszerről szóló NEIH-OVI űrlapnak a kívánt biztonsági osztály szerint kitöltött példányát.

A biztonsági szint esetében, csak a létfontosságú információs szerelemmel rendelkező szervezet tehet a Hatóság felé írásbeli kérelmet alacsonyabb biztonsági szint engedélyezésére.

- b) az Ibtv. 3. § (2) - (3) bekezdése lehetőséget ad arra, hogy a Hivatal egyes elektronikus információs rendszereit Magyarország területén kívül üzemeltesse, illetve azokban külföldön végezzenek adatkezelést.

A (3) bekezdésre tekintettel a Hivatal az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet nyújthat be a Hatóságnak.

A kérelemhez csatolni kell:

- az EGT tagállamaiban történő adatkezelés indokát,
- az EGT tagállamaiban kezelt adatok és adatbázisok leírását,
- azt, hogy az adatkezelő rendszer, valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy neve, beosztása, elérhetősége ismert-e,
- az adatkezelő rendszer technikai és technológiai leírását, ideértve a hardver- és szoftverkomponenseket is,
- az adatkezelő rendszer információbiztonságának ismertetését, a rendszerhez kapcsolódó, továbbá az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
- a kötelezően lefolytatandó biztonsági rendszerfelülvizsgálat eredményét,
- a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot,
- azt, hogy az üzemeltetés helyszínén illetékes hatóságok jogosultak-e a kezelt adatokba betekinteni.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 21 / 89



Nem szükséges a Hatóság engedélye, ha a külföldi adatkezelést vagy üzemeltetést nemzetközi szerződés írja elő.

1.2 KOCKÁZATELEMZÉS

1.2.1 Kockázatelemzési és kockázatkezelési eljárásrend

Az információbiztonsági felelős előkészíti, dokumentálja a Hivatal kockázatelemzési és kockázatkezelési eljárásrendjét. A törvényi célok teljesítése, a lakosság és a partnerek bizalmának megtartása érdekében biztosítja az információk kockázatarányos kezelését, ennek érdekében minden munkatárs számára tudatossá kell válnia az információbiztonság fontosságának, és a Hivatalnak ezen egységes értelmezése alapján kell tevékenykednie az információbiztonság érdekében. Ez vonatkozik különösképpen az új, innovatív informatikai technológiák hasznosítására. A Hivatal alapfeladatait ellátandó területek (osztályok) saját felelősséggel tartoznak az általuk hasznosított és feldolgozott információk/adatok kockázatarányos védelméért. Ez a felelősség magába foglalja az egyes személyeknek az információk használatával kapcsolatosan felmerülő elszámoltatási kötelezettségét is.

1.2.2 Biztonsági osztályba sorolás

A Hivatalnak elektronikus információs rendszereit - az információbiztonsági felelős irányításával - jogszabályban meghatározott szempontok szerint biztonsági osztályba kell sorolnia kockázatuk alapján. Az elemzés eredményét a kizárólag az érintettek számára hozzáférhető rendszerbiztonsági terv és rendszerenként a *NEIH-OVI Osztályba sorolás és védelmi intézkedés űrlapok* tartalmazzák.

Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást kockázatelemzés alapján kell elvégezni. A kezelt adatok és a funkciók figyelembe vételével a lehetséges kármértéket kell megállapítani, míg a kár bekövetkezésének valószínűsége a körülmények mérlegelésével becsülhető. A biztonsági osztályba soroláskor figyelembe veendő káreseményeket a 41/2015. (VII. 15.) BM rendelet 1 melléklet 2. pontja rendeli az egyes biztonsági osztályokhoz.

Azokban az esetekben, amikor a Hivatal külső szolgáltatót, illetve jogszabály alapján kijelölt szolgáltatót vesz igénybe, a biztonsági osztályba sorolás a szolgáltató feladata, amelyről a Hivatal tájékoztatást kell, hogy kérjen.

A kockázatelemzés és kockázatkezelés során azonban, a Hivatalnak figyelembe kell vennie a külső szolgáltató által meghatározott biztonsági osztály értékét.

A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt (a 41/2015 [VII.15.] BM rendelet iránymutatása alapján).

Az elektronikus információs rendszer biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket. Azokat a kontrollokat, amelyek nem valósulnak meg, kockázatelemzés útján prioritásukat tekintve intézkedési tervben (cselekvési tervben) kell kezelni.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 22 / 89



1.2.3 Kockázatelemzés

Az információbiztonság területén fellépő kockázatokat az információbiztonsági felelős az adatgazdák és a rendszergazda bevonásával értékeli és teszi meg az intézkedési javaslatait a kockázatok kezelésére a jegyző felé.

A Hivatalnak évente legalább egyszer dokumentált módon végre kell hajtania a biztonsági kockázatelemzéseket a *Kockázatelemzési és kockázatkezelési eljárásrend*ben rögzítettek alapján. Ezenkívül, bármilyen változás (fejlesztés, fenyegetések, sebezhetőségek) esetében ismételt kockázatelemzési tevékenységet kell végeznie. Az információbiztonsági felelős a kockázatelemzés során megismert eredményeket, az intézkedéshez szükséges feladatokat, felelősöket, határidőket valamint maradék kockázatokat rögzíti és megismerteti a jegyzővel.

A kockázatelemzés eredményei és a kockázatkezelésre hozott intézkedések bizalmas információnak minősülnek ezért megfelelő jogosultsági szintekkel szükséges tárolni.

A kockázatértékelés eredményeit, illetve az abból származó szükséges intézkedéseket az érintettek felé kommunikálni szükséges, amelyet az információbiztonsági felelős tesz meg.

A *Kockázatkezelési és kockázatelemzési eljárásrend* tartalmazza azokat a közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat, amelyeket – a Hivatal jellemzőire tekintettel – a kockázatelemzés és kockázatkezelés során figyelembe kell venni.

A kockázatelemzési és kockázatkezelési módszertan kialakítása során figyelembe kell venni a vonatkozó törvényi (Ibtv.) és rendeleti (41/2015 [VII.15.] BM rendelet) elvárásokat, informatikai biztonsági szabványok irányelveit.

1.3 RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

1.3.1 Beszerzési eljárásrend

Az információbiztonsági felelős (egyeztetve a rendszergazdával) megfogalmazza, és a Hivatalra érvényes követelmények szerint dokumentálja, jóváhagyásra előterjeszti a beszerzési eljárásrendet (összhangban a Hivatal Beszerzési szabályzatával), mely az elektronikus információs rendszerre, rendszerelemre, az ezekhez kapcsolódó szolgáltatások és biztonsági eszközök beszerzésére vonatkozó szabályait fogalmazza meg. Elősegíti az ehhez kapcsolódó ellenőrzések megvalósítását.

Az informatikai, üzemeltetési eszközök, információbiztonsági követelmények megvalósításához szükséges informatikai eszközök és szoftverek beszerzésénél mindig a Hivatali beszerzésekre vonatkozó elvek szerint kell eljárni, figyelembe kell venni a Hivatal hatályos szabályzatait (összeghatárok, érvényes ajánlatkérések, a kiválasztás menete, garancia stb.).

A beszerzett számítástechnikai eszközöket, szoftvereket a rendszergazdának haladéktalanul nyilvántartásba kell venni.

Az irodai munkavégzéshez szükséges irodatechnikai eszközök, alkalmazások megfelelő minőségben és mennyiségben történő készletezése (készletezés tervezése) a megbízott szervezeti egység vezető vagy rendszergazda feladata. Ezekből a kellékekből mindig akkora készlettel kell rendelkezni, mely biztosítja a folyamatos üzemvitelt.

Azokban az esetekben, amikor a Hivatal olyan elektronikus információs rendszert vesz igénybe, amelynek használatához jogszabályi előírásban kerül meghatározásra a szükséges eszközök beszerzése, (pl. önkormányzati ASP), értelemszerűen a követelményeknek megfelelő eszközök beszerzése az elvárt.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 23 / 89



1.3.2 Erőforrás igény felmérés

A Hivatal éves költségvetésének tervezésekor, illetve beruházások, beszerzések során be kell vonni az információbiztonsági felelőst is, aki a rendszergazdával való egyeztetés után javaslatot tesz az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges információbiztonsági erőforrások (eszközök, szolgáltatások, humán erőforrás) beszerzésére.

A beruházással járó fejlesztések, módosítások, felújítások során az információbiztonsági felelős meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, a beruházás tervezés részeként, és azt bizalmasan kezeli. Figyelembe kell venni a már meglévő technikai és humán kapacitásokat is az egyes erőforrások beszerzése előtt, ugyanakkor a további feladatterhelés nem eredményezheti a már meglévő erőforrások túlzott kimerítését és ezzel összességében a biztonság gyengítését.

A védelmi erőforrásokkal való gazdálkodást kockázatértékelés tárgyává kell tenni.

1.3.3 Beszerzések

Az információbiztonsági felelős a rendszergazdával egyeztetve meghatározza a Hivatal elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési (ideértve a fejlesztést, az adaptálást, a beszerzéshez kapcsolódó rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként:

- a funkcionális biztonsági követelményeket,
- a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint),
- a biztonsággal kapcsolatos dokumentációs követelményeket,
- a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket,
- az elektronikus információs rendszer fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.

A szolgáltatók/szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges.

A külső féllel történő megállapodás megkötését megelőzően az információbiztonsági felelős megvizsgálja, hogy a külső fél által nyújtott szolgáltatásnak milyen információbiztonsági kockázatai vannak. Az így megállapított kockázatokkal arányosan kell meghatározni a megállapodásban a külső fél által teljesítendő információbiztonsági kötelezettségeket.

A szerződések átvizsgálása, véleményezése és releváns információbiztonsági szabályok meghatározása az információbiztonsági felelős, a szolgáltatók/szállítók felé történő kommunikálásról a jegyző gondoskodik.

Szolgáltató/szállító, harmadik személy részére logikai vagy fizikai hozzáférés megadása csak a szállítóval kötött szerződéses megállapodás alapján történhet. A szerződésnek tartalmaznia kell a kockázatokat elfogadható mértékre csökkentő intézkedéseket, szabályokat.

A Hivatal részéről az információbiztonsági felelős (egyeztetve a rendszergazdával) feladata;

- a 3. félével kapcsolatos kockázatok felmérése,
- a vonatkozó biztonsági követelmények azonosítása,
- az esetleg szükséges egyedi óvintézkedések meghatározása,
- a biztonsági követelmények dokumentálása, jegyző felé történő kommunikálása.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 24 / 89



A partnereknek a megfelelő titoktartási megállapodás aláírása után, a szükséges hozzáférés kiadható. A hozzáféréseket nyilván kell tartani és rendszeresen felülvizsgálni.

A hosting szolgáltatást nyújtó külső szolgáltatók kiválasztásánál azok szolgáltatási képességeit, kapacitásait, referenciáit és szolgáltatásuk megbízhatóságát értékelni és ellenőrizni kell.

A szolgáltatók kiválasztásánál preferálni kell a tanúsított információbiztonsági rendszerrel rendelkező szolgáltatókat.

A külső szolgáltatókkal kötött szolgáltatási szerződésekben a Hivatal információbiztonságot érintő elvárásait meg kell határozni.

A szerződésben meg kell határozni, hogy a szolgáltató miként biztosítja a szolgáltatás rendelkezésre állását, a szolgáltatásban érintett és Hivatal tulajdonát képező információ és informatikai eszközök sértetlenségének és bizalmasságnak megőrzését. Ha egy szolgáltatás esetén a sértetlenség és a bizalmasság nem biztosítható maradéktalanul, az adatbiztonság megőrzésére egyéb eljárásokat kell alkalmazni (pl. titkosítás).

A szerződésben meg kell határozni, hogy a szolgáltató miként képes egy esetleges katasztrófa helyzetben szolgáltatását folytatni. Amennyiben ilyen kitétel a szerződésben nem szerepel, a Hivatal feladata a szolgáltatás kiesése esetén alkalmazott eljárás kialakítása, szükség esetén további szolgáltatók és üzemelési helyszínek bevonása a szolgáltatásba.

A Hivatal működése szempontjából kiemelten fontos szolgáltatások vonatkozásában több egyenértékű szolgáltatást kell igénybe venni (kivéve azoknál a szolgáltatóknál, amelyek jogszabályi előírás alapján kerültek igénybevételre), vagy legalább tervet kell készíteni a szolgáltatás elvesztése esetén a szolgáltatás aktiválására, az átállásra.

A megrendeléseket írásban kell megtenni, és a beszerzéshez kapcsolódó feljegyzéseket meg kell őrizni. A beszerzett termékeket, eszközöket a lehetséges mértékig az átvétel során ellenőrizni szükséges.

1.3.4 A védelem szempontjainak érvényesítése a beszerzés során

Ahhoz, hogy a Hivatal védeni tudja az elektronikus információs rendszert, rendszerelemet vagy rendszerszolgáltatást a beszerzés, vagy a beszerzett eszköz beillesztéséből adódó kockázatok ellen, szerződéses követelményként meg kell határoznia a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

Az információbiztonsági felelős feladatai teljesítéséhez szükséges mértékben az elektronikus információs rendszerek valamennyi elemének tervezésével, fejlesztésével, beszerzésével és üzemeltetésével kapcsolatban megilleti a tanácskozási, véleményezési, javaslattételi kezdeményezési, ellenőrzési, betekintési és hozzáférési jogosultság.

1.3.5 Külső elektronikus információs rendszerek szolgáltatásai

A külső elektronikus információs rendszer szolgáltatók értékelése és a szolgáltatási szerződések átvizsgálása (ahol az lehetséges) az információbiztonsági felelős (egyeztetve a rendszergazdával) feladata. Az ügymenethez kritikus szállítók felé a releváns információbiztonsági szabályokat kommunikálni szükséges, amelyről a jegyző gondoskodik. A szerződésben meg kell határozni, hogy a szolgáltató miként biztosítja a szolgáltatás rendelkezésre állását, funkcionális és garanciális biztonsági követelményeket (pl. biztonságkritikus termékek elvárt garanciaszintje), illetve, hogy mik a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 25 / 89



A Hivatal eljárásában rögzíti a külső elektronikus információs rendszer felhasználóinak feladatait és kötelezettségeit.

A szolgáltatási szerződésben lehetőség szerint meg kell határozni, hogy a szolgáltató tevékenységét milyen formában lehet ellenőrizni. Amennyiben erre nincs lehetőség, úgy a szolgáltató munkáját ettől függetlenül ellenőrizni és értékelni kell (például a szolgáltatás során tapasztaltak alapján, amelyet a szolgáltató felé kommunikálni szükséges).

A szolgáltatók tevékenységének folyamatos információbiztonsági ellenőrzése az információbiztonsági felelős kötelessége. A külső szállítókat/szolgáltatókat/harmadik feleket a rendszergazda nyilvántartja.

A külső szállító/szolgáltató/harmadik fél szolgáltatásában bekövetkező változások információbiztonságot érintő várható hatásait értékelni kell, és az ebből eredő kockázatok csökkentése érdekében intézkedni kell.

A megrendeléseket írásban kell megtenni, és a beszerzéshez kapcsolódó feljegyzéseket meg kell őrizni. A beszerzett termékeket, eszközöket a lehetséges mértékig az átvétel során ellenőrizni szükséges.

További szerződéses követelményt, a *Harmadik felekkel szembeni szerződéses követelmények* dokumentum tartalmaz.

1.4 ÜZLETMENET- ÜGYMENET- FOLYTONOSSÁG TERVEZÉSE

1.4.1 Ügymenet-folytonosságra vonatkozó eljárásrend

A Hivatal tevékenységére vonatkozó jogszabályok, a szolgáltatások jellege egyértelműen előírják, hogy a Hivatalnak rendelkeznie kell olyan tervekkel, melyek lehetővé teszik a rendeltetésszerű működéstől eltérő, rendkívüli helyzetek kezelését. Ezen tervekben az alapvető információbiztonsági követelményeket be kell építeni. (A terv nem ronthatja le az eredetileg tervezett és megvalósított biztonsági elemeket).

Az ügymenet-folytonossági folyamat kitér a következőkre:

- kritikus erőforrások, funkciók, szolgáltatások azonosítása,
- elvárások és prioritások azonosítása,
- tervezés – folyamat létrehozása, szerepkörök rögzítése, megismerés,
- kommunikáció,
- tesztelés,
- rendkívüli események bekövetkezése esetén a tervek aktiválása,
- tapasztalatok alapján a tervek felülvizsgálata, fejlesztése.

Az ügymenet-folytonosság tervezés (BCP) célja a legfontosabb (kritikus) folyamatok kiesési idejének minimalizálása, a rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt kockázatokkal arányosan lehessen megvalósítani.

A katasztrófa-elhárítási terv (DRP) célja pedig első sorban a támogató információs / informatikai rendszerek teljes működésének (minden funkcionalitásának) a visszaállítása, vagy újra felépítése.

A folyamat, valamint az ügymenet-folytonosság tervezés és a katasztrófa-visszaállítási terv gazdája az információbiztonsági felelős, aki a terv kidolgozásába bevonja a rendszergazdát.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 26 / 89



A külső elektronikus információs rendszerek szolgáltatói által a Hivatal felé nyújtott szolgáltatások ügymenet-folytonosságának a biztosítása és tervezése, a szolgáltatás üzemeltetését végző feladata (amelyet a szolgáltatási szerződés keretében szükséges meghatározni). A Hivatalnak a saját felhasználói környezetében ügyfelei számára szintén biztosítani kell a szolgáltatás folytonosságát egy esetleges kompromittálódást követően is.

1.4.2 Ügymenet-folytonossági terv informatikai erőforrás kiesésekre

Az ügymenet-folytonossági terv eljárások, vagy tevékenységlépések sorozata annak biztosítására, hogy a Hivatal információfeldolgozó képességeit – a szükséges aktuális adatokkal – a bekövetkezett katasztrófa után elfogadhatóan rövid időn belül helyre lehessen állítani.

A Hivatalon belül kizárólag a folyamatos működés szempontjából kulcsfontosságú személyek számára szükséges kihirdetni az elektronikus információs rendszerekre vonatkozó ügymenet-folytonossági tervet.

A terveknek ki kell térniük minimum az alábbiakra:

- alapfeladatok, alapfunkciók, alapfunkciót támogató kritikus rendszerelemek,
- definiált alapszolgáltatások fenntartása, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is,
- tervezhető rendkívüli helyzetek / katasztrófahelyzetek,
- ügymenet-folytonossági célértékek (alapfunkciók, alapszolgáltatás és összes funkció újrakezdésének időpontja, az ügymenet-folytonossági terv életbelépését követően, tervezett szolgáltatási szint),
- a folytonosság biztosításába bevont szerepkörök meghatározása és megszemélyesítése,
- a tervek aktiválási (életbe léptetési) körülményei,
- az aktiválásról értesítendő személyek,
- a végrehajtásba bevonandó személyek, azok elérhetősége, valamint kapcsolódó feladatok,
- incidens (biztonsági események is) kezelési folyamatának integrálása a tervekben,
- rendkívüli helyzetek / katasztrófa helyzet kezelési folyamatainak részletei, szabályai, prioritások,
- a normál üzletmenetre történő visszaállási eljárásokat (úgy, hogy az nem ronthatja az eredeti ügymenet minőségét),
- rendkívüli helyzetekben szükséges kritikus erőforrások egyes rendkívüli helyzetekhez kapcsolódó információbiztonsági elvárt szinteket.

Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

A változó környezet, változó érdekelt felek változásai a tervek folyamatos naprakészségének a megőrzését követelik meg. A Hivatal szervezetében, működésében, az informatikai rendszerekben bekövetkező minden lényegi változással párhuzamosan, azzal összehangoltan meg kell történnjen az érintett terv elemeinek naprakészé tétele. Ennek érdekében a terveket folyamatosan és rendszeresen felül kell vizsgálni azok alkalmazhatósága, naprakészsége vonatkozásában.

A terveket éves rendszerességgel, illetve szervezeti változások, vagy tesztelés nem megfelelő eredménye esetén minden esetben felül kell vizsgálni. Változások esetén az érintettek felé történő kommunikáció az információbiztonsági felelős felelőssége.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 27 / 89



Az ügymenet- folytonosság tesztelését évente legalább egyszer tervezetten el kell végezni, annak megállapítása céljából, hogy a tervek alkalmasak-e adott rendkívüli helyzetek megfelelő módon történő kezelésére az alábbi tesztelési típusok valamelyikével: szimulációs teszt, végig járás teszt, dokumentum ellenőrzés.

A tervek jogosulatlanok számára nem kommunikálhatók, védeni kell azt a jogosulatlan hozzáféréstől.

Példa ügymenet-folytonosság tervezéséhez:

- a) az elemi kár,
- b) az áramszünet,
- c) a rendszerleállás, szolgáltatásszünetelés, hálózati hiba,
- d) az adatsérülés,
- e) az adatvesztés,
- f) információ-feldolgozó eszközök, adattárolók rongálódása,
- g) eszközök megszokottól eltérő működése (hardver hibás működése),
- h) futtatási hiba (program hibás működése),
- i) biztonsági események.

1.4.3 Kritikus rendszerelemek meghatározása

Meg kell határozni az elektronikus információs rendszer alapfunkcióit támogató kritikus rendszerelemeket, ezeket az ügymenet-folytonossági tervben kezelni szükséges.

1.4.4 A folyamatos működésre felkészítő képzés

A képzés célja az ügymenet-folytonosság jelentőségének tudatosítása, az ügymenet-folytonosság tervezés alapismereteinek átadása, a tervben foglaltak megismerése és elsajátítása. A folyamatos működésre felkészítő képzésben szimulált eseményeket is lehet alkalmazni, hogy elősegítse a személyzet hatékony reakcióját a kritikus helyzetekben.

Az információbiztonsági felelős feladata a munkatársak ügymenet- és szolgáltatásfolytonossággal, valamint az ehhez kapcsolódó információbiztonsági szempontokkal kapcsolatos képzések tervezése, valamint ezen képzések elvégzése.

Minden a tervek végrehajtásában, valamint a rendkívüli események észlelése és eszkalálási folyamatában érintett munkatársat oktatni szükséges évente legalább egyszer (releváns belépő munkatársat a munkakezdés előtt kell oktatni).

A képzések tervezésének bemenő elemei:

- a) tesztek és gyakorlatok eredményei,
- b) érintett felektől gyűjtött direkt visszajelzések,
- c) rendkívüli helyzetek tapasztalatai,
- d) információs rendszerben történő változások,
- e) munkatársi változások,
- f) kapcsolódó utasításokban történő változások.

A képzés, tudatosítás történhet a következő módokon:

- a) e-mail tájékoztatás,
- b) dokumentum elosztás,
- c) személyes képzés, szimulált esemény.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 28 / 89



1.4.5 Üzletmenet-folytonosság elérhetőség

A Hivatalnak ki kell jelölnie egy biztonsági tárolási helyszínt, ahol az elektronikus információs rendszer mentéseinek másolatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja. A biztonsági tárolási helyszínhez történő hozzáférés érdekében (egy esetleges vészhelyzet/katasztrófa esetén) vészhelyzeti eljárásokat kell kidolgozni (ha a mentett adatoknak az elsődleges tárolási helyszínen bajuk esne, hogyan férünk hozzá a másodlagos tárolási helyszínen tárolt adatokhoz).

1.4.6 Infokommunikációs szolgáltatások

A Hivatal - az NTG-re csatlakozó elektronikus információs rendszerek kivételével - tartalék infokommunikációs szolgáltatásokat létesít (internet szolgáltatás), és erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkciói, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a biztonsági tárolási helyszínen.

1.4.7 Szolgáltatás prioritási rendelkezések

Ha az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, az tartalmazza a szolgáltatás-prioritási rendelkezéseket, a Hivatal rendelkezésre állási követelményeivel (köztük a helyreállítási idő célokkal) összhangban.

1.4.8 Az elektronikus információs rendszer mentései

A Hivatal olyan mentési megoldásokat alkalmaz, illetve működtet, amivel biztosítani tudja, hogy az informatikai eszközök sérülése, meghibásodása, adathordozókon tárolt adatok sérülése, használhatatlanná válása esetén, a kiesett informatikai szolgáltatás elfogadható időn belül visszaállítható, illetve az elveszett adatmennyiség mértéke még kezelhető szinten marad. Azon adatok esetén, amelyek hosszú távú megőrzéséért a Hivatal felelős, a mentéseknek alkalmasnak kell lenni az adatok jogszabályban előírt megőrzési idejének végéig történő visszaállítására.

A mentések szakszerű elvégzését a rendszergazda, vagy a Hivatallal kötött megállapodásban rögzítettek szerint az adott elektronikus információs rendszer üzemeltetője (az ASP esetében a szolgáltató) végzi saját adatmentési és naplózási eljárása körében.

A Hivatal a rendszerbiztonsági és üzletmenet-folytonossági elvárásokkal összhangban, mentést végez, amely:

- a) meghatározott gyakorisággal inkrementális (növekményes),
- b) meghatározott gyakorisággal teljes (full) mentést.

A rendszergazda az információbiztonsági felelőssel való egyeztetés után felülbírálni, hogy mennyi adatvesztést képes a Hivatal áthidalni, és ennek megfelelően mi az elfogadható adatvesztési kockázat.

Mentés az alábbi adatállományokról kell, hogy történjen, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal:

- a) az elektronikus információs rendszerben tárolt felhasználószintű információkról,
- b) az elektronikus információs rendszerben tárolt rendszerszintű információkról,
- c) az elektronikus információs rendszer dokumentációiról, köztük a biztonságra vonatkozókat is.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 29 / 89



Az elkészült mentéseket:

- a) védelmi intézkedésekkel kell ellátni (jelszóval védett tömörített állomány vagy titkosított partíció),
- b) offline mentés esetén – helyrajzilag máshol, de minimum másik irodában - védelmi intézkedésekkel ellátott helyiségben található páncélszekrényben szükséges elhelyezni,
- c) dokumentált visszaállíthatósági ellenőrzést kell végrehajtani (adatvisszaállítás teszt jegyzőkönyvek),
- d) biztonsági mentés - rotációban történő törlés esetén, az aktuális ellenőrzés korábban kell, hogy végrehajtásra kerüljön, minthogy az utolsó, még meglévő vissza ellenőrzött biztonsági mentés törlődjön.

A Hivatalnál történő mentést a *Mentési Eljárásrend* részletezi (de alapvetően, 2 egymástól elkülönített helyre történik). A szabályzat elkészítése és naprakészen tartása a rendszergazda feladata. A mentéseknek biztosítaniuk kell bármely információbiztonsági eseményből következő adatvesztések, vagy adat sérülések esetén az adatok hiánytalan visszaállításának lehetőségét, oly módon, hogy azok bizalmassága mindvégig megmaradjon.

1.4.9 Az elektronikus információs rendszer helyreállítása és újraindítása

A Hivatal gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újra indításáról egy összeomlást, kompromittálódást vagy hibát követően.

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az elektronikus információs rendszerek üzemszerű működése és a bennük kezelt adatok előre nem látható esemény (különösen katasztrófa vagy hardver, illetve szoftver meghibásodása, vagy emberi mulasztás) bekövetkezésekor helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell továbbá, hogy az üzemidő-kiesés, adatsérülés és adatvesztés oly mértékű legyen, amely a Hivatal által meghatározott elfogadható kockázati értéken belül marad.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 30 / 89



1.5 A BIZTONSÁGI ESEMÉNYEK KEZELÉSE

1.5.1 Biztonsági eseménykezelési eljárásrend

Biztonsági eseménynek kell tekinteni a nem kívánt vagy nem várt egyedi eseményt vagy eseménysorozatot, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amely hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, rendelkezésre állása, funkcionalitása elvész, megsérül.

1.5.2 Biztonsági esemény kezelése

Az elektronikus információs rendszerben bekövetkezett biztonsági eseményeket dokumentálni kell, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében.

Ennek megfelelően az információbiztonsági felelős megfogalmazza, dokumentálja a biztonsági eseményekre vonatkozó eseménykezelési eljárást, amely szabályozza az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.

Az információbiztonsági felelős;

- összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével,
- egyezteti az eseménykezelési eljárásokat az ügymenet-folytonossági tervéhez tartozó tevékenységekkel,
- az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, továbbképzésekbe és tesztelésbe.

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági események típusát, terjedelmét, az általuk okozott károkat, helyreállítás lehetőségeit és költségeit, a helyreállítás időtartamát.

Az eseménykezelési folyamat fejlesztéséhez kapcsolódó ötleteket bármelyik munkatárs jelezheti az információbiztonsági felelősnek.

A folyamat működtetése és fejlesztése, a kapcsolódó szabályrendszer naprakészen tartása (személyi változások, infrastruktúra változások, gyakorlati események tapasztalatai stb. miatt), valamint azok kommunikálása az információbiztonsági felelős feladata. A felülvizsgálatot évente minimum egyszer el kell végezni, illetve változások esetén azonnal.

1.5.3 A biztonsági események figyelése

A Hivatal nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit. A biztonsági eseményekkel kapcsolatos tevékenységeket az információbiztonsági felelős koordinálja.

Az elektronikus információs rendszerek működése során fellépő eseményeket megfelelő részletességgel naplózni kell. A rendszergazdának ezeket a naplóállományokat rendszeresen ellenőriznie kell, az ellenőrzés eredményéről rendszeresen és szükség esetén időszakosan jelentést kell tennie az információbiztonsági felelős részére.

A biztonsági események folyamatos figyelése és észlelés esetén azok jelentése, valamennyi munkatárs, szerződött fél felelőssége.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 31 / 89



1.5.4 A biztonsági események jelentése

Minden vélt vagy valós információbiztonsági incidenst a felhasználóknak azonnal jelenteniük kell a felettesüknek és /vagy a rendszergazdának, aki jelenti azt az információbiztonsági felelősnek. A felhasználó köteles a tapasztalt jelenséget, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul a rendszergazda rendelkezésére bocsátani (pl. feljegyzés, képernyőkép). A jelentési csatornákat az információbiztonsági felelős kommunikálja az érintettek felé.

Példák információbiztonsági eseményekre:

- a) betörés, lopás,
- b) bizalmas információk kiszivárgása, kiszivárgásának gyanúja,
- c) vírustámadás,
- d) jogosulatlan hozzáférés elektronikus információs rendszerhez és rendszerelemhez,
- e) emberi mulasztás (dokumentált eljárások megszegése),
- f) hálózatbiztonsági incidensek.

A biztonsági esemény észlelésekor, a biztonsági eseményt meg kell szüntetni, vagy az esemény jellegéből adódóan azt izolálni szükséges. Az izolálást azonnal meg kell kezdeni, amelyért a rendszergazda a felelős az érintett felek bevonásával.

Az információbiztonsági incidensről, valamint annak életútjáról jegyzőkönyvet kell készíteni, amelyet az információbiztonsági felelős készít el és jelenti azt a Hivatal vezetője felé.

Az információbiztonsági eseményről készült jegyzőkönyveket megfelelő jogosultsági szinttel kell ellátni.

Az információbiztonsági felelős a 41/2015 (VII.15.) BM rendelet értelmében jelenti azokat a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek (GovCERT-Hungary), amelyek hálózatbiztonsági incidensekből adódnak.

Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni, azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivatalnál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi.

Ha az önkormányzati ASP-t üzemeltetői, működtetői oldalon éri biztonsági incidens, az üzemeltető szervezet veszi fel a kapcsolatot a jogszabályban megjelölt Hatósággal.

1.5.5 Segítségnyújtás a biztonsági események kezeléséhez

A felhasználók felé az információbiztonsági események kezeléséhez kapcsolódó információk és irányelvek megadása, tanácsadás és támogatás az információbiztonsági felelős feladata, a rendszergazda közreműködésével. A támogatást a felhasználók szükség szerint igényelhetik. A biztonsági események figyeléséről, észleléséről és jelentéséről a felhasználókat oktatni kell.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 32 / 89



1.5.6 Biztonsági eseménykezelési terv

Az információbiztonsági felelős megfogalmazza és dokumentálja a biztonsági eseménykezelési tervet. Évente legalább egyszer tervezetten felülvizsgálja, illetve frissíti, figyelembe véve az elektronikus információs rendszer és a szervezet változásait vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat. Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető, módosítható.

Az információbiztonsági események, incidensek kezelési folyamatához kapcsolódóan meg kell határozni és folyamatosan pontosítani kell a biztonsági események kiértékelésének, kategorizálásának (pl. súlyosság, stb) kritériumrendszerét.

Tervezni kell azokat az erőforrásokat és vezetői támogatást, melyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

A tervben meg kell határozni azokat a hálózatbiztonsági incidenseket (pl. DDOS támadás), amelyeket be kell jelenteni az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezetnek (GovCERT-Hungary). Ezekben az esetekben első sorban;

- a) az információbiztonsági felelős,
- b) biztonságiesemény-kezelési megbízott, valamint,
- c) a hatáskörrel rendelkező Kormányzati Eseménykezelő Központ vehet részt.

A biztonsági eseménykezelés a következő folyamatokra terjed ki:

1. *Észlelés, jelentés*

2. *Vizsgálat*

- a) incidensek okának azonosítani, és elemzése, kivizsgálása,
- b) bizonyítékok gyűjtése,
- c) incidens behatárolása.
- d) A vizsgálat során meg kell állapítani, hogy:
 - milyen események történtek?
 - az események milyen és mekkora kárt okoztak, illetve okozhattak?
 - milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?
 - mik voltak az események kiváltó okai, előzményei?

Felelős: információbiztonsági felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők.

3. *Elszigetelés (az esemény jellegéből adódóan)*

4. *Megszüntetés*

- a) a szükséges intézkedések meghatározása,
- b) az incidensekre hozott döntéseket, intézkedéseket dokumentáltan szükséges megtenni,
- c) intézkedések végrehajtása,
- d) az incidenssel kapcsolatos jegyzőkönyvet, egyéb feljegyzéseket meg kell őrizni, annak érdekében, hogy ha egy incidens következtében bármilyen peres (polgári, vagy büntető) eljárásra kerül sor, megfelelő bizonyítékokat lehessen bemutatni.

Felelős: információbiztonsági felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 33 / 89



5. Helyreállítás

Helyreállítási felelősségek kijelölése:

- az ügymenet-folytonosságot érintő események esetén (az esemény jellegéből adódóan) az ügymenet-folytonossági terv, vagy a Katasztrófa-elhárítási tervben rögzített módon kell eljárni.
- a helyreállítási tevékenység ellenőrzése.

Felelős: információbiztonsági felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők.

A biztonsági eseménykezelési folyamatok tesztelését az ügymenet-folytonossághoz kapcsolódó kidolgozott tervek tesztelési folyamatával együtt kell elvégezni.

1.5.7 Képzés a biztonsági események kezelésére

Az információbiztonsági incidensekkel kapcsolatos képzések, valamennyi munkatárs felé belépéskor az alap információbiztonsági oktatás részeként megtörténnek. Ezen felül évente legalább egyszer, vagy súlyos információbiztonsági események után ismétlődő képzés történik a tudatosság fenntartása, illetve fejlesztése érdekében. A képzéseket az információbiztonsági felelős tartja.

A hálózatbiztonsági incidensek (amelyeket be kell jelenteni az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek) kivizsgálásában részt vevő személynek a megbízása előtt részt kell vennie, a *biztonságiesemény-kezelő eljárásról szóló*, a Kormányzati Eseménykezelő Központ által tartott *tájékoztató előadáson*.

1.6 EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG

1.6.1 Személybiztonsági eljárásrend

A személybiztonsággal kapcsolatos elvárás, eljárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki az elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. A Hivatal szerződéses partnereivel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni a szerződéses partnerekkel, harmadik felekkel a Hivatal szabályzatait, eljárásrendjeit, titoktartási kötelezettségekre vonatkozó felételeket.

Az elektronikus információs rendszerek felhasználói, illetve a bevezetésben és felhasználásában közreműködő külső fél munkatársai és vezetői titoktartási nyilatkozat tételére kötelesek, vagy a Hivatal és a külső fél közötti jogviszony alapjául szolgáló megállapodásban kell rendelkezni a külső fél titoktartási kötelezettségéről. A titoktartási kötelezettségnek ki kell terjedni az elektronikus információs rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásukra jutó valamennyi információra. Figyelembe kell venni a központi szolgáltató előírásait.

1.6.2 Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot biztonsági szempontból besorol, rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását.

Az egyes munkakörökbe, feladatokra csak az előre meghatározott képzettséggel és képességekkel rendelkező munkavállalót, szerződéses partnert, harmadik felet lehet alkalmazni.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 34 / 89



A szükséges képzettségi szinteket, gyakorlati elvárásokat a munkaköri leírásokban, szerződésekben szükséges meghatározni. Új munkakör esetén a kereséshez profil, majd az alapján a belépés napjáig munkaköri leírás készül.

A jelentkező, valamint az átlépő munkavállalóknál az átvilágítás mértéke arányos az egyes munkakörök, pozíciók információbiztonsági szempontok szerinti fontosságával, az ennek megfelelően történő besorolásával.

A munkaköröket a Hivatal;

- a) jogokat kiosztó, engedélyező (vezető) és
- b) végrehajtó, felhasználó

biztonsági kategóriákba sorolja.

Ha egy munkakör nem kategorizálható egyértelműen az általános szabályok alapján, vagy kérdés merül fel az általános szabályok alkalmazásával kapcsolatban, akkor az információbiztonsági felelős bevonása szükséges, mely jogosult dönteni ilyen esetekben.

A Hivatal vezetőjének jogában áll egyedi indokok alapján a fenti szempontokból adódó besorolásnál szigorúbb igényeket támasztani egyes munkavállalókra, szerződéses partnerekre, harmadik felekre vonatkozóan.

A Hivatalnál nincsen nemzetbiztonsági ellenőrzés alá eső munkakör és feladat.

1.6.3 A személyek ellenőrzése

A Hivatal a hozzáférési jogosultság megadása előtt ellenőrzi, hogy a hozzáférési jogosultságot igénylő személy (munkavállaló, szerződéses partner, harmadik fél) az adott szervezeti munkakörnek vagy a szervezethez kapcsolódó feladat biztonsági szempontból történő besorolásának megfelelő feltételekkel rendelkezik-e.

A munkafelvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek egyértelmű képet adnak a jelentkező;

- a) szakmai, erkölcsi, informatikai, információbiztonság tudatosság oldaláról tett alkalmasságáról,
- b) mérlegelni kell a foglalkoztatni kívánt személy egyéni tulajdonságait is (pl. megbízhatóság, felelősségtudat, elkötelezettség, terhelhetőség, koncentrálóképeség stb.).

Az átvilágításon túl a Hivatalnál az alkalmazási kikötések és feltételek a következők:

- a) minden munkavállaló, szerződéses partner, harmadik fél, aki hozzáfér az érzékeny információkhoz (az ASP szakrendszerein túl), alá kell, írjon egy titoktartási megállapodást (Titoktartási nyilatkozat 2. számú melléklet), mielőtt a hozzáférés biztosítása megtörténik. Ezen kívül minden munkavállaló az ASP szakrendszereinek használatba vétele előtt, Felhasználói titoktartási nyilatkozat ír alá, amelyet a szolgáltatási szerződés tartalmaz;
- b) a munkakörökhöz meghatározott, releváns szabályozó dokumentumokat minden munkavállalónak, szerződéses partnernek, harmadik félnek figyelembe kell venni, valamint a mindenkor érvényes Informatikai Biztonsági Szabályzatot meg kell ismernie, azt elfogadni és betartani köteles;
- c) a betartandó szabályozó dokumentumokkal kapcsolatban alá kell írjon, egy nyilatkozatot, hogy azokat szerepköréhez kapcsolódóan megismerte, betartja és a nem ismerete nem ad felmentést a be nem tartásuk következményei alól. (Megismerési nyilatkozat-ITB 3. számú melléklet);

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 35 / 89



d) kötelező képzések elvégzését igazoló feljegyzések (Munka és tűzvédelem, ITB oktatás).

Az információbiztonsági felelős véleményezi az egyes munkakörökhöz, feladatokhoz tartozó leírásokat és javaslatot tesz annak információbiztonsági kikötéseire, amelyeket a jegyzői jóváhagyás után a jegyző által kijelölt munkatársnak a munkaköri leírásokban, szerződéseiben rögzítenie kell.

A humán erőforrás fentebb leírt pontjai nem lehetnek ellentmondásban a Hivatal hatályos Informatikai Biztonsági Szabályzatával.

Az átvilágítás módját és a szükséges átvilágítási elemeket szintén a Hivatal *Munkakörök biztonsági szempontú besorolása* dokumentuma tartalmazza.

A besorolási eljárás előkészítése és dokumentálása az információbiztonsági felelős feladata.

1.6.4 Eljárás a jogviszony megszűnésekor

Az alkalmazás megszűnéséről a Hivatal munkáltatói jogait gyakorló vezető dönt. A jogosultságok megszüntetése során figyelembe kell venni, a felmondás jellegét (felmondás, közös megegyezés, azonnali hatályú felmondás), illetve a szerződésben rögzített felmondási és egyéb határidőket és a jogosultságok visszavonásának ütemezését ehhez kell igazítani.

A jogviszony megszűnésekor az alkalmazottnak, a szerződőknek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. A jogosultságok visszavonása a rendszergazda feladata, az információbiztonsági felelős a jogosultságok visszavonásáról meggyőződik, hiba esetén intézkedést kezdeményez.

A rendszergazda megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit, beleértve a hitelesítésre szolgáló eszközöket, felhasználói kártyákat (pl. anyakönyvi kártya), a Hivatal területére való belépésre jogosító kártyákat (pl. proximity kártya).

Az alkalmazás megszűnésekor a kilépő munkatársnak, szerződőnek, harmadik félnek kötelessége minden a Hivatal tulajdonát képező vagyontárgyat visszaszolgáltatni. A rendszergazda a kiadott eszközökről nyilvántartást vezet, és a nyilvántartásnak megfelelően ellenőrzi a munkavállalóra bízott vagyontárgyak hiánytalanságát. A hiányokat vagy károkat a munkatárs köteles megtéríteni.

Abban az esetben, ha a dolgozó saját eszközt használt, meg kell győződni arról, hogy az eszköz nem tartalmaz üzleti információt.

A távozó munkatárs jogosult távozását megelőzően a személyes adatait tartalmazó elektronikus üzeneteket és dokumentumokat törölni, de nem jogosult a munkavégzésével, feladatkörével kapcsolatos üzenetek és dokumentumok törlésére.

A távozó munkatárs levelezési fiókját, elektronikus információs rendszerhez való hozzáférést az információbiztonsági felelős hozzájárulásával, szorosan csak a munkavégzés folyamatosságának fenntartása érdekében ameddig szükséges a rendszergazda archiválja, megtartja (szükség esetén más munkatárshoz irányítja). Minden egyéb esetben a fiókot törölni kell.

Az ASP szakrendszerek esetében 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 Hivatal vezetője az érintetteket értesíti a munkatárs, szerződő, harmadik fél jogviszonyának megszűnéséről, és gondoskodik még a jogviszony megszűnése előtt az elektronikus

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 36 / 89



információs rendszerrel és annak biztonságával kapcsolatos feladatok ellátásáról. Megelőzi az elektronikus információs rendszert, illetve abban tárolt adatokat érintő, információbiztonsági szabályokat sértő magatartását.

Az alkalmazás megszűnését követő meghatározott időszakig történő titoktartást a munkatársaktól, szerződő partnertől, harmadik féltől az alkalmazás megkezdésekor kitöltött titoktartási nyilatkozatban kell rögzíteni. Emlékeztetni kell a titoktartásban vállalt felelőségekről, a távozó munkatársat, szerződő partnert, harmadik felet.

Gondoskodni kell a jogviszony megszűnését követően a megszűnt jogviszonyú felhasználó azonosítójával történő visszaélések elkerüléséről. A jelentést, vagy eszközök visszavételét elmulasztók, mulasztásuk arányában együttesen felelnek.

1.6.5 Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezések, átirányítások esetén, ha szükséges el kell végezni a munkakörnek megfelelően a személyek ellenőrzésére vonatkozó eljárást.

Biztosítani kell mind a logikai, mind pedig a fizikai hozzáférést az újonnan használni kívánt elektronikus információs rendszerhez.

Amennyiben szükséges, módosítani kell, vagy meg kell szüntetni az áthelyezés miatt megváltozott hozzáférési engedélyeket.

A Hivatal vezetője az érintetteket értesíti a munkatárs, szerződő, harmadik fél jogviszony változásáról.

A szerepkörök és jogosultságok változtatását, változáskezelés keretében kell végrehajtani, és a szükséges dokumentumokat módosítani kell (pl. szerződésben meghatározott szerepkör, feladatok, jogok és kötelezettségek, munkaköri leírás). A jogosultság változást jogosultság igénylő lapon kell dokumentálni, illetve központi szolgáltató esetén, az általa meghatározott dokumentált módon. Az adatgazdának kell funkciója keretében, valamennyi személyi változást és a jogosultságok ebből eredő változásait a rendszergazda és az információbiztonsági felelő felé, a jogosultságok aktualizálása érdekében dokumentáltan jelenteni.

1.6.6 A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények

A Hivatal más, külső szervezettel történő szerződés létesítésekor megköveteli, hogy a partner szervezet rendelkezzen olyan, belső biztonsági szabályozással, amelyben meghatározza a biztonsági szerep- és feladatköröket, azonosítja az ilyen feladatkörbe kinevezett vagy azzal megbízott személyeket, rögzíti a velük szembe támasztott elvárásokat.

A partner szervezet által, a saját hatáskörbe tartozó biztonsági munkatársakkal szemben támasztott követelmények és kiválasztási elvek, legalább feleljenek meg a Hivatal által is megkövetelt biztonsági szintnek és eljárásnak, melyet követhető módon dokumentálnak is. A személybiztonsági követelményeknek való megfelelésre a Hivatal a partnernél ellenőrzési jogot köt ki magának, az ellenőrzéssel érintettek körét a szerződésben rögzíteni kell.

A partnernek a Hivatalt haladéktalanul tájékoztatnia kell arról, ha változik a saját információbiztonsági felelősének személye, a biztonsági eseményeket kommunikálni jogosult kapcsolattartó személye és/vagy az elérhetőségének módja, illetve, ha a Hivatal rendszeréhez bármilyen hitelesítési eszközzel vagy kiemelt jogosultsággal hozzáférő munkatársának jogviszonya megszűnik, vagy munkaköre módosul.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 37 / 89



Hitelesítési eszközt vagy kiemelt jogosultságot a partner nem ruházhat át másik munkatársára. Alap felhasználói jogosultság kiadására és visszavonására azonban a partner egy munkatársát a Hivatal felhatalmazhatja, aki a végzett módosításokért ekkor teljes felelősséggel tartozik.

A Hivatal törekszik arra, hogy a meglévő szolgáltatási és egyéb, harmadik féllel kötött szerződéseiben, azok módosításai útján következetesen érvényesíti a fenti kötelezettségeket.

Az információbiztonsági felelős felelőssége, hogy az informatika külsős felek által, a szerződött feladatok végrehajtására kijelölt személyek a munkavégzés kockázataival arányos mértékben átvilágításra kerüljenek.

A jegyző gondoskodik arról, hogy a szerződő felek a szerződésben rögzítsék a kockázatokkal arányosan a titoktartás követelményeit és az együttműködés egyéb kikötéseit.

A szerződéses követelményeket, a *Harmadik felekkel szembeni szerződéses követelmények* dokumentum tartalmaz.

1.6.7 Fegyelmi intézkedések

Minden alkalmazottnak és külső partnernek be kell tartania a Hivatal információbiztonsági szabályait. Minden ennek megtagadásából származó információbiztonsági incidens fegyelmi eljárást vonhat maga után. Az információbiztonsági felelős a tudomására jutott incidenst mérlegeli annak súlyosságától függően, és jelenti azt a jegyző felé. A fegyelmi eljárás módját a jegyző az információbiztonsági felelőssel együttműködve határozza meg az eset súlyosságát figyelembe véve. A fegyelmi intézkedés a jogszabályok és a Hivatal belső szabályai szerint történik.

Szerződéses (külső) partner esetén az információbiztonsági szabályok megsértése során fellépő következményeket a szerződésben rögzíteni kell. A szerződésben foglaltak megszegése esetén érvényesíteni kell a szerződésben meghatározott következményeket, és szükség szerint meg kell vizsgálni és alkalmazni kell az egyéb jogi lépéseket.

1.6.8 Belső egyeztetés

A Hivatal információbiztonsági felelőse tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeket. Meghatározza, szabályozza és folyamatosan felülvizsgálja az elektronikus információs rendszer biztonságát érintő tevékenységekhez szükséges folyamatokat. Minden vezetőségi átvizsgálás során, éves tervkészítéskor felülvizsgálja az erőforrásigényeket, meghatározza és kellő időben rendelkezésre bocsátja azokat a jegyző felé, aki az erőforrásokat, amelyek szükségesek az elektronikus információbiztonság bevezetéséhez, javításához, fenntartásához, rendelkezésre bocsátja.

Az információbiztonság folyamataihoz kapcsolódóan a nem szabályozott tevékenységekhez tervezési folyamatot végez. A tervezés gondoskodik arról, hogy a változtatásokat ellenőrzött módon hajtsa végre, és hogy a változások alatt fenntartsa az információbiztonsági rendszer kifogástalan működését.

1.6.9 Viselkedési szabályok az interneten

Az internet és az e-mail használat legbiztonságosabb módjának kialakításáról a rendszergazda gondoskodik, az információbiztonsági felelőssel együttműködve.

A felhasználónak a Hivatal hálózatában TILOS:

- a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás),

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 38 / 89



- tiltott haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
- b) egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám;
 - c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
 - d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásait indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység;
 - e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés kísérlete, a hozzáférés átruházása más személy részére;
 - f) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
 - g) a Hivatal weboldala ellen bármiféle betörési kísérletet végrehajtani, illetve a szervezet hálózatát felhasználni más oldalak ellen elkövetett szabálysértés támogatására (kivéve a tervezett információbiztonsági ellenőrzéseket);
 - h) a Hivatallal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele;
 - i) az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni;
 - j) fájlcsereelő alkalmazásokat futtatni, illetve nem hivatali munkavégzéshez szükséges letöltéseket végezni;
 - k) a Hivatal elektronikus levelezési rendszerét és a Hivatal tulajdonában lévő internet hálózatot feladatellátásain kívül másra használni;
 - l) a Hivatal informatikai hálózatán, eszközein a képernyőmegosztás, külföldi felhőszolgáltatás, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb. használata.

Weboldalak tiltása:

- a) azokon az eszközökön, amelyeken az Hivatal szakfeladataihoz szükséges ASP elektronikus információs rendszerek elérhetőek, vagy a szakfeladatokhoz szükséges adatok, dokumentumok tárolására kerül sor, csak a munkavégzéshez közvetlenül szükséges weboldalak használata engedélyezett;
- b) technikai intézkedésekkel tiltani kell a szakfeladatokhoz nem szükséges weboldalak elérését. A munkavégzéshez engedélyezett weboldalakat a felhasználókkal való egyeztetést követően az információbiztonsági felelős határozza meg, amelyet jegyzői jóváhagyás után a rendszergazda tesz elérhetővé;
- c) a közösségi oldalak (pl. a Hivatal facebook oldala), egyéb a szakrendszeri hálózaton tiltott oldalak elérése, kizárólag a Hivatal szakrendszeri hálózatáról leválasztott számítógépeken engedélyezettek, a munkavégzéshez szükséges minimális időtartamban.

A rendszergazda a felhasználók által böngészett oldalak listáját szükség szerint naplózza. A naplófájl készítésének és ellenőrzésének célja, hogy a felhasználók Internet használata megfeleljen a Hivatal biztonsági követelményeinek és jogos érdekeinek.

A Hivatal kizárólag a számára dedikált kommunikációs kapcsolaton keresztül vagy saját infrastruktúráján megvalósított felhő alapú szolgáltatást (magánfelhőt), használhat. Az informatikai kockázatok és az adatok feletti felügyelet hiánya miatt tilos nyilvános felhőalapú rendszerek használata.

A rendszergazda köteles rendszeresen ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 39 / 89



E-mail biztonsági szabályok:

- a) a Hivatal tulajdonát képező levelező rendszer csak Hivatali célokra alkalmazható. Magáncélra, valamint etikailag kifogásolható célokra a hivatali postafiókok nem használhatók. Ezen túlmenően a felhasználó felel valamennyi, a címéről elküldött levél rendeltetési helyéért és annak tartalmáért;
- b) ha a felhasználó hosszabb időn át nem tudja postaládáját ellenőrizni, állítson be „Házon kívül” szabályt, így a feladó tudatában lesz annak, hogy a közeljövőben nem fog üzenetére közvetlen választ kapni. Ezzel egyidejűleg adja meg a helyettesítő személy nevét és elérhetőségét, hogy sürgős esetben legyen kihez fordulniuk távolléte alatt;
- c) szükséges a felhasználóhoz kötött egyéni, teljes névvel ellátott, a Hivatal által használt domain nevű egyedi email címek létrehozása, (minta.janos@domain.hu);
- d) tilos a Hivatal saját tulajdonú domain névhez tartozó levelezőrendszerén kívüli levelezőrendszer-használat. Az ingyenes levelezőrendszerek (pl. freemail, gmail, stb.) használatát a szakrendszerek munkaadásainak technikai korlátozásokkal tiltani kell;
- e) ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt felettesének vagy a rendszergazdának. Amennyiben a megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek nem küldheti tovább;
- f) az alkalmazottaknak tilos más alkalmazottak postafiókjához felhatalmazás nélkül hozzáférniük;
- g) a kilépett alkalmazott, megszűnt szerződésű partner levelezési hozzáférését azonnal meg kell szüntetni, az érintett levelezési fiókját a rendszergazda a kilépést követően legalább 30 napig figyeli (vagy ameddig szükséges), ezt követően a fiókot meg kell szüntetni;
- h) tilos a távozott munkatárs nevében elektronikus üzenetet küldeni;
- i) a levelezési rendszerben a hozzáférést biztosító jelszavak létrehozására, kezelésére és változtatására vonatkozóan az általános jelszó használati szabályok érvényesek (ld. 3.7.5. *Jelszó (tudás) alapú hitelesítés*);
- j) a munkatársak kötelesek a levelezési fiókjuk hozzáférését biztosító jelszót titkosan kezelni, azt mások tudomására hozni még a munkafolyamat felgyorsítása érdekében is tilos;
- k) az munkatársak kötelesek azonnal jelenteni a jelszavuk nyilvánosságra kerülésére utaló minden gyanút és körülményt;
- l) tilos a Hivatal levelezési rendszerében használt felhasználónévvel magánérdekből, publikus rendszerekben regisztrálni, fórumokon megjelenni, hírlevelekre feliratkozni;
- m) tilos a Hivatal nevében olyan e-mailt küldeni, melyek:
 - bizalmas, kritikus információt tartalmaznak vagy szerződési, illetve jogi következménnyel lehetnek a Hivatalra nézve,
 - a Hivatal hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatja, illetve a Hivatal ügyfeleinek érdekét sértheti,
 - a Hivatal bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki és a felhasználó erre nem lett felhatalmazva, vagy munkakörének nem része az adott területre vonatkozó vélemény nyilvánítása,
 - szerzői jogokat sérthetnek,
 - vírusokkal fertőzhetik meg a Hivatal infrastruktúráját,
 - vallási, etnikai, politikai vagy egyéb másokra nézve potenciálisan sértő, zaklató tevékenység.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 40 / 89



- n) a felhasználó által küldött elektronikus leveleket a felhasználónak kell aláírnia. Nem használható önállóan csupán a Hivatal neve, vagy annak variációi önálló aláírásként – a felhasználóknak a saját nevüket, és opcionálisan beosztásukat kell használni aláírásként;
- o) a munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából, archiválni szükséges;
- p) a csatolt állományok készítéséhez és a partnerekhez való küldéshez a dokumentumokat előzetesen PDF formátumra kell átalakítani, amennyiben nem szükséges azt szerkeszthető formátumban továbbítani.

Levelezés a Hivatal saját tulajdonú domain névhez kapcsolódó tárhelyen történhet, a rendszergazda által meghatározott vagy a tárhely szolgáltató által biztosított levelező rendszer használatával (lehetőség szerint (SSL) POP3 hozzáféréssel vagy webmail igény esetén (SSL) IMAP hozzáféréssel).

A rendszergazda az elektronikus levelezést korlátozza, az Internetről letöltött, illetve a tárhelyeken tárolt állományokat ellenőrzi. A nem a feladatellátáshoz szükséges állományokat törölni kell.

Az Ibtv. 3. § (2) -(3) bekezdése alapján a külföldi adatkezelést, az egyes elektronikus információs rendszerek Magyarország területén kívül üzemeltetését előzetesen engedélyeztetni kell. (honlap üzemeltetés, email szerver).

Tilos az elektronikus információs rendszerek biztonsági beállításainak megváltoztatása, illetve a vírusellenőrző és Internet böngésző kontrollok kiiktatása.

A felhasználó tudomásul veszi, hogy a Hivatal által meghatározott viselkedési szabályok megsértése fegyelmi intézkedést vonhat maga után.

1.7 TUDATOSSÁG ÉS KÉPZÉS

1.7.1 Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel

A Hivatal, a 2013. évi L. törvény 2. § (1) bek. k) pontja alapján e törvény hatálya alá tartozik.

A 41/2015. (VII. 15.) BM rendelet nevesíti a Hivatal információbiztonsági felügyeletét ellátó Hatóságot, mely e hatáskörében a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH).

A Nemzeti Elektronikus Információbiztonsági Hatóságnál kell kezdeményezni a Hivatal informatikai rendszerének, információbiztonsági felelőségének és Informatikai Biztonsági Szabályzatának regisztrációs eljárását. A Hatóság a sikeres regisztrációt követően felügyeleti funkciókat gyakorol az informatikai rendszer felett, mely során a Hivatal együttműködni köteles.

Fenti törvény 19-20. §-a részletezi a Kormányzati Eseménykezelő Központ feladatkörét. Az informatikai rendszert érintő biztonsági eseményeket a Hivatal e Központ felé köteles jelenteni. Az információcsere és a Központ kárenyhítő intézkedései során a Hivatal együttműködni köteles.

Az információbiztonsági felelős a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében figyelemmel kíséri a Hatóság honlapján közzétett tájékoztatókat, riasztásokat.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 41 / 89



1.7.2 Képzési eljárásrend

A Hivatal köteles rendszeres és tartalmas információbiztonsági továbbképzést tartani minden dolgozójának annak érdekében, hogy a felhasználók tudatában legyenek az információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelősségeiknek. Ehhez az információbiztonsági felelős folyamatosan aktualizált oktatási tervet készít, amelyet egyeztet a rendszergazdával és a jegyzővel. Az oktatási tervnek megfelelően a meglévő dolgozóknak éves szinten megtartja az információbiztonsággal kapcsolatos belső oktatásokat, illetve akkor, ha az információbiztonsági folyamatokban történő változás szükségessé teszi. Új belépő esetén, a munkába állást megelőzően kell megismertetni az információbiztonsági követelményeket. A belső oktatásokon, illetve éves továbbképzéseken kötelező a részvétel, amelyről részvételi nyilvántartást kell vezetni.

1.7.3 Biztonság tudatosság képzés, belső fenyegetés

Az információbiztonsági belső fenyegetések (incidensek) felismerésére, az események jelentésére vonatkozó képzések, valamennyi munkatárs felé belépéskor az alap információbiztonsági oktatás részeként meg kell történnének. Ezen felül évente legalább egyszer, vagy súlyos információbiztonsági események után ismétlődő képzést kell tartani a tudatosság fenntartása, illetve fejlesztése érdekében. A képzések tervezése és azok megtartása az információbiztonsági felelős feladata, a jegyző pedig biztosítja az ehhez szükséges eszközöket, támogatást, és ő maga is részt vesz az oktatásokon. Az oktatásnak az elméleti ismereteken túl, gyakorlati példákat is tartalmaznia kell.

Az információbiztonsági felelős a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében figyelemmel kell kísérje a szakmai fórumokat és a Hatóság honlapján közzétett tájékoztatókat, riasztásokat, ezeket be kell építse az oktatási tervbe.

Belső fenyegetés lehet egy kártevőt tartalmazó e-mail, egy rosszindulatú alkalmazott, vagy akár egy ártatlan felhasználó, akinek ellopták a belépési adatait, esetleg feltörték a számítógépét.

Az oktatás ennek megfelelően legalább az alábbiakra térjen ki:

- a) bevezető (az információbiztonság fogalma és alapelvei),
- b) az információbiztonság fontossága a Hivatalnál, az IBSZ szerepe,
- c) hogyan lehet felismerni a belső fenyegetéseket? Hogyan kerüljük el a fenyegetéseket?
- d) felhasználó megtévesztése – socialengineering,
- e) a gondatlan felhasználói viselkedés veszélyei, a felhasználói viselkedés szabályai az alábbi esetekben;
 - a jelszavak/jogosultságok kezelése, fizikai belépést biztosító eszközök használata, védelme,
 - tiszta asztal, üres képernyő,
 - mobil eszközök (laptop, pendrive, stb) védelme, használata a hivatalon belül és azon kívül,
 - viselkedési szabályok az interneten, e-mail biztonsági szabályok (vírusok, adathalászat),
 - ügymenet-folytonosság (felhasználói szintű).
- f) mit tegyünk, ha már baj van? (jelentési kötelezettség)
- g) összefoglaló, ellenőrző kérdések,
- h) aktualitások.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 42 / 89



Az oktatást követően (akár még aznap, vagy néhány nappal később), rövid és lényegre törő kérdéssort kell a felhasználókkal kitöltetni, amellyel ellenőrizni lehet, hogy a fentebb megjelölt témák mennyire tudatosultak. A nem megfelelően teljesítő felhasználónál, pót oktatást kell tartani.

A teljes munkaidős alkalmazottak oktatása nem elég. Komoly kockázatot jelenthetnek azok a partnerek, beszállítók, alvállalkozók is, akik hozzáférnek a Hivatal eszközeihez, adataihoz, IT hálózatahoz.

Fontos, hogy az alvállalkozók is részesüljenek a biztonsági oktatásban. Ha a Hivatal olyan partnerrel dolgozik, amelynél nincs hasonló képzés házon belül, akkor gondoskodni kell arról, hogy csak megfelelő tájékoztatás után kapja meg az alvállalkozó a hozzáférést a hálózathoz, adatokhoz és erőforrásokhoz.

1.7.4 Szerepkör, vagy feladat alapú biztonsági képzés

Az információbiztonsági felelős feladata a szerepköröknek megfelelő, biztonság tudatosság képzéshez szükséges oktatási anyag összeállítása, lebonyolítása, naprakészen tartása.

A Hivatal a *1.1.7 Szerepkörök, tevékenységek felelősségek* fejezetben határozta meg a Hivatal információbiztonságával kapcsolatos szerepköröket, így ezekre a szerepkörökre nézve kell biztonsági oktatást tervezni és tartania.

Az informatikai rendszerekhez felhasználói jogosultságot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal információbiztonsági szabályait.

Minden munkatárs és új belépő az alábbi alap információbiztonsági képzésben részesül:

- a) bevezető (az információbiztonság fogalma és alapelvei),
- b) az információbiztonság fontossága, az IBSZ szerepe a Hivatalnál, főbb pontjai,
- c) az információk kezelése, az elektronikus információs rendszer használata,
- d) a jelszavak/jogosultságok kezelése, fizikai belépést biztosító eszközök használata, védelme,
- e) az e-mail és internet használata,
- f) belső fenyegetések felismerése, elkerülése, jelentése,
- g) ügymenet-folytonosság (felhasználói szintű),
- h) felelősségek,
- i) aktualitások.

A képzést szükséges megtartani:

- a) a biztonsági tudatosság érdekében, az elektronikus információs rendszer újonnan belépő felhasználói számára, a kezdeti képzés részeként,
- b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi,
- c) amikor a Hatóság honlapján tájékoztatót és riasztást tesz közzé,
- d) ismétlődően évente,
- e) amikor a jegyző erre utasítást ad, vagy erre vonatkozóan utasítás, elrendelés érkezik.

Az alap információbiztonsági oktatáson túlmenően a rendszergazda meghatározott rendszerességgel vegyen részt üzemeltetési és információbiztonsági képzéseken, új technikák, technológiák ismertető előadásain, akár e-learningen tartott, akár workshopokon tartott előadások keretében.

Az alap információbiztonsági oktatáson felül a jegyző és az információbiztonsági felelős:

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 43 / 89



A jegyző (az elektronikus információs rendszerek védelméért felelős vezető) és az információbiztonsági felelős (az elektronikus információs rendszerek biztonságáért felelős személy), a 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének alapján képzésre és éves továbbképzésre kötelezett. A továbbképzéseket (belépő képzések) és az éves továbbképzéseket (ismétlődő képzések) a Nemzeti Községi Egység szervezi.

Amennyiben nem kizárólag az információbiztonsági felelős látja el az elektronikus információs rendszer biztonságával összefüggő feladatokat, akkor a feladatok ellátásában részt vevő személy(ek) képzését, éves továbbképzését is tervezni kell a jogszabály előírása szerint.

Amennyiben nem a 2013. évi L. törvény 13. § (8) -(10) bekezdésben meghatározott feltételekkel rendelkező munkatárs vagy külső szakértő látja el az információbiztonsági felelős feladatait, a kijelölt személy beiskolázásáról is gondoskodni kell. A szakirányú képzés, továbbképzés beiskolázási feltételeit a 26/2013. (X. 21.) KIM rendelet tartalmazza.

A képzéseket az erre szolgáló központi alkalmazással tervezni szükséges, melynek felelőse a jegyző vagy az általa megbízott felelős.

1.7.5 A biztonsági képzésre vonatkozó dokumentációk

Az alap-, és szerepkör alapú biztonsági képzésekről dokumentum születik, mely tartalmazza a képzés helyét, tárgyát, idejét stb. és a résztvevők, illetve oktató aláírásait. Az oktatásokkal kapcsolatos dokumentumokat az információbiztonsági felelős kezeli, tárolja.

A belső képzéseken túl a külső képzésekről a részvételi, ill. látogatási igazolást és egyéb dokumentumokat, a kapott bizonyítványokat a Hivatal archiválja a személyi anyagban, melyet zárt tűzvédtett páncélszekrényben tárol. A képzési dokumentációk megtekintését kérés esetén a Hatóságoknak biztosítani kell.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 44 / 89



2 FIZIKAI VÉDELMI INTÉZKEDÉSEK

2.1 FIZIKAI ÉS KÖRNYEZETI VÉDELEM

2.1.1 Fizikai védelmi eljárásrend

A Hivatalnak gondoskodnia kell a fizikai és környezeti védelmére vonatkozó folyamatainak működtetéséről és fejlesztéséről, a kapcsolódó szabályrendszer naprakészen tartásáról, valamint azok kommunikálásáról az érintettek felé. Az információbiztonsági felelős a rendszergazda közreműködésével kidolgozza a Hivatal fizikai védelmére vonatkozó kontrollokat, megfogalmazza az információbiztonsággal kapcsolatos fizikai engedélyezéseket, amelyek kiterjednek a Hivatal hozzáférési/belépési engedélyek folyamatára.

Az informatika biztonsági rendszer rendkívüli módosításakor, vagy biztonsági esemény bekövetkeztekor, de legalább évente az eljárásrendet újra kell vizsgálni, szükség szerint módosítani.

Az eljárásrend kidolgozása és alkalmazása során, figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre.

A védelmi eljárásrendnek ki kell terjednie az elektronikus információs rendszerek szempontjából érintett létesítményekre, helyiségekre. Az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni. Biztosítani kell a környezeti feltételeket, mint hőmérséklet, páratartalom, szünetmentes áramellátás az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben.

A bárki által szabadon látogatható, vagy igénybe vehető publikus területekre nem vonatkoznak a fizikai és környezeti biztonsági követelmények.

A fizikai védelmi intézkedések követelményeit a Hivatal és az elektronikus információs rendszer üzemeltetője (szolgáltató) saját hatókörén belül teljesíti.

A fizikai biztonságra vonatkozó követelmények betartását a jegyző és az információbiztonsági felelős legalább évente ellenőrzi, az eredményt jegyzőkönyvben rögzíti. A jegyzőkönyvet egy esetleges vizsgálat során az ellenőrzésre jogosult hatóságoknak amennyiben kéri, át kell adni.

Amennyiben az ellenőrzések során fény derül arra, hogy a Hivatal nem teljesíti hiánytalanul a fizikai és környezeti védelmi követelmények megvalósítását, akkor a hiányosságokról intézkedési tervet (cselekvési tervet) készít és rendelkezik annak megvalósításáról.

2.1.2 Fizikai belépési engedélyek

A Hivatal területéhez tartozó épületek, helyiségek biztonsági zónákhoz történő hozzáférése lehetővé teszi a belépésvédelemmel kapcsolatos intézkedések hatékony végrehajtását a mindenkor védelmi igény függvényében.

Az információbiztonsági felelős biztonsági zónákba sorolja a Hivatal területeit és a rendszergazda közreműködésével meghatározza ezen területek esetében a belépésre jogosult személyek listáját, belépéshez szükséges fizikai követelményeket. Ahhoz, hogy az engedélyezett belépési jogosultságok ellenőrizhetőek legyenek, szükséges a Hivatalnak belépési jogosultságot igazoló dokumentumokat (pl. kitűzők, azonosító kártyák, intelligens kártyák) kibocsátania.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 45 / 89



Az információbiztonsági felelősnek meg kell határoznia a kulcsok/kártyák, intelligens kártyák felvételére és leadására vonatkozó szabályokat, az illetékeséget, a kulcsok/kártyák, intelligens kártyák megőrzési rendjét. A kulcsokhoz, kártyákhoz, intelligens kártyákhoz, vagy kódhoz való hozzájutás csak dokumentált módon történhet, a jogosultság kiosztását követően (a jóváhagyást és átvételt dokumentálni kell). A kulcsot, kártyát, intelligens kártyát vagy kódot az a rendszergazda adja ki.

A belépésre jogosultak listáját a rendszergazda folyamatosan felülvizsgálja, és az érvénytelen/megszűnt jogosultságokat eltávolítja. Jogosultságvisszavonás esetében gondoskodik a kiadott kulcsok, kitűzők, kártyák, intelligens kártyák visszavonásáról, megsemmisítéséről, törléséről. Új jogosultság igénye esetén, a jogosultság kiadását megelőzően egyeztet az információbiztonsági felelőssel.

A kulcsokat, kártyákat, intelligens kártyákat olyan helyen kell tárolni, ami nem teszi lehetővé illetéktelenek számára a hozzáférést.

A Hivatal biztonsági zónái:

Zóna	Biztonsági követelmények	Helyszínek/belépésre jogosultak
0 biztonsági zóna	Alacsony biztonsági követelmény	A Hivatal épületein belül és kívül elhelyezkedő mindazon területek, amelyek bárki (pl. ügyfél, látogató) részére nyilvánosan elérhetőek (pl. váróterem, nyilvános folyosó, parkoló)
1. biztonsági zóna	Közepes biztonsági követelmények	A Hivatal azon helyiségei, irodái, amelyekben nincsenek elhelyezve szakfeladatait támogató elektronikus információs rendszerek (pl. tárgyalók), így ide a Hivatal minden munkatársa beléphet, illetve a látogatók/ügyfelek, ők viszont csak kíséret és felügyelet mellett.
2. biztonsági zóna	Magas biztonsági követelmények	A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségek (pl. ASP, anyakönyv) A belépés csak az arra jogosultaknak lehetséges, a látogatók/ügyfelek belépése és ott tartózkodása csak kíséret és felügyelet mellett engedélyezett.
3. biztonsági zóna	Kritikus biztonsági követelmények	IT- és ellátó infrastruktúra valamennyi helyisége, pl. elosztó- és szerverhelyiségek (ideértve a szerverfunkciójú számítógépeket, adatmentő szervereket is, NTG hálózati eszközöket). A belépés kizárólag a rendszergazdának engedélyezett, munkatársak, ügyfelek, látogatók, karbantartók stb. kizárólag felügyelettel léphetnek be és tartózkodhatnak ott.



2.1.3 A fizikai belépés ellenőrzése

A Hivatalnak meg kell határoznia az ügyfélforgalom számára a be-, és kilépési pontokat, melyet az ügyfélfogadási időn kívül zárva kell tartania, ügyfélfogadáson kívül a belépés csak felügyelet és kíséret mellett lehetséges. A nem az ügyfélforgalom számára kijelölt külön bejáratokat kulccsal zárva kell tartani, a belépést csak a kiosztott kulccsal rendelkezők számára lehet biztosítani. A nyilvános területeken kívül, minden belépő ügyfelet, látogatót felügyelet alatt kell tartani, az irodákba, tárgyaló termekbe csakis kísérettel mehetnek be és tartózkodhatnak ott. A látogatót, ügyfelet fogadó munkatárs felelős a látogatóért, annak minden, az információbiztonságot veszélyeztető tetteért. Azokban az esetekben, amikor az épületbe karbantartási (akár épület, akár eszköz), vagy ellenőrzési célból érkeznek, a Hivatalnak kísérnie kell ezeket a személyeket is és figyelemmel kell követnie a tevékenységüket.

A Hivatal takarítását végző személy/személyzet nem takaríthat felügyelet nélkül azon irodákban, ahol informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. szerverszoba, NTG hálózati végpont) van.

Az 1. biztonsági zóna helyiségeinek legalább kulccsal (a kulcs ne legyen a zárban), a 2. és 3. biztonsági zóna helyiségeinek intelligens kártyával, vagy kóddal zárhatónak kell lennie, amely így lehetővé teszi a biztonsági ponton való átjutás ellenőrzését, felügyeletét. A rendszergazda a beléptető eszközöket úgy konfigurálja, hogy az a belépési ponton ellenőrizze az egyéni belépési engedélyt, jogosultságot.

A Hivatalnak vészhelyzetek esetére pótkulcsot, illetve adminisztrátori jogosultságú intelligens kártyát, vagy kódot kell tartania, amelyet hitelesítéssel ellátott borítékban, vagy lepecsételt kulcsdobozban kell elhelyezni, és védett helyen kell tartani (pl. pánccsaszekrény).

A kulcsdoboz, vagy boríték rendkívüli felnyitásáról a felhasználónak telefonon és írásos feljegyzésben értesítenie kell az információbiztonsági felelőst. A hitelesítéssel ellátott boríték felnyitását, a kód használatát követően, a kódot meg kell változtatni.

A rendszergazda, a fizikai belépést ellenőrző eszközökről nyilvántartást vezet, amelyben legalább az alábbiak szerepelnek:

- a) biztonsági zóna (2. és 3. biztonsági zóna),
- b) eszköz (kártyaazonosító/ eszköz szériaszám),
- c) gyártó/szállító/karbantartó,
- d) telepítés/üzembe helyezés dátuma.

A rendszergazda meghatározott rendszerességgel (pl. 3 havonta, fél évente, évente) megváltoztatja a hozzáférési kódokat és kulcsokat, vagy azonnal, ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az adott személy elveszti/megszünteti a belépési jogosultságát. Az információbiztonsági oktatások keretében a Hivatal minden tagjának fel kell hívni a figyelmét a rendellenességek jelentésére, amelyet a felettesük vagy a rendszergazda felé kell megtenniük (pl. elvesztett eszköz, jogosulatlan hozzáférés, belépési jogosultság ellenére belépés megtagadása, stb.).

2.1.4 Hozzáférés az adatátviteli eszközökhöz és csatornákhöz

A rendszergazdának ellenőrzés alatt kell tartania az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe (pl. szerverszoba, irodák, folyosók) történő fizikai belépést. A fizikai belépések naplózása szükséges az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. szerverszoba) esetében (pl. ki, mikor, milyen céllal lépett be, aláírás stb.).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 47 / 89



2.1.5 A kimeneti eszközök hozzáférés ellenőrzése

A fénymásoló és nyomtató berendezéseket/multifunkcionális nyomatkészítőket, a fax készülékeket és minden egyéb kimeneti eszközt védett területen belül kell elhelyezni, ahol a felügyeletük biztosítható, illetve az illetéktelen hozzáférés megakadályozható. Lehetőség szerint úgy kell beállítani a kimeneti eszközöket, hogy a munkafolyamat azonosítható legyen (pl. a nyomtatónál kód használata). A kinyomtatott, faxolt vagy másolt dokumentumokat nem szabad őrizetlenül az eszközökben hagyni. A hibásan nyomtatott, nem használt dokumentumokat meg kell semmisíteni (pl. iratmegsemmisítő).

A képernyőket, úgy kell elhelyezni, hogy azok minél kevesebb lehetőséget biztosítsanak illetéktelen személyek betekintésére.

2.1.6 A fizikai hozzáférések felügyelete

A rendszergazda a 2. és 3. biztonsági zóna szerinti elektronikus információs rendszereknek helyt adó helyiségekre vonatkozóan meghatározott rendszerességgel ellenőrzi a fizikai hozzáférésekről készült naplókat, annak érdekében, hogy észlelje a fizikai biztonsági eseményeket és reagáljon arra.

Azonnal át kell vizsgálni a hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak. Ezekben az esetekben össze kell hangolni a biztonsági események kezelését a napló átvizsgálásának eredményével.

2.1.7 Behatolás riasztás, felügyeleti berendezések

A Hivatal egész épületére érvényes, hogy azt behatolást riasztó berendezéssel kell ellátnia, amely esetében gondoskodni kell a távfelügyeletre való bekötésről. A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségek (2. biztonsági zóna), illetve az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (3. biztonsági zóna) esetében gondoskodni szükséges további védelmi eszköz elhelyezéséről (üvegtörés érzékelő vagy védőfólia az ablakokra). A Hivatalnak gondoskodnia kell arról, hogy rendszeresen átvizsgálásra kerüljön a riasztó berendezés naplója, illetve felügyeleti berendezések felvételei (pl. kamerafelvételek, ha vannak).

Azonnal át kell vizsgálni a behatolás riasztásról készített naplókat, felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre, illetve illetéktelen hozzáférésekből adódóan az elektronikus információ rendszer/rendszerem kompromittálódására utalnak.

2.1.8 A látogatók ellenőrzése

A Hivatalnak a Hivatalba történő látogatói/ügyfél belépésekről információkat kell gyűjtenie (ügyfél/látogató nyilvántartás).

A nyilvántartás legalább az alábbiakat tartalmazza:

- a) dátum,
- b) látogató/ügyfél neve (lehetőség szerint személyazonosítóval igazolva),
- c) ügyfajta, vagy ügyintéző neve.

A megőrzési időt a kockázattal arányosan kell meghatározni (kb. 3 hónap), a selejtezésekről jegyzőkönyvet kell készíteni és megőrizni.

Az irodák/helyiségek ajtajait, ablakait zárva kell tartani, amikor senki sem felügyeli azokat.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 48 / 89



2.1.9 Áramellátó berendezések és kábelezés

A Hivatalnak meg kell védenie az elektronikus információs rendszert árammal ellátó berendezéseket, valamint a kábelezést a sérüléssel és rongálással szemben. Az elsődleges áramforrás kiesése esetére a 3. biztonsági zónában lévő eszközök szabályos leállításhoz a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást kell biztosítani (különös tekintettel az NTG hálózati eszközökre).

2.1.10 Tűzvédelem

A Hivatalnak az elektronikus információs rendszereknek helyt adó irodákban/helyiségekben/szerverszobában független áramellátással támogatott észlelő, az informatikai eszközökhöz megfelelő tűzelfojtó berendezéseket szükséges alkalmaznia, és karban tartania. Ezen kívül a folyosókon, illetve ahol tűzvédelmi szempontból indokolt, tanúsított porral oltó készüléket kell tartani.

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

A Hivatalnak védenie kell a 2. és 3. biztonsági zónában lévő elektronikus információs rendszereket/rendszer elemeket a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzáró szelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségek tervezése (pl. szerver szoba, NTG végpont) során biztosítani kell, hogy az a víz-, és más hasonló kártól védett legyen, ha szükséges, akár csővezetékek kiváltásával, áthelyezésével is. Ezekben a helyiségekben, közvetlenül mellettük, felettük vizesblokk kialakítása tilos.

2.1.12 Be- és kiszállítás

A hivatalvezetője engedélyezi, vagy tiltja a létesítménybe bevitt, onnan kivitt információs rendszer elemeket. A Hivatal tulajdonában lévő kiadott eszközökről kiadási jegyzőkönyvet (átvételi elismervényt) kell írni, amely egyértelműen tartalmazza a kiadott eszköz jellemzőit és a kiadással járó felelősségeket. Az eszköz visszaszolgáltatásakor a rendszergazdának meg kell győződnie arról, hogy az megfelel a kiadáskori állapotának.

Az eszközök igénylését a megbízott szervezeti egység vezetőhöz kell benyújtani.

Behozott eszköz esetében az üzembehelyezést megelőzően meg kell vizsgálni az eszközt, hogy megfelel-e a munkavégzéshez szükséges követelményeknek, információbiztonsági elvárásoknak. Amennyiben az eszköz nem felel meg az elvárt követelményeknek, úgy nem engedélyezhető a Hivatal belső hálózatára való csatlakoztatása.

A behozott eszköz munkahelyi használatból való kivonását megelőzően a rendszergazdának át kell azt vizsgálnia, hogy nem tartalmaz-e a munkavégzés során keletkezett bizalmas, illetve egyéb adatokat.

A hivatal vezetője a kiadott/behozott eszközökről (mobil eszközökről) nyilvántartást kell, hogy vezessen.

A nyilvántartás legalább az alábbiakat tartalmazza:

- a) eszköz megnevezése, (pl. laptop, pendrive, telefon stb.),
- b) szériaszám (modellszám),
- c) kinek adta ki/ki hozta be,
- d) mikor adta ki/ mikor hozta vissza, mikor hozta be/mikor viszi el,
- e) alapkonfiguráció (operációs rendszer, szoftverek, stb) ahol értelmezhető,

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 49 / 89



- f) ellenőrzés eredménye (pl. a visszahozott eszköz megfelel a kiadáskori állapotának, a korábban behozott eszköz nem tartalmaz munkavégzésből származó adatokat),
- g) szükséges intézkedések (pl. telepítés, frissítés, törlés, javítás),
- h) Aláírás (rendszergazda, munkatárs/harmadik személy).

Eszköz szervizbe történő szállítása esetén jegyzőkönyvet kell készíteni, és a rendszergazdának az adathordozókra vonatkozó adatvédelmi szabályoknak megfelelően kell eljárnia (Lsd.3.6 *Adathordozók védelme*). A szerviz által kiadott szállító levelet a rendszergazdának szükséges megőriznie.

2.1.13 Az elektronikus információs rendszer elemeinek elhelyezése

Az irodahelyiségekben az íróasztalokon rendet kell tartani. Csak a munkához felhasznált iratok, adathordozók lehetnek az asztalokon munkaidőben. Munkavégzés után, vagy ha nem tartózkodik senki a helyiségben, az íróasztalokról az adathordozókat, munkához felhasznált iratokat zárható szekrénybe szükséges elhelyezni, illetve az iroda ajtaját zárva kell tartani.

Ha a monitoron minősített információk jelennek meg, biztosítani kell, hogy illetéktelen személy ne lássa a képernyőt (gondolni kell azokra az esetekre is, amikor az épületen kívülről láthatnak be). A felhasználók kötelesek a munkájuk megszakítása vagy befejezése után a számítógépüket zárolni vagy kikapcsolni. Amennyiben a felhasználó elhagyja munkaállomását, úgy használja a képernyő zárolását.

A tárgyalókkal kapcsolatosan az alábbi szabályokat kell betartani:

- a) tilos a tárgyalókban felügyelet nélkül hagyni számítógépet,
- b) bizalmas információ kivetítése, vagy táblán (flipchart-on) történő bemutatása esetén az illetéktelenek betekintését meg kell akadályozni. A fényvédő redőnyöket le kell engedni vagy sötétítő függönyöket el kell húzni,
- c) a táblákon, flipchart-okon hagyott információkat a tárgyalóterem elhagyása előtt törölni kell,
- d) a tárgyalóban is alkalmazni kell a "Tiszta asztal" szabályt.

2.1.14 Karbantartók

A külső szolgáltatónak, illetve a karbantartást végző személynek meg kell ismernie a Hivatal információbiztonsági előírásait, és titoktartási nyilatkozatot kell aláírnia.

A karbantartást csak, az arra kijelölt személyek végezhetik el, akik névsora szerepel a létrejött szerződéses megállapodásban, illetve az eszközökhöz, rendszerekhez, szükséges karbantartási jogosultságuk megfogalmazására került. A szerződésben ki kell kötni, hogy személyi változás esetén, haladéktalanul tájékoztatást kell küldeni a Hivatalnak.

A Hivatalba történő belépéshez, a karbantartási feladatok ellátásához a személyazonosságot igazolni szükséges (külső karbantartók esetében). E nélkül a belépés nem lehetséges. Az eszközök, rendszerek karbantartási munkálatait külső karbantartók esetében a rendszergazdának felügyelni szükséges, hogy kizárásra kerüljenek a jogosulatlan hozzáférések, illetve hibás karbantartási tevékenységek.

A hibákat, rendszerleállásokat, minden karbantartási tevékenységet, (pl. karbantartási naplóban) dokumentálni kell.

A rendszergazdának nyilvántartást kell vezetnie a karbantartó szervezetekről/személyekről, elérhetőségeikről, azok jogosultságairól és arról, hogy mit tartanak karban, és ezt változások esetén aktualizálnia kell.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 50 / 89



További szerződéses követelményt, a *Harmadik felekkel szembeni szerződéses követelmények* dokumentumban -*Amennyiben a harmadik fél fizikai hozzáférést kap*- fejezet tartalmaz.

2.1.15 Időben történő javítás

A biztonsági követelmények teljesítése érdekében az elektronikus információs rendszerelemek (eszközök) karbantartásáról gondoskodni kell. Gondoskodni kell arról, hogy az elektronikus információs rendszerelemek időben történő javítása megtörténjen. Ehhez szükséges tudatosítani a felhasználókban a hiba/eltérés időben történő jelentését, illetve naprakészen kell tartani a karbantartást végzők nyilvántartását, azok elérhetőségeit és azonnal fel kell venni velük a kapcsolatot a mielőbbi elhárítás érdekében.

A karbantartást csak, az arra kijelölt személyek végezhetik el.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 51 / 89



3 LOGIKAI VÉDELMI INTÉZKEDÉSEK

3.1 ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

3.1.1 Engedélyezés

A Hivatal jelen fejezetben fogalmazza meg az információbiztonsággal kapcsolatos logikai engedélyezéseket, amelyek kiterjednek a rendszer- és felhasználó, valamint külső és belső hozzáférési engedélyek folyamatára. A Hivatal a 1.1.7 *Szerepkörök, tevékenységek, felelősségek* fejezetben határozta meg az információbiztonsággal összefüggő szerepköröket, tevékenységeket, felelősségeket.

A Hivatalnak az elektronikus információbiztonsági engedélyezési folyamatokat kockázatkezelési eljárásban rögzítenie kell, összhangban az Informatikai Biztonsági Szabályzattal.

Felügyelnie kell az elektronikus információs rendszer és környezet biztonsági állapotát.

ASP-re vonatkozó engedélyezési szabályok:

Az önkormányzati ASP rendszerben csak a 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről jogszabályban említett szereplők végeznek, illetve végeztetnek központilag fejlesztői, üzemeltetői, működtetői tevékenységet. Bármilyen fejlesztői tevékenységet az ASP Központ vezetője engedélyez írásban.

Az önkormányzati ASP rendszerben tesztelést végezni csak az idézett Korm. rendeletben meghatározott felek jogosultak.

3.1.2 Az elektronikus információs rendszer kapcsolódásai

Szabályozni kell és szükség esetén belső engedélyhez kell kötni az elektronikus információs rendszerek kapcsolódását más elektronikus információs rendszerekhez, dokumentálni kell az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát.

Szabályrendszert kell felállítani és alkalmazni a külső elektronikus információs rendszerekhez való kapcsolódásokhoz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

3.1.3 Belső rendszerkapcsolatok

A Hivatal belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

3.1.4 Külső kapcsolódásokra vonatkozó korlátozások

A Hivatal a külső elektronikus információs rendszerekhez való kapcsolódásokhoz az Informatikai Biztonsági Szabályzatában szabályrendszert állít fel, és alkalmaz, amelynek eredménye lehet az összes kapcsolat engedélyezése vagy tiltása, meghatározott kapcsolatok engedélyezése, meghatározott kapcsolatok tiltása.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 52 / 89



3.1.5 Személybiztonság

A személybiztonsággal kapcsolatos elvárás, eljárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki az elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. A Hivatal szerződéses partnereivel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni a szerződéses partnerekkel, harmadik felekkel a Hivatal szabályzatait, eljárásrendjeit, titoktartási kötelezettségekre vonatkozó felételeket.

Az elektronikus információs rendszerek felhasználói, illetve a bevezetésben és felhasználásában közreműködő külső fél munkatársai és vezetői titoktartási nyilatkozat tételére kötelesek, vagy a Hivatal és a külső fél közötti jogviszony alapjául szolgáló megállapodásban kell rendelkezni a külső fél titoktartási kötelezettségéről. A titoktartási kötelezettségnek ki kell terjedni az elektronikus információs rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásukra jutó valamennyi információra. Figyelembe kell venni a központi szolgáltató előírásait.

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot a *1.6.2 Munkakörök, feladatok biztonsági szempontú besorolása* fejezetben leírtaknak megfelelően besorol a hozzáférési jogosultság megadása előtt. *1.6.3 A személyek ellenőrzése* fejezetnek megfelelően ellenőrzi, hogy a hozzáférési jogosultságot igénylő személy az adott szervezeti munkakörnek vagy a szervezethez kapcsolódó feladat biztonsági szempontból történő besorolásának megfelelő feltételekkel rendelkezik-e.

További szerződéses követelményt, a *Harmadik felekkel szembeni szerződéses követelmények* dokumentumban - *Amennyiben a harmadik fél logikai hozzáférést kap* - fejezet tartalmaz.

3.2 TERVEZÉS

3.2.1 Biztonságtervezési szabályzat

Az információbiztonsági felelős megfogalmazza, a Hivatalra érvényes követelmények szerint dokumentálja a biztonságtervezési szabályzatot, amely tartalmazza a biztonságtervezési eljárás folyamatait, valamint biztosítja annak ellenőrzését. A biztonságtervezési szabályzatot évente egyszer felül kell vizsgálni és ha szükséges frissíteni kell. A biztonságtervezési szabályzatot meg kell ismertetni a munka- és feladatkörük miatt érintettekkel.

3.2.2 Rendszerbiztonsági terv

A Hivatalnak saját hatókörébe tartozó elektronikus információs rendszer tervezésekor rendszerbiztonsági tervet kell készítenie, amely összhangban áll a szervezeti felépítésével, vagy szervezeti szintű architektúrájával.

A rendszerbiztonsági terv a következőket tartalmazza:

- a) az elektronikus információs rendszer hatókörét, alap feladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alap funkcióit,
- b) az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát,
- c) az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerrel való kapcsolatait.

Az elektronikus információs rendszer biztonsági követelményeit rendszerdokumentációba kell foglalni.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 53 / 89



Ezen követelmények tekintetében meg kell határozni az aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

A rendszerbiztonsági tervet és azok változásait csak az érintett személyi és szerepkörökben dolgozók ismerhetik meg.

A terv és kapcsolódó rendszerdokumentációk elkészítése az információbiztonsági felelős feladata.

Az elektronikus információs rendszer rendszerbiztonsági tervét évente felül kell vizsgálni, illetve soron kívül, ha a rendszerbiztonsági tervben, vagy az elektronikus információs rendszerben vagy annak üzemeltetési környezetében változás történt, vagy ha a terv végrehajtása vagy a védelmi intézkedések értékelése során problémák kerültek feltárára.

3.2.3 Cselekvési terv

Az információbiztonsági felelős cselekvési tervet készít, amennyiben a meghatározott biztonsági osztálynál/szintnél hiányosságot állapít meg (tehát, ha valamely védelmi intézkedés nem valósul meg, vagy a bevezetett kontroll hibás/hiányos) és ezekhez mérőföldkövet rendel.

A feltárt hiányosságokat kockázatelemzést követően a kockázatokra adott válasz tevékenységek prioritása alapján teszi sorrendbe (jellemzően a nagy kockázattal járó hiányosságokat helyezi előtérbe).

A cselekvési tervet a hiányosságok megállapítását követően kell elkészíteni:

- a kockázatkezelési stratégia és a kockázatokra adott válasz tevékenységek prioritása alapján,
- az elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál megállapított hiányosságot, a vizsgálatot követő 90 napon belül kell felülvizsgálni, a hiányosság(ok) megszüntetése érdekében,
- ha a meghatározott biztonsági szint alacsonyabb, mint a Hivatalra érvényes szint, a vizsgálatot követő 90 napon belül kell a felülvizsgálatot elkészíteni, az előírt biztonsági szint elérése érdekében.

A cselekvési tervet folyamatosan aktualizálni kell, a biztonsági értékelések, biztonsági hatáselemzések és a folyamatos felügyelet eredményei alapján. A kitűzött feladatok megvalósulását a cselekvési tervben a Hivatal vezetője az információbiztonsági felelős közreműködésével követi nyomon.

A cselekvési terv legalább az alábbi pontokat tartalmazza:

- megvalósulatlan védelmi intézkedés (meghatározott biztonsági osztályhoz tartozó OVI-úrlapból a „nem valósult meg” sorok), bevezetett hibás/hiányos kontrollok, elektronikus információs rendszer ismert sérülékenységei, a kockázatelemzés eredményének sorrendjében,
- tervezett intézkedés,
- felelős,
- tervezett határidő,
- megvalósítás dátuma,
- intézkedés eredménye (teljesült/nem teljesült),
- ellenőrző személy megnevezése.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 54 / 89



A védelmi intézkedések megvalósulását a Hatóság számára a *NEIH-OVI Osztályba sorolás és védelmi intézkedés űrlappal* kell megküldeni. A nem teljesült/hibás kontrollokra létrehozott cselekvési tervet a Hatóság számára szintén meg kell küldeni.

Mivel ezek a tervek bizalmas információkat tartalmaznak, ezért ezt csak a jegyző, az információbiztonsági felelős, és az információbiztonsági felelős által kijelölt személyek ismerhetik meg.

3.2.4 Személyi biztonság

A Hivatalnak gondoskodnia kell arról, hogy az elektronikus információs rendszer felhasználói, a hozzáférési jogosultságot igénylők megismerjék a rájuk vonatkozó szabályokat, felelősségeket és a kötelező, illetve tiltott tevékenységeket az elektronikus információs rendszerben történő munkavégzés, felhasználás tekintetében.

Ennek értelmében minden munkatársnak és új belépőnek, jogosultságot igénylő személynek az alábbi képzésben szükséges részesülnie az elektronikus információs rendszer használatba vételét megelőzően:

- a) az elektronikus információs rendszer működése, funkciói, használata,
- b) az információk kezelése,
- c) az elektronikus információs rendszerhez kapcsolódó elvárások, vonatkozó szabályok, felelősségek,
- d) az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységek.

A képzést szükséges megtartani:

- a) az elektronikus információs rendszerhez jogosultságot igénylők számára a használatba vételt megelőzően, újonnan belépő felhasználók számára a kezdeti képzés részeként,
- b) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi.

Az adatgazda az elektronikus információs rendszerhez való hozzáférés engedélyezése előtt írásbeli nyilatkozattételre kötelezi a felhasználót, hozzáférési jogosultságot igénylő személyt, aki nyilatkozatával igazolja, hogy az elektronikus információs rendszer használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

A szakrendszerhez kapcsolódó felhasználói jogosultság átadását követően, a betanulási időszakban, az új munkavállaló szakrendszerben végzett munkájának fokozott ellenőrzése szükséges. Az ellenőrzés a megbízott szervezeti egység vezető, vagy a jegyző által kijelölt munkatárs feladata.

Az új bevezetésű szakrendszerek felhasználóinak (pl. ASP keretrendszer és szakrendszerek) részt kell venni a központ által előírt oktatásokon.

A Hivatal információbiztonsági felelőse a megbízott szervezeti egység vezetők együttműködésével legalább évente felülvizsgálja és frissíti az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységet a viselkedési szabályok betartását. Változás esetén a hozzáféréssel rendelkezőket tájékoztatja a követelményekről.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 55 / 89



3.3 RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

A 41/2015 (VII.15.) BM rendelet 4. számú melléklet 3.3.3 pontban meghatározott eljárásokat abban az esetben kell alkalmazni, ha a Hivatal saját hatókörében (elektronikus információs rendszer, rendszerelem) rendszerfejlesztési tevékenységet végezne, vagy végeztetne.

3.3.1 A rendszer fejlesztési életciklusa

Amennyiben a Hivatal rendszerfejlesztési tevékenységet végezne, vagy végeztetne figyelemmel kíséri az elektronikus információs rendszer teljes életútját, hogy megbizonyosodjon informatikai biztonsági helyzetéről, annak minden életciklusában.

A Hivatal meghatározza és kijelöli az információbiztonsági szerepköröket és felelőségeket a fejlesztési életciklus egészére, szerződésben, munkaköri leírásban rögzíti ezeket a szerepköröket vonatkozó tevékenységeket, felelőségeket.

A rendszer életciklus szakaszai során a következőket határozza meg:

a) követelmény meghatározás:

A fejlesztéseket, beszerzéseket megelőzően a rendszerkövetelményeket meg kell határozni, amelyeket a szerződésben, fejlesztési dokumentációkban rögzíteni szükséges. Rögzíteni szükséges, a beszerzés, fejlesztés során alkalmazandó információbiztonsági követelményeket.

b) fejlesztés vagy beszerzés:

A beszerzési, fejlesztési szerződésnek és dokumentációknak megfelelően az információbiztonsági követelmények betartása mellett a rendszer, rendszerelem beszerzése, fejlesztése.

c) megvalósítás vagy értékelés:

A beszerzett, fejlesztett rendszer/rendszerelem értékelése annak céljából, hogy ellenőrzésre kerüljön az elvárt követelmények teljesülése. A rendszerek működési vizsgálatához minta adatbázisokat kell használni, a rendszerek teszteléséhez éles adatbázist használni tilos.

d) üzemeltetés és fenntartás:

A beépítésre kerülő rendszerelem, bevezetésre kerülő elektronikus információs rendszer üzemeltetésére és frissítésére meghatározott követelményeket a szerződésben, rendszer dokumentációban rögzíteni kell. Meg kell követelni az üzemeltetéshez, frissítéshez szükséges dokumentációk naprakészen tartását, információbiztonsági elvárások megfogalmazását és betartását.

e) kivonás (archiválás, megsemmisítés):

Az elavult rendszereket, rendszerelemeket, egyéb eszközöket az információbiztonsági követelményeknek megfelelően kell kivonni a Hivatal életéből, amelyet az érintettek felé kommunikálni szükséges.

3.4 KONFIGURÁCIÓKEZELÉS

3.4.1 Konfigurációkezelési eljárásrend

A konfigurációkezelés célja az informatikai infrastruktúra adatainak kézben tartása, az egyes komponensek beazonosítása, figyelemmel követése (incidensfelügyelet, problémakezelés) és karbantartása. A Hivatal életében bekövetkezett változások nyomon követése, hogy mindig naprakészen elérhető legyen, mely változás a rendszer mely pontjában/verziójában ment végbe. Ezáltal elkerülhető, hogy az infrastruktúrán elvégzett változtatások nem várt szolgáltatás kiesést okoznak.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 56 / 89



A információbiztonsági felelős a rendszergazda közreműködésével megfogalmazza és dokumentálja a konfigurációkezelési eljárásrendet, mely szabályozza a konfigurációkezelési folyamatot (konfigurációs elemek kibocsátását és módosítását azok teljes életciklusára vonatkozóan) és elősegíti annak ellenőrzését.

A konfigurációkezelési eljárásrend változásainak nyomon követését az információbiztonsági felelős végzi, és tartja naprakészen.

Minden más esetben, legalább évente egyszer felül kell vizsgálni, mind az eljárásrendet, mind pedig a nyilvántartást.

3.4.2 Alap konfiguráció

A rendszergazdának az elektronikus információs rendszerhez (rendszerekhez) egy-egy alapkonfigurációt szükséges készítenie, amelyet dokumentáltan, bizalmasan naprakészen tart. Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni. A rendszergazda által készített alapkonfiguráció kiterjed valamennyi, hardver és szoftver elemre, valamint telepítő dokumentációkra/leírásra, azok változásaira.

Bármilyen változásnak, ami módosítja a konfigurációs nyilvántartás tartalmát, felügyelet alatt kell lennie, amely a rendszergazda feladata. Ilyenek például az eszközökön, szoftvereken, és a hálózaton végzett változtatások.

Minden egyes fejlesztés/újítás, hibajavítás vagy módosítás esetében a változásokat rögzíteni szükséges és ennek megfelelően frissíteni kell az alapkonfigurációt, de meg kell őrizni az alapkonfiguráció frissítés/újítás előtti verzióját, hogy szükség esetén lehetőség legyen az erre való visszatérésre.

3.4.3 Legszűkebb funkcionalitás

Az elektronikus információs rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője ill. üzemeltetője az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa (pl. a jogszabályban előírt szolgáltató).

A Hivatal saját hatókörén belül meghatározza és biztosítja azokat a minimum konfigurációs beállításokat, amelyek a munkavégzéshez szükségesek. Ennek köszönhetően, semmilyen felesleges beállítás, plusz szolgáltatás/funkció nem kerül konfigurálásra.

A Hivatal korlátozza egyes szoftverek és szolgáltatások hozzáférését. Továbbá tiltja egyes portok, protokollok elérhetőségét elkerülve ezzel a külső támadásokat.

Bármely módosítás esetén szükséges a konfigurációs beállításokat, szoftver és szolgáltatás korlátozásokat, valamint port és protokoll tiltásokat felülvizsgálni és frissíteni, amely a rendszergazda feladata.

3.4.4 Elektronikus információs rendszerelem leltár

A rendszergazdának szükséges:

- a) nyilvántartást készítenie az elektronikus információs rendszer(ek) elemeiről,
- b) azt rendszeres időközönként, minimálisan évente felülvizsgálnia és frissítenie,
- c) az alapkonfigurációs nyilvántartásban vagy más dokumentumban kezelnie.

A leltár célja, hogy információval szolgáljon a Hivatalnál használt eszközökről, ahol lehetséges ezek alapkonfigurációiról, valamint a bekövetkezett változásokról.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 57 / 89



Ennek érdekében úgy kell elkészíteni, hogy pontosan tükrözze az elektronikus információs rendszer aktuális állapotát, valamint az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza.

A leltár legalább a következőkre térjen ki (elektronikus információs rendszerként):

a) Felhasználói ICT eszközök

Felhasználók által használt ICT (információs és kommunikációs technológia) eszközök és az azokhoz kapcsolódó főbb információk (típus, operációs rendszer, elhelyezkedés, felhasználó).

b) Felhasználói alkalmazások, liszenszek

Felhasználó oldali alkalmazások és azok funkciói, egyedi beállítások, liszenszek (szoftver megnevezése, liszensz típusa, liszenszszám).

c) Nyomtatók (megnevezés, típus, sorozatszám, elhelyezkedés).

d) Szerverek

A Hivatal által használt összes szerver, és főbb kapcsolódó információi. (pl. szerver neve, típusa, ip cím, rendszer, CPI, RAM, futó alkalmazások stb.).

e) Szerver oldali alkalmazások, liszenszek

Szerver oldali szoftverek és azok funkciói, egyedi beállítások, liszenszek (szoftver megnevezése, liszensz típusa, liszenszszám).

f) Adatbázisok

A Hivatal adatbázisai, a kapcsolódó információkkal, a mentések módjával (az adatbázisok elnevezése, az egyes adatbázisokon tárolt információk, a mentések módja).

g) Hálózati eszközök, UPS (megnevezés, típus, sorozatszám, elhelyezkedés).

3.4.5 Duplikálás elleni védelem

A rendszergazdának szükséges ellenőriznie, hogy az általa készített elektronikus információs rendszer leltárban nem szerepelnek-e olyan rendszerelemek, amelyek más elektronikus információs rendszer hatókörébe tartoznak.

3.4.6 A szoftver használat korlátozásai

A Hivatal kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak. A szoftver használat főbb szabályai a következők;

- a telepítések során figyelembe kell venni a konfigurációs változáskezelési folyamatra vonatkozó irányelveket;
- a rendszergazda felelőssége a mindenkor ügyleti követelményeknek, valamint információbiztonsági követelményeket teljesítő szoftverek, alkalmazások telepítése. Más felhasználók szoftvertelepítési jogot nem kaphatnak;
- minden új és meglévő szoftver telepítése/frissítése esetében a kiadott telepítési / frissítési útmutatók az irányadók;
- tilos a Hivatal által üzemeltetett munkaállomásokra olyan szoftvert telepíteni, melyhez nincs a Hivatalnak liszensze, vagy (ingyenes liszensz esetén) amelyet a Hivatal nem engedélyez;
- a Hivatal által vásárolt szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek tilos, hacsak megfelelő licenyszerződés ezt nem szabályozza

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 58 / 89



másként, ebben az esetben viszont szükséges nyomon követni a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát;

- f) a biztonsági másolat használat létrehozása és tárolása megengedett az információbiztonsági követelmények betartása mellett (védett tárolás);
- g) minden, a felhasználók rendelkezésére bocsátott hardver és szoftver a Hivatal tulajdonát képezi, és mint ilyen eszköz előzetes bejelentés nélkül bármikor ellenőrizhető;
- h) megfelelő jogosultság nélkül a Hivatal alkalmazottja nem férhet hozzá a Hivatal rendszereihez, illetve olyan számítógépekhez, melyek ügyfél adatokat vagy a Hivatalra vonatkozó bizalmas információt tartalmaznak. Nem végezhetnek jogosulatlanul bármiféle változtatást a Hivatal rendszerein, beleértve az adatok törlését vagy megváltoztatását is;
- i) a szerverekre az operációsrendszer és a felhasználási módnak megfelelő alkalmazás csomag, valamint a megfelelő biztonsági beállítások telepítése a rendszergazda által történik.

A szabályok betartását a jegyző és az információbiztonsági felelős belső auditok keretében ellenőrzi.

3.4.7 A felhasználó által telepített szoftverek

Rendszerprogramokat, illetve felhasználói alkalmazásokat kiszolgálókra és munkaállomásokra, infokommunikációs eszközökre csak a rendszergazda telepíthet, másolhat, távolíthat el.

A felhasználók semmilyen szoftvert, alkalmazást nem telepíthetnek a munkaállomásaikra, az infokommunikációs eszköz használata során kizárólag, az eszközre telepített szoftvereket, alkalmazásokat használhatják. Új szoftver, alkalmazás telepítését vagy a meglévő alkalmazás jogosultságváltozását igényelni kell. A rendszergazda jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági vagy gazdasági okból annak elutasítására.

A felhasználó az infokommunikációs eszközre telepített szoftvereket, alkalmazásokat a szoftverhez, alkalmazáshoz kiadott felhasználói leírás szerinti módon, szakszerűen köteles használni.

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb. (pl. TeamViewer, rAdmin, VNC).

A külső felek által üzemeltetett alkalmazásokhoz kapcsolódó jogosultság igényléseket, változásbejelentéseket és levelezéseket az adatgazdának szükséges másodpéldányban megküldeni a rendszergazdának. A külső fél által biztosított informatikai szolgáltatások használata során az általa kiadott előírások szerint kell eljárni.

A szoftverek adathordozóit, üzemeltetési és felhasználói dokumentációját, liszensz dokumentációját a rendszergazda tárolja és tartja nyilván.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 59 / 89



3.5 KARBANTARTÁS

3.5.1 Rendszer karbantartási eljárásrend

A rendszeres karbantartás célja, hogy a Hivatal biztosítani tudja, az ügymenethez szükséges eszközök és szolgáltatások zavartalan működését, hiba esetén időben történő javítását. A rendszeres karbantartás során a karbantartásra jogosultaknak szükséges ellenőrizni a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát, az esetlegesen felmerülő problémák megoldásáról gondoskodniuk kell. Az információbiztonsági felelős megfogalmazza és dokumentálja a rendszeres karbantartásra vonatkozó kontrollokat, mely szabályozza a rendszeres karbantartási folyamatot és elősegíti annak ellenőrzését.

3.5.2 Rendszeres karbantartás

A rendszeres karbantartásokat csak az arra jogosult személy(ek) végezheti(k) (Lsd. 2.1.14 *Karbantartók* fejezet). A Hivatal a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentáltatja, felülvizsgálja és jóváhagyja az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban.

A Hivatalnak a karbantartásokra karbantartási tervvel szükséges rendelkeznie, amelynek elkészítése a rendszergazda feladata. A karbantartási tervben meghatározásra kerül a munkaállomások, szerverek, perifériák, hálózati eszközök fizikai és szoftveres állapotát ellenőrző karbantartások ütemezése, felelőse.

Külső személy/szolgáltató esetében a karbantartások ütemezését és azok feltételeit a szerződésben rögzíteni szükséges.

A hibákat, rendszerleállásokat, minden karbantartási tevékenységet dokumentálni szükséges (karbantartási napló/nyilvántartás).

A dokumentálásnak legalább az alábbiakra szükséges kitérnie:

- ütemezés (pl. előre ütemezett (tervezett), nem tervezett karbantartás),
- mikor történ a karbantartást (dátum, idő),
- a karbantartás megnevezése (ellenőrzés, javítás, frissítés stb.),
- az érintett eszköz/szoftver, rendszer megnevezése,
- módszer (pl. szemrevételezés),
- karbantartáshoz szükséges eszközök megnevezése,
- ki/kik végezte/ték a karbantartást,
- mennyi ideig tartott a karbantartás,
- ha volt rendszerleállás, mennyi ideig tartott,
- a karbantartás ellenőrzés tényét (sikeres, sikertelen),
- intézkedés megjelölése sikertelen karbantartás esetén,
- aláírás.

A karbantartások utáni megfelelő működés ellenőrzése a rendszergazda, illetve külső személy/szolgáltató esetében a megbízott személy/szolgáltató feladata. Sikertelennek bizonyuló működés esetén, az adott eszközt, rendszert nem lehet újra üzembe helyezni, egészen addig, amíg a fennálló hibát ki nem javítják. A javításokért a rendszergazda illetve külső megbízott esetén a külső személy/szolgáltató felelős.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 60 / 89



A karbantartások történhetnek munkaidőn kívül, vagy munkaidőn belül. A tervezett munkaidőn belüli karbantartásokat, ha azok az ügymenet kiesésével járnak, a karbantartás előtt 1 héttel közölni kell az ügyfelekkel.

A Hivatal birtokában lévő fizikai szerverek karbantartása a rendszergazda illetve külső személy/szolgáltató esetében a megbízott személy/szolgáltató feladata, szerződéses megállapodás szerint. A szerverek karbantartását ütemezetten, lehetőség szerint, munkaidőn kívül kell végrehajtani.

Adattartalommal bíró adathordozók, információs rendszer vagy rendszerelem szállítása esetén a megfelelő információbiztonsági intézkedések betartása kötelező a 3.6. *Adathordozók védelme* fejezetnek megfelelően. Karbantartás céljából az adathordozók, információs rendszer vagy rendszerelem szállítását a rendszergazda, külső személy/szolgáltató esetében a megbízott személy/szolgáltató végzi.

A Hivatal által használt szoftveres frissítéseket a rendszergazda végzi, figyelemmel kísérve egy-egy új patch megjelenését.

3.5.3 Adathordozó ellenőrzés

A rendszergazda a Hivatali munkaállomásokon lévő víruskeresőt úgy állítja be, hogy az automatikusan ellenőrizze a munkaállomásra csatlakoztatott diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, mielőtt azt az elektronikus információs rendszerben használnák.

3.5.4 Távoli karbantartás

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, tilos olyan alkalmazást használni, amely az eszközt az ASP Központon kívüli harmadik féllel köti össze, és amellyel lehetőség van távoli támogatásra, vezérlésre, távoli hozzáférésre, képernyő átvételére stb. (pl. távoli asztal, TeamViewer, rAdmin, VNC).

Egyéb esetben (saját hatókörbe tartozó elektronikus információs rendszer, pl. levelező/webszerver stb.) a rendszergazda az alábbiak szerint jár el a távoli karbantartás tekintetében:

- jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket,
- akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, ha az összhangban áll az Informatikai Biztonsági Szabályzattal, és dokumentálva van az elektronikus információs rendszer rendszerbiztonsági tervében,
- hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál,
- lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik,
- nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 61 / 89



3.6 ADATHORDOZÓK VÉDELME

3.6.1 Adathordozók védelmére vonatkozó eljárásrend

A Hivatal jelen eljárásában rögzíti az adathordozók védelmére vonatkozó előírásait.

A Hivatali munka során használt adathordozók kezelésének szabályozása a megfelelő és biztonságos működés és rendelkezésre állás érdekében történik.

A munkavégzéshez a Hivatal tulajdonában lévő, nyilvántartott adathordozót lehet használni, illetve behozott adathordozó esetében a rendszergazda által ellenőrzött és engedélyezett eszközt (Lsd. 2.1.12. *Be- és kiszállítás*). Az adathordozó használatára való igényt a hivatal vezetőjéhez kell benyújtani. A rendeltetésszerű eszközhasználatot a Hivatal elektronikus információs rendszereihez történő csatlakoztatás után, a rendszergazda szűrőpróba szerűen ellenőrizheti.

Adatot adathordozón/mobil eszközön (laptop, pendrive, floppy, CD stb.) a Hivatalból kijuttatni csak a hivatalvezető írásos engedélyével szabad az információbiztonsági előírásoknak megfelelően. A Hivatal az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

Az adathordozók információbiztonsági kezelésének általános irányelvei:

- a) informatikai eszközöket, adathordozókat tilos nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizetlenül hagyni;
- b) munkavégzés közben nem lehet a használatban lévő mobil eszközöket felügyelet nélkül hagyni, a használaton kívüli eszközöket védett helyen kell tárolni („tisztas asztal” szabálya);
- c) az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani nem lehet;
- d) tilos az olyan hordozható adathordozó használata az elektronikus információs rendszerben, melynek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni;
- e) az adathordozókat a felhasználók nem csatlakoztathatják egymás eszközeihez úgy, hogy az eszköz tulajdonosa nem tud róla;
- f) amennyiben kívülről érkezik adat valamilyen adathordozón, annak a megtekintése csak előzetes ellenőrzés és a vírus mentesség megállapítása után használható.

3.6.2 Hozzáférés az adathordozókhoz

A rendszergazda meghatározza az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosultságuk tartalmát.

A Hivatalból kilépő munkatársak vagy szerződéses viszony esetén a szerződés megszűnésében érintett megbízott harmadik felek kötelesek minden a birtokukban vagy használatukban lévő, a Hivatal tulajdonát képező eltávolítható adathordozót a rendszergazdának biztonságosan átadni, aki ellenőrzi, hogy az adathordozó állapota megegyezik-e a kiadáskori állapotával.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 62 / 89



3.6.3 Adathordozók tárolása

A Hivatalnak biztosítani kell az adathordozók fizikailag ellenőrizhető és biztonságos tárolását, az arra kijelölt vagy engedélyezett helyen. Mind addig védeni kell az elektronikus információs rendszer adathordozóit, amíg az adathordozókat jóváhagyott eszközzel, technikákkal és eljárásokkal meg nem semmisítik, vagy nem törlik a rajtuk tárolt adatokat.

3.6.4 Adathordozók szállítása

Az adathordozók szállítása során az alábbi biztonsági szabályokat szükséges alkalmazni:

- a szállításhoz lehetőleg zárható és a káros környezeti hatásoktól védő tokot, dobozt, táskát kell használni;
- szállítás közben az adathordozót folyamatosan a munkatárs személyi felügyelete alatt kell tartani;
- szállítás során nem szabad az adathordozót másnak átadni, mások felügyeletére bízni,
- óvni kell a nagy melegtől, nagy hidegtől, gyors hőmérséklet változástól, közvetlen napsugárzástól, portól, nedvességtől;
- ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg szobahőmérsékletre kerül;
- a munkatársak kötelesek az általuk szállított fizikai adathordozókkal kapcsolatos minden eseményt (elvesztés, sérülés, lopás) felettesüknek vagy az információbiztonsági felelősnek haladéktalanul jelenteni;
- gépkocsival történő szállítás esetén az információs rendszer elemeket zárt/fedett csomagtartóban kell elhelyezni oly módon, hogy védve legyen a rázkódásból, sérülésből adódó károktól. Az információs rendszer elemeket és adathordozókat tilos (még rövid időre is) az autóban hagyni, a munkatársnak jármű elhagyásakor magával kell azokat vinnie;
- tilos az informatikai eszközök használatát harmadik feleknek átengedni, sem idegenek, sem családtagok, rokonok, ismerősök nem használhatják ezeket. A tiltás vonatkozik a saját tulajdonú eszközökre és a távmunka során használt eszközökre is.

A rendszergazda az adathordozók szállításával kapcsolatos tevékenységeket azokra a személyekre korlátozza, akik általa az eszközök be- és kiszállítására engedélyt kaptak. Az adathordozók szállításával kapcsolatos engedélyeket, tevékenységeket dokumentálnia kell.

„Bizalmas” feletti besorolású adatokat tartalmazó adathordozót különös gondossággal kell szállítani. A mentési adathordozók szállítását csak a rendszergazda vagy az általa megbízott személyek végezhetik.

3.6.5 Kriptográfiai védelem

Minden olyan hordozható eszközt, amelyet a Hivatal területén kívül használnak, szállítanak kriptográfiai (hardver titkosítási) mechanizmusokkal kell védeni a digitális adathordozókon tárolt információk bizalmosságának és sértetlenségének védelme érdekében (hordozható adattároló, pl. okostelefon, laptop, pendrive stb.).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 63 / 89



3.6.6 Adathordozók törlése

Az adathordozók törlésére vonatkozó biztonsági irányelvek:

- a) az adathordozókat elhasználódásuk esetén cserélni és selejtezni kell az adatvesztés elkerülése érdekében,
- b) az adathordozókat selejtezés előtt minden esetben adat mentesíteni kell ilyen célú megfelelő alkalmazással,
- c) a nem törölhető adathordozókat meg kell semmisíteni iratmegsemmisítőben vagy más módon össze kell törni,
- d) az adatmentesítés a rendszergazda feladata és felelőssége,
- e) a beépített, azaz nem mobil (nem cserélhető) lemez meghajtók szükség szerinti cseréje, és az elhasználódottak selejtezése a rendszergazda feladata.

A törlési mechanizmusokat a rendszergazda az információ minősítési kategóriájával arányos erősségnek és sértetlenségnek megfelelően alkalmazza:

- a) a „belső használatú” védelmi osztályba sorolt információkat tartalmazó adathordozót úgy kell megsemmisíteni, hogy ne legyen lehetőség a jogosulatlan hozzáférésre,
- b) a „bizalmas” védelmi osztályba sorolt információkat tartalmazó adathordozókat úgy kell megsemmisíteni, hogy az információk helyreállítása csak jelentős támogatással/eszközkészlettel, emberi erőforrással és időbefektetéssel legyen lehetséges,
- c) a „szigorúan bizalmas” védelmi osztályba sorolt információkat tartalmazó adathordozók helyreállítására nem lehet mód korszerű eszközökkel,
- d) adathordozó selejtezés céljára harmadik félnek, csak adat mentesítve adatható át.

Ha harmadik félnél történő javításra van szükség, és az elmentett adatok előzetes és biztonságos törlésére nem volt lehetőség, akkor a javítást külön megállapodás keretében helyszíni jelenlét betartásával kell elvégeztetni. A selejtezéssel, megsemmisítéssel megbízott 3. féllel titoktartási megállapodást kell kötni.

3.6.7 Adathordozók használata

A Hivatal engedélyezheti, korlátozhatja vagy tilthatja bizonyos, vagy bármely adathordozó típusok használatát a kijelölt elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági intézkedések használatával.

3.6.8 Ismeretlen tulajdonos

A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 64 / 89



3.7 AZONOSÍTÁS ÉS HITELESÍTÉS

3.7.1 Azonosítási és hitelesítési eljárásrend

A Hivatalnak gondoskodnia kell arról, hogy a Hivatalnál jelenlévő felhasználók mindegyike egyedileg legyen azonosítva és hitelesítve, valamint egyedileg legyenek azonosítva és hitelesítve a felhasználók által végzett tevékenységek.

Biztosítania kell ezt mindazért, hogy a tevékenységek és a hozzájuk tartozó felelőségek egyértelműen azonosíthatók legyenek, illetve, hogy elkerülhetővé váljanak a jogosulatlan hozzáférések, ezáltal csökkenthetőek a jogosulatlan hozzáférésekből származó információbiztonsági incidensek.

A szükséges jogosultságokat a felhasználóknak, az írásos jogosultság igénylését az adatgazdák hagyják jóvá és a rendszergazda/központi szolgáltató által kijelölt adminisztrátor osztja ki/állítja be.

A Hivatalnál jelenlévő felhasználóknak kiosztott jogosultságokról a rendszergazdának nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdákkal közösen felül kell vizsgálni. Frissíteni kell továbbá, bármilyen módosítást követően.

3.7.2 Azonosítás és hitelesítés (Hivatalon belüli felhasználók)

A Hivatal a munkaállomásokon egyedileg azonosítja és hitelesíti a Hivatal felhasználóit, a felhasználók által végzett tevékenységeket/ szerepköröket.

A munkavégzéshez tartozó tevékenységi köröket és az azokhoz szükséges jogosultságokat az információbiztonsági felelős az adatgazdák és a rendszergazda közreműködésével határozza meg. Más, Hivatali rendszerhez (pl. szerver) való jogosultságokat és tevékenységi köröket az adott rendszerben kell megadni.

A központi szolgáltató rendszereinek használatához szükséges azonosítási és hitelesítési eljárást az üzemeltető határozza meg.

ASP-ben a kétfaktoros azonosítás elvárás, amely a jelszó (tudás) alapú hitelesítés és a birtoklás alapú (E-személyi) hitelesítésből áll össze.

- a. E-személyi, kártyaolvasó, PIN kód
- b. felhasználónév-jelszó

A tenant szintű jogosításokat és eszköz alapú hitelesítéseket az ASP központ üzemeltetője osztja ki, módosítja és vonja vissza, a megfelelő igazgatásszervezési feladatok során meghatározott rend szerint.

A Hivatalnál tilos a csoportos felhasználói azonosítók használata.

3.7.3 Azonosító kezelés

A Hivatal a munkaállomásaihoz és az elektronikus információs rendszerhez, rendszerelemhez való hozzáféréshez szükséges azonosítókat szerepkörök vagy személyek jogosultságaihoz köti.

Az önkormányzati ASP rendszer használata során a jó áttekinthetőség érdekében összehangolt szerepkör-megnevezéseket szükséges alkalmazni. Ugyanannak a felhasználónak több szerepköre is lehet.

A Hivatalnál nincs mód, az azonosítók újbóli felhasználására.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 65 / 89



A Hivatalnál a felhasználók azonosítója 2 hét inaktivitás után letiltásra kerül a rendszergazda által, és amikor a felhasználó ismét aktív az azonosítóját újra engedélyezi.

A munkaállomáshoz, rendszerelemhez, elektronikus információs rendszerhez, történő hozzáférést biztosító azonosítókat;

- a rendszergazda (munkaállomáshoz, rendszerelemhez/eszközhöz),
- az önkormányzati ASP adminisztrátor (bérlő fiók, tenant szintű felhasználó kezelés)
- az önkormányzat szakrendszerei adminisztrátor(ok) (szakrendszer szintű jogosultságkezelés)
- egyéb központi szolgáltató (pl. anyakönyv) által kijelölt adminisztrátor

biztosítja.

3.7.4 A hitelesítésre szolgáló eszközök kezelése

Az E-személyi segítségével a Hivatali felhasználó azonosíthatja magát és beléphet az ASP szakrendszerekbe, továbbá a hozzárendelt elektronikus aláírás segítségével hitelesítheti az elektronikus dokumentumokat.

Amennyiben a Hivatal felhasználója nem elektronikus személyazonosító okmánnal hitelesíti magát, a Hivatal:

- ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát,
- meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát,
- biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat,
- dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket,
- megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során,
- meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit,
- a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket,
- megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól,
- megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét,
- lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

3.7.5 Jelszó (tudás) alapú hitelesítés

A Hivatalnál az alábbi szabályozások kerültek meghatározásra, a hitelesítésre szolgáló jelszavak kezelését illetően:

- a munkaállomások, rendszerelemek, rendszerek hozzáféréséhez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni;
- a munkaállomásokhoz, rendszerelemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni;

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 66 / 89



- c) **a jelszavak erősségének irányelve:** a jelszavak minimális hossza 6 karakter, tartalmazniuk kell kis- és nagybetűket, speciális és numerikus karaktereket egyaránt. Tilos olyan jelszavakat alkalmazni, melyek könnyen kitalálhatóak, mint például a személyes adatok, egyértelmű dátumok vagy általános szavak (pl. „admin”, „password”), illetve amelyek gyári beállítású, alapértelmezett jelszavak;
- d) a felhasználók és megbízott harmadik felek felelősek a személyes jelszavaik megfelelő védelméért és annak következményeiért, ha a jelszavaik mások által ismertté válnak;
- e) a jelszavakat azonnal meg kell változtatni, ha a felhasználó úgy gondolja, hogy azok más tudomására jutottak, vagy valami szokatlan tapasztaltak a számítógépes rendszerükben;
- f) a jelszavakat rendszeres időközönként, legalább 3 havonta cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített időközönként;
- g) új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni;
- h) tilos a felhasználóknak bejelentkezni a Hivatal rendszereibe olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak;
- i) a felhasználók a személyes azonosítójukkal és jelszavukkal elkövetett cselekedetekért felelősséggel tartoznak;
- j) a hardver eszközökkel rendelkező felhasználók az adott eszközt kötelesek biztonságos helyen tárolni, és eltűnésük esetén azt haladéktalanul jelenteni, azzal az információval együtt, hogy milyen Bizalmas/Szigorúan Bizalmas minősítésű dokumentum kompromittálódott;
- k) amennyiben a felhasználók által használt rendszerek valamelyike a fentieknél alacsonyabb biztonsági szintet követelne meg, a felhasználóknak minden esetben az itt szereplő szabályok szerint kell eljárni;
- l) ez a jelszó politika érvényes azokra a külső (nem a Hivatal által üzemeltetett) rendszerekre is, amelyeket a felhasználók a munkájukkal kapcsolatosan elérnek.

A központi szolgáltató kötelező elvárásokat érvényesít a jelszó megadásával kapcsolatban.

3.7.6 Birtoklás alapú hitelesítés

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

3.7.7 Személyes vagy megbízható harmadik fél általi regisztráció

A Hivatal szükség esetén meghatározott hitelesítő eszköz átvételéhez olyan regisztrációs eljárást követel meg, melyet meghatározott regisztrációs szervezet folytat le a Hivatal által meghatározott személyek vagy szerepkörök jóváhagyása mellett.

3.7.8 A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszernek fedett visszacsatolást kell biztosítani a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 67 / 89



A Hivatalnál alkalmazott hitelesítési módszerek érdemi információval nem szolgálnak az esetleges támadóknak. A sikertelen belépést követően, a rendszer minimális üzenetet küld vissza a felhasználónak (pl. elrontott felhasználónév vagy jelszó esetén: „belépés sikertelen, elfelejtett jelszó” stb.)

3.7.9 Azonosítás és hitelesítés (hivatalon kívüli felhasználók)

A Hivatalnak az elektronikus információs rendszerben, rendszerelemben egyedileg kell azonosítania és hitelesítenie a Hivatalon kívüli felhasználókat és a tevékenységüket.

Külső partnerek (szerződött partnerek, harmadik személyek) vonatkozásában a Hivatal IT rendszereihez való hozzáférés csak szerződés alapján biztosítható.

Külső partnerek esetén a hozzáférési jog maximum a szerződés lejáratáig adható.

A Hivatal IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés/ megállapodás és titoktartási nyilatkozatok alapján gyakorolhatják.

3.7.10 Hitelesítésszolgáltatók tanúsítványának elfogadása

Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el a Hivatalon kívüli felhasználók hitelesítéséhez.

3.8 HOZZÁFÉRÉS ELLENŐRZÉS

3.8.1 Hozzáférés ellenőrzési eljárásrend

Az információbiztonsági felelős megfogalmazza és dokumentálja a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A jogosultság kezelés során figyelembe kell venni a központi szolgáltató előírásait.

Az elektronikus információs rendszer, rendszerelem használója kizárólag olyan munkatárs vagy a Hivatallal szerződéses jogviszonyban álló szerződött partner, harmadik személy lehet, aki a munkavégzéshez szükséges feltételekkel az 1.6.3. *A személyek ellenőrzése* fejezetnek megfelelően rendelkezik. Megismerte jelen szabályzatot, a rá vonatkozó rendelkezéseket, és ennek megfelelően hozzáférési jogosultságot kapott az elektronikus információs rendszerek használatához (a továbbiakban: felhasználó).

A központi szolgáltatók szakrendszereihez történő hozzáféréseket az üzemeltető által meghatározott szabályok alapján kell kezelni.

A hozzáférési jogosultságokat az adatgazda engedélyezi a hatáskörébe tartozó elektronikus információs rendszerek, rendszerelemek, adatok, tevékenységek tekintetében. A jogosultságok beállítását adott rendszertől függően a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor végzi. A kiadott jogosultságok engedélyezéséhez kapcsolódó feljegyzéseket meg kell őrizni.

A Hivatalnál jelenlévő felhasználóknak kiosztott jogosultságokról a rendszergazdának nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdával közösen felül kell vizsgálni. Frissíteni kell továbbá, bármilyen módosítást követően.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 68 / 89



A hozzáférési jogosultságok megszüntetéséről az alábbi esetekben szükséges intézkedni:

- a) dolgozó kilépése esetén,
- b) ha a Hivatal munkavállalóját a Hivatalon belül áthelyezték,
- c) ha a munkavállaló szervezeti egységen belül marad, de a munkaköre jelentősen megváltozott,
- d) ha a külső partner szerződése lejárt vagy megszűnt,
- e) tartós betegség, távollét, illetve helyettesítés esetén,
- f) visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.

A jogosultságok visszavonását adott rendszertől függően a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor végzi.

3.8.2 Felhasználói fiókok kezelése

A Hivatallal szerződéses jogviszonyban álló szereplők, a szerződésben meghatározott szerepkörökre kaphatnak jogosultságot. Kizárólag csak az *1.6.3. A személyek ellenőrzése* fejezet követelményeinek teljesülése esetén lehet jogosultságot kiosztani.

Az elektronikus információs rendszer felhasználói fiókjait és típusait (ahol megengedett) a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor határozza meg.

A felhasználói fiókok kezelése a rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor feladata. Meghatározzák a munkacsoportokhoz/ szerepkörökhöz tartozó felhasználói feltételeket.

Meghatározzák és dokumentáltan kezelik az elektronikus információs rendszerhez hozzáférési jogosultsággal rendelkezők körét, a munkacsoportokhoz/ szerepkörökhöz tartozó jogosultságokat, valamint (szükség esetén) a felhasználói fiókok további jellemzőit.

Hozzáférést csak a szükséges mértékben és időtartamra lehet engedélyezni, figyelembe véve a szerepkörökhöz tartozó feladatokat. Tartományba léptetett eszközök esetén célszerű beállítani a fiókok automatikus tiltását, maximum 5 rontott jelszó, illetve 2 hét inaktivitást követően.

A rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a Hivatal, valamint a központi szolgáltató által meghatározott feltételekkel összhangban.

A rendszergazda, vagy a központi szolgáltató által kijelölt adminisztrátor ellenőrzi a felhasználói fiókok használatát.

A rendszergazdát, vagy a központi szolgáltató által kijelölt adminisztrátort értesíti kell, ha:

- a) a felhasználói fiókokra már nincsen szükség,
- b) a felhasználók kiléptek vagy áthelyezésre kerültek,
- c) az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

A munkaállomásokon a felhasználóknak nem lehet adminisztrátori joguk.

Minden felhasználónak saját felhasználói azonosítóval kell rendelkeznie, az ehhez szükséges jelszavakat az alkalmazott jelszó szabályoknak megfelelően kell képezni. Az első bejelentkezést követően a felhasználóknak meg kell változtatniuk a jelszavukat, a jelszó szabályokat figyelembe véve.

Tiltani kell a csoportos felhasználói azonosítók használatát.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 69 / 89



A Hivatalnál több szerepkört betöltő személyek jogosultságai, a szerepköröknek megfelelően külön-külön kell, hogy kialakításra kerüljön.

A rendszergazda meghatározott gyakorisággal (a központi szolgáltató által kijelölt adminisztrátor a központi szolgáltató előírásai alapján), minimálisan évente felülvizsgálja a felhasználói fiókokat, ellenőrzi a fiókkezelési követelményekkel való összhangot.

3.8.3 Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer és a szabályzatok közötti összhangot szükséges megteremteni annak érdekében, hogy az elektronikus információs rendszer érvényesítse a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.8.4 A felelősségek szétválasztása

A Hivatal meghatározza a felhasználók szerepköreit és az azokhoz tartozó feladatokat, felelősségeket, és ezt dokumentáltan a munkaköri leírásokban (külső szerződött partner esetében a szerződésben) kezeli. Minden szerepkörhöz külön-külön meghatározza a hozzáférés jogosultságait, a felelősségek szétválasztása érdekében.

3.8.5 Legkisebb jogosultság elve

A hozzáférés biztosításának alapelvei;

- hozzáférést csak a szükséges mértékben és időtartamra szabad engedélyezni, olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében indokolt. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is;
- a felhasználónak a tőle elvárható gondossággal kell eljárnia az adatkezelés során. Meg kell akadályoznia a kapott hozzáférési jogokkal való visszaélést azáltal, hogy megőrzi a hozzáférési adatok titkosságát;
- a Hivatal által használt rendszerekhez, rendszerelemekhez csak a jogosultságkezelési folyamat betartásával adható hozzáférés;
- külső partnerek (vállalkozók, hatóságok stb.) vonatkozásában a Hivatal rendszereihez, rendszerelemeihez való hozzáférés csak szerződés alapján biztosítható;
- külső partnerek esetén a hozzáférési jog maximum a szerződés lejáratáig adható;
- a Hivatal rendszereihez, rendszerelemeihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés, megállapodás vagy titoktartási nyilatkozatok alapján gyakorolhatják;
- a hozzáférési jogosultságokkal történő visszaélés gyanúja esetén a Hivatal minden dolgozója és szerződéses partnere köteles értesíteni az információbiztonsági felelőst,
- a felhasználó elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett, vagy végeztek;
- az elektronikus információs rendszerekről és eszközökről kizárólag a jegyző, az általa kijelölt személy vagy az információbiztonsági felelős szolgáltathat adatokat;
- jelen szabályzattól eltérni az információbiztonsági felelős engedélye esetén lehetséges (ilyen esetekben is szükséges a folyamat megfelelő dokumentálása).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 70 / 89



A központi szolgáltató rendszereiben szintén törekedni kell a legkisebb jogosultság kiosztására a felhasználók körében. Az adminisztrátornak a jogosultságok kiosztásánál javasolt figyelembe vennie a *Szervezeti és Működési Szabályzatot*, amely nem kerülhet ellentmondásba sem a Hivatal IBSZ-vel, sem a központi szolgáltató előírásaival.

3.8.6 Jogosult hozzáférés a biztonsági funkciókhoz

A Hivatal a szerepköröknek megfelelően hozzáférési jogosultságokat biztosít a biztonsági funkciókhoz és biztonságkritikus információkhoz.

3.8.7 Nem privilegizált hozzáférés a biztonsági funkciókhoz

A Hivatal kötelezővé teszi, hogy a Hivatal biztonsági funkcióihoz vagy biztonságkritikus információihoz hozzáférési jogosultsággal rendelkező felhasználói, a nem biztonsági funkciók használatához ne a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

3.8.8 Privilegizált fiókok

A Hivatal az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

Minden olyan jogosultság ebbe a körbe tartozik, amely a felhasználói jogoknál több jogot jelent (pl. backup operátor, rendszeradminisztrátor stb.). Főbb szabályok a privilegizált jogosultságokkal kapcsolatban:

- a rendszerek adminisztrációjához kellő rendszergazdai jogosultságot (előjogokat) csak a rendszergazdai feladatkörben foglalkoztatott munkatárs kaphat és csak a feladatkörnek megfelelő rendszerekre érvényesen. A rendszergazdai jogosultságok (előjogok), ahol ennek kifejezett műszaki akadálya nincsen, legyenek egyértelműen személyhez kötöttek, a csoportos azonosítók használata mindenképpen kerülendő;
- a rendszergazda az előjogokat biztosító azonosítóját csak a munkavégzéshez feltétlenül szükséges mértékben használja, minden más esetben a normál felhasználói azonosítójával dolgozzon;
- mindenképpen kerülni kell olyan rendszerek üzembeállítását, amelyek nem rendszergazda munkakörben dolgozó felhasználók rendszergazdai jogosultságokkal történő felruházását igényelnék;
- a központi szolgáltató egy esetleges biztonsági incidens során az adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti. Biztonsági audit során, ha az indokoltnál magasabb hozzáférés állapítható meg egyes felhasználók esetében, annak oka jegyzőkönyvben kell, hogy szerepeljen. Általánosságban megállapítható, hogy a jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

3.8.9 A munkaszakasz zárolása

A rendszergazdának a munkaállomásokon szükséges automatikus képernyővédelmet beállítani, hogy kizárásra kerüljön az illetéktelen használat. A képernyővédelmet úgy kell beállítani, hogy felhasználói inaktivitást követően 2 percen belül automatikusan zárolja a munkaállomást.

Az ismételt bejelentkezés kizárólag a felhasználó azonosításával és hitelesítésével történhet (felhasználónév és jelszó megadása).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 71 / 89



3.8.10 Képernyőtakarás

A rendszergazda úgy állítja be a munkaállomást, hogy a munkaszakasz zárolásakor a képernyőn korábban látható információ egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - legyen eltakarva.

3.8.11 A munkaszakasz lezárása

A rendszergazda a Hivatal saját hatókörébe tartozó elektronikus információs rendszereket úgy állítja be, hogy az automatikusan lezárja a munkaszakaszt a Hivatal által meghatározott feltételek vagy a munkaszakasz szétkapcsolást igénylő események megtörténte után.

3.8.12 Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

A Hivatalban jelenleg nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

Amennyiben a Hivatal ezt mégis engedélyezné, kijelöli azokat a felhasználói tevékenységeket, amelyeket azonosítás vagy hitelesítés nélkül is végre lehet hajtani az elektronikus információs rendszerben, indokolja és dokumentálja a rendszerbiztonsági tervben, vagy más szabályzatban.

3.8.13 Vezeték nélküli hozzáférés

Abban az esetben, ha a Hivatal engedélyezi a vezeték nélküli kapcsolaton keresztüli csatlakozást az elektronikus információs rendszeréhez, eljárásrendjében megjelöli a konfigurálásra és csatlakozásra vonatkozó követelményeket, valamint technikai útmutatót ad ki. A vezeték nélküli hozzáférés feltételeként engedélyezési eljárást folytat le, felhasználói korlátozásokat vezet be.

3.8.14 Mobil eszközök hozzáférés ellenőrzése

A rendszergazdának a magánhasználatú mobil eszközöknek a Hivatal helyi hálózatához vagy a munkaállomásaihoz, a hivatali célú elektronikus információs rendszerlemeihez csatlakoztatását a helyi beállításokban szükséges korlátozni.

3.8.15 Titkosítás

A Hivatal a mobil eszközök adattároló egységein lehetőség szerint hardveres titkosítást, más esetben fizetett szoftveres titkosítást alkalmaz, a mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, illetve az információk hozzáférhetetlenné tételére. Továbbá a mobil eszközöket hitelesítési eljárással védi (pl. BIOS jelszó).

3.8.16 Külső elektronikus információs rendszerek használata

A Hivatal meghatározza, hogy milyen feltételek és szabályok betartása mellett jogosult a felhasználó külső rendszerből hozzáférni a Hivatal saját hatókörébe tartozó elektronikus információs rendszeréhez. Külső rendszerből való hozzáférés esetén is biztosítani kell azokat a feltételeket, amelyeket a Hivatal a Hivatali belső rendszerek biztonsága érdekében megvalósít (pl. naprakész víruskereső, naprakész operációsrendszer, tűzfal, biztonságos protokoll használat stb.)

A Hivatal meghatározza, hogy külső elektronikus információs rendszerek segítségével hogyan jogosult a felhasználó feldolgozni, tárolni vagy továbbítani a Hivatal által ellenőrzött információkat.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 72 / 89



A központilag biztosított szakrendszerek esetében nem megengedett a külső rendszerből való hozzáférés.

3.8.17 Korlátozott használat

A Hivatal csak abban az esetben engedélyezi a jogosult felhasználóknak külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az által ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha:

- a) előzetesen ellenőrizte a szükséges biztonsági intézkedések meglétét a külső rendszeren saját szabályzóinak megfelelően,
- b) vagy, ha jóváhagyott kapcsolat van az elektronikus információs rendszerek között,
- c) vagy, ha megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

3.8.18 Hordozható adattároló eszközök

A Hivatal szükség szerint korlátozza vagy megtiltja az ellenőrzött hordozható tárolóeszközök használatát külső elektronikus információs rendszerben is jogosultsággal rendelkező felhasználók számára.

3.8.19 Információ megosztás

A Hivatal elősegíti az információmegosztást azzal, hogy engedélyezi a jogosult felhasználóknak eldönteni, hogy a megosztásban résztvevő partnerhez rendelt jogosultságok megfelelnek-e az információra vonatkozó hozzáférési korlátozásoknak, olyan meghatározott információmegosztási körülmények esetén, amikor felhasználói megítélés szóba jöhet (tehát a jogosult felhasználó eldöntheti, hogy akivel az információt megosztaná, az jogosult-e arra, hogy az információ birtokába jusson). Lehetőség szerint automatizált mechanizmusokat vagy kézi folyamatokat alkalmaz arra, hogy segítséget nyújtson a felhasználóknak az információmegosztási vagy együttműködési döntések meghozatalában.

3.8.20 Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Hivatal a publikus weboldalt.

A Hivatal kijelöli a weblap tartalom felelőst, aki a jogszabályi követelményeknek és a Hivatal belső szabályainak megfelelően a tartalom feltöltési és karbantartási feladatok ellátásáért felelős. Tilos a hatályos törvénybe, jogszabályba, belső szabályzatba ütköző, vagy a Hivatal érdekeit, a jó ízlést és közérkölcset sértő tartalmat közzétenni.

A Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatokat közöl, a települést mutatja be, aktuális híreket és információkat közöl az állampolgárok számára.

Havonta legalább egyszer, illetve adatfeltöltés után szükséges a honlapot átvizsgálni, és az esetlegesen nem nyilvános adattartalmakat eltávolítani.

Az információbiztonsági felelős feladata, hogy a nyilvánosan közzé tehető adatokról oktatást tartson, a nem nyilvános adattartalmak közzétételének elkerülése érdekében.

Amennyiben a Hivatallal szerződéses jogviszonyban álló külső szolgáltató rendelkezik technikai hozzáféréssel, számára a jegyző vagy megbízottja adhat át dokumentált módon írásban – nyilvános közzétételre szánt, ellenőrzött – információt.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 73 / 89



3.9 RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

3.9.1 Rendszer- és információsértetlenségre vonatkozó eljárásrend

Az elektronikus információs rendszerek, illetve az adatok sértetlenségére vonatkozóan a következő eljárásrendet kell alkalmazni. Az eljárásrend célja, hogy a Hivatal által használt elektronikus információs rendszerben, rendszerelemekben bekövetkezett változások úgy, mint: hibajavítás, frissítés, új hardver üzembe helyezése, vagy a rendszerben bekövetkezett bármi nemű módosítás esetén, az információsértetlenséget biztosítani tudja.

A Hivatal saját hatáskörében az előbb felsorolt változtatásokat, kizárólag a rendszergazda végezheti.

A rendszergazdának kell gondoskodnia arról, hogy a rendszer működéséhez szükséges alkalmazások, programok mindig naprakészen működjenek. Továbbá gondoskodnia kell a működéshez szükséges hardver elemekről, ezek bővítéséről, cseréjéről, selejtezéséről.

Az ehhez szükséges frissítéseket, konfigurációs beállításokat/módosításokat/javításokat tervezetten kell elvégeznie.

A módosítások folyamán gondoskodnia kell arról, hogy a felhasználói adatok ne sérüljenek, és illetéktelenek ne tudjanak hozzáférni.

A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni, illetve a módosításoknak megfelelően a dokumentációkat is frissíteni kell. (pl. frissítési/telepítési útmutatók, konfigurációs beállítások).

Központi szolgáltatás esetében, a központi szolgáltató határozza meg, hogy ki jogosult fejlesztői, üzemeltetői, működtetői, tesztelési tevékenységet végezni a központi rendszer tekintetében.

3.9.2 Hibajavítás

A műszaki sebezhetőségek ellenőrzés alatt tartása érdekében, a rendszerek műszaki sebezhetőségeit jelentős késedelem nélkül, tervszerűen és ellenőrzött módon ki kell javítani a gyártók által biztosított frissítések (pl operációs rendszer szintű patchek, BIOS, ROM, FIRMWARE), patchek, megkerülő megoldások használatával. A felhasználók haladéktalanul jelzik felettesüknek vagy a rendszergazdának, ha az informatikai rendszerben fennakadást, leállást, zavart észlelnek. Az ellenőrzést, azonosítást, javítást és jelentést a rendszergazda biztosítja.

Az operációs rendszerek vagy üzletileg kritikus alkalmazások verziófrissítése csak megtervezett módon történhet meg. A biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül telepíteni szükséges (a frissítések történhetnek automatikusan is az adott operációs rendszer frissítési beállításainak megfelelően).

Egyéb biztonsági kockázatot nem jelentő frissítéseket csak abban esetben kell telepíteni, ha azok üzleti szempontból lényeges hibák, sérülékenységek kijavítását, funkcióbővítést eredményeznek.

A változást előzetesen tesztelni kell egy a Hivatali környezethez hasonló teszt rendszerben minden kritikus szolgáltatás és alkalmazás vonatkozásában a kompatibilitás, az alkalmazások helyes működése szempontjából. A változást követően ellenőrizni kell a változás eredményét és hatását.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 74 / 89



A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni, illetve a módosításoknak megfelelően a dokumentációkat is frissíteni kell. (pl. frissítési/telepítési útmutatók, konfigurációs beállítások).

A központi szolgáltatású rendszer esetében (ASP) a felhasználóknak lehetőségük van a rendszerrel kapcsolatos észrevételek, hibák bejelentésére. Ennek a bejelentési felülete a hibabejelentő rendszer.

3.9.3 Kártékony kódok elleni védelem

Információ feldolgozó rendszerek biztonságos üzemeléséhez és a feldolgozott információ biztonságos kezeléséhez, a sértetlenség és a bizalmasság megőrzéséhez nélkülözhetetlen, a hatékony védekezés a vírusok és a kémprogramok ellen, ezért:

- a) minden szolgáltatás fejlesztéséhez, üzemeltetéséhez, támogatásához stb. használt asztali és mobil számítógépet, valamint szervert védeni kell a vírusoktól folyamatosan frissülő vírusvédelmi rendszer működtetésével. Ezen felül, ha műszakilag lehetséges és információbiztonsági szempontból indokolt egyéb mobil eszközökre is megfelelő védelmet kell biztosítani (okos telefonok);
- b) a vírusvédelmi rendszer kiválasztása, és megfelelőségének ellenőrzése, a rendszergazda feladata;
- c) a kiválasztásnál figyelembe kell venni, hogy a védendő rendszer eszközeinek teljesítményét csak elfogadható mértékben korlátozza, a hatékony munkavégzést ne gátolja;
- d) a vírusvédelmi rendszert úgy kell üzemeltetni, beállítani, és szabályokat (házirendeket) meghatározni, hogy az akadályozza meg a vírusok adathordozón, vezetékes vagy vezeték nélküli hálózaton, elektronikus levelezésben, vagy internet használat során történő bejutását a rendszerekbe;
- e) a kártékony kódok elleni védelmet úgy kell beállítani, hogy rendszeres ellenőrzéseket hajtson végre a belépési/kilépési pontokon, amikor a fájlokat letöltik, megnyitják, vagy elindítják;
- f) az esetlegesen mégis bejutott vírusok kártételének meggátolása céljából a rendszereket lehetőleg automatikusan, a felhasználó beavatkozását nem igénylő módon, heti rendszerességgel át kell vizsgálni, és a bejutott kártékony kódokat meg kell semmisíteni;
- g) a kártékony kódok észlelése és megsemmisítése során jelentkező esetleges téves riasztásokat rendszergazda ellenőrzi;
- h) a rendszer konfigurálása a rendszergazda, a vonatkozó házirendek kialakítása, azok megfelelő működésének ellenőrzése és dokumentálása az információbiztonsági felelős feladata;
- i) a szolgáltató által kiadott frissítéseket a rendszergazda a konfigurációkezelési eljárásnak megfelelően hajtja végre;
- j) a Hivatal minden munkatársa köteles az általa használt eszközökön a vírusvédelmet használni, azt semmiféle okból ki nem kapcsolhatja;
- k) kártékony kód észlelése esetén a kártékony kódokat azonnal karanténba kell helyezni, és jelezni kell a rendszergazdának;

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 75 / 89



- l) a rendszergazdának jelentenie kell az információbiztonsági felelős felé a kártékony kódok jelenlétét a rendszerben;
- m) a kártékony kódok megsemmisítése során, figyelembe kell venni annak, a rendszer rendelkezésre állására való kihatását;
- n) a kártékony kódok elleni intézkedéseket az információbiztonsági felelősnek dokumentáltan kell kezelnie és jelentenie kell azt a Kormányzati Eseménykezelő Központ felé.

Az elektronikus postafiókba érkező, ismeretlen feladótól származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldeményekkel – a fennálló vírusveszély miatt – fokozott óvatossággal kell eljárni. Gyanús küldemény érkezésekor, illetve a vírusvédelmi rendszer riasztása esetén a csatolmányt megnyitni tilos. Tilos lánclevelek indítása vagy továbbítása.

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

Az internethasználatra vonatkozó szabályokat az 1.6.9. *Viselkedési szabályok az interneten* fejezet tartalmazza.

További szabályokat a Hivatal *Vírusvédelmi szabályzata* tartalmaz.

3.9.4 Automatikus frissítés

A kártékony kódok elleni védelmi mechanizmusokat a rendszergazda úgy konfigurálja, hogy a víruskereső adatbázis automatikusan frissüljön.

3.9.5 Az elektronikus információs rendszer felügyelete

A rendszergazda a rendszer megfelelő működése érdekében figyelemmel kíséri az elektronikus információs rendszer, rendszerlemeinek rendelkezésre állását. Meghibásodás/rendszer hibaüzenet esetén meg kell oldania a problémát. Ellenőrzi, és valós esetben javítja a felhasználatól érkezett észrevételeket (pl. mikor a felhasználó lassúnak észleli a rendszert), majd ezeket kommunikálja feléjük.

Azonosítja az elektronikus információs rendszer jogosulatlan használatát, és védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. Az üzembiztonság érdekében a kiszolgálók operációs rendszereinek telepítőkészleteit tartalék adathordozón is tárolja, valamint rendszeresen menti az operációs rendszer beállításait.

Minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel, a rendszergazda erősíti a rendszer felügyeletét.

Meghibásodás/nem megfelelő üzemelés, esetleges támadás esetén közvetlenül az észlelést követően a rendszer felügyeletéből gyűjtött információkat az információbiztonsági felelős felé kommunikálja.

3.9.6 Biztonsági riasztások és tájékoztatások

Az információbiztonsági felelős folyamatosan figyeli a Kormányzati Eseménykezelő Központ által a fenyegetésekről, sebezhetőségekről, kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket. Folyamatosan figyelemmel kíséri továbbá a Nemzeti Elektronikus Információbiztonsági Hatóságtól érkező értesítéseket, szükség esetén

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 76 / 89



belső biztonsági riasztást és figyelmeztetést ad ki, illetve a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez.

Az informatikai rendszert érintő biztonsági eseményeket a Hivatal e központ felé köteles jelenteni. Az információcsere és a központ kárenyhítő intézkedései során a Hivatal együttműködni köteles. Az ellenintézkedéseket a Hivatal az *1.5.6 Biztonsági eseménykezelési terv* fejezetnek megfelelően végzi el.

Az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivatalnál, de kizárni sem lehet). Ennek a bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi.

Az információbiztonsági felelős a biztonsági riasztásokat és az azzal kapcsolatos intézkedéseket elektronikus nyilvántartásban vagy egyéb dokumentumban rögzíti.

3.9.7 Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi az információ belépési pontok érvényességét.

3.9.8 A kimeneti információ kezelése és megőrzése

A Hivatal az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

3.10 NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.10.1 Naplózási eljárásrend

Azért, hogy a Hivatal elektronikus információs rendszeréről, rendszerelemeiről naprakész információk álljanak rendelkezésre, gondoskodni kell a rendszer naplózási beállításairól. A naplózási beállítások elvégzése a rendszergazda feladata és felelőssége.

A naplózási beállításokat legalább évente egyszer a rendszergazdának kell felülvizsgálni és szükség esetén módosítani, illetve akkor, ha az elektronikus információs rendszerben változás történik.

Ha a Hivatal az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja, a naplózás és elszámoltathatóság követelményeit ezen elemek és funkciók tekintetében kell teljesíteni.

Amennyiben külső fél végzi a tevékenységet, a szolgáltatás részleteit szerződésben kell rögzíteni.

3.10.2 Naplózható események

A rendszergazda – az információbiztonsági felelőssel egyeztetve – meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszert. Naplóeseményeket az adatvédelmi szabályok betartásával lehet gyűjteni és kiértékelni.

A naplózható események meghatározásakor a rendszergazda lehetőség szerint vegye figyelembe az érintett a naplófájlok várható nagyságát és megőrzési idejüket.

Az adminisztrátori tevékenységeket a rendszerek meglévő naplózási szolgáltatásai rögzítik, ezekről külön gondoskodni jelenleg nem szükséges.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 77 / 89



A Hivatal által használt rendszerek legalább az alábbiakat naplózzák;

- a) a felhasználók be/ki jelentkezését és a profilmódosításokat,
- b) a rendszergazdai jogosultsággal végzett tevékenységeket,
- c) az adatbázisain történő változásokat,
- d) a konfigurációkezelésnek és a változáskövetésnek megfelelően a konfigurációs beállításokat,
- e) a rendszerben bekövetkezett hibákat, eseményeket,
- f) határvédelem logolása,
- g) vírusbeállítások.

A rendszergazdának és az információbiztonsági felelősnek közösen kell felülvizsgálnia a naplózott eseményeket, hogy azok elegendők-e, egy esetlegesen bekövetkezett biztonsági eseményt követő vizsgálat során.

3.10.3 Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele. (pl. felhasználók azonosítója, esemény időpontja, hibakód, vírustámadás stb).

3.10.4 Időbélyegek

A szerverek, a munkaállomások és a tűzfalak belső óráját a naplóbejegyzések követhetősége érdekében úgy kell beállítani, hogy azok az internetről automatikusan szinkronizálódjanak a szokásos internetes időszolgáltatások (NTP) egyikéről. Az óraszinkronizáláshoz szükséges protokoll átengedését a tűzfalakon biztosítani kell.

3.10.5 A naplóinformációk védelme

Az elektronikus információs rendszert, szervereket és munkaállomásokat úgy kell konfigurálni, hogy csak a rendszergazdai jogosultsággal rendelkezők tudjanak a naplóinformációkhoz hozzáférni. Továbbá az adatvédelemmel kapcsolatban az e szabályzatban foglaltak alapján kell mindenkor eljárni.

3.10.6 A naplóbejegyzések megőrzése

A rendszergazda gondoskodik a naplóbejegyzések megőrzéséről, hogy azok segítségül szolgáljanak az esetleges biztonsági események bekövetkeztét követő kivizsgáláskor. A naplózási szolgáltatásokat úgy kell beállítani, hogy azok lehetőség szerint (amennyiben a rendelkezésre álló tárhely lehetővé tesz) legalább 1 évre visszamenőleg rendelkezésre álljanak.

3.10.7 Naplógenerálás

Az elektronikus információs rendszernek biztosítani kell a naplóbejegyzések előállítási lehetőségeit a 3.10.2 *Naplózható események* fejezetben meghatározottaknak megfelelően.

Lehetővé kell tegye, hogy a rendszergazda kiválassza, mely naplózható események legyenek naplózva az információs rendszer egyes elemeire.

A rendszernek biztosítani kell a naplóbejegyzések előállítását a 3.10.2 *Naplózható események* fejezetben meghatározottak szerinti eseményekre, a 3.10.3 *Naplóbejegyzések tartalma* pontban meghatározott tartalommal.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 78 / 89



Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 79 / 89



3.11 RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM

3.11.1 Rendszer- és kommunikáció védelmi eljárásrend

A Hivatalon belüli kommunikáció, információáramlás célja, hogy a munkatársak hozzájussanak mindazon információkhoz, mely a Hivatal hatékony működéséhez szükséges. Különös tekintettel vonatkozik ez a szakmai jellegű információk, információbiztonsági előírások átadására, eljuttatására a Hivatal minden érintett munkatársa számára.

A Hivatalon belül az információk átadása az alábbi módszerekkel történhet:

- a) értekezletek, megbeszélések,
- b) elektronikus levelezési rendszerben küldött üzenetek,
- c) megosztott mappák.

Az értekezlet(ek)ről feljegyzés/jegyzőkönyv készül, amelyek esetében minden munkatárs saját felelőssége, hogy az értekezleten elhangzott információkat bizalmasan kezelje, munkája során alkalmazza, és a feladatokat végrehajtsa.

Az információbiztonsági felelős feladata, hogy minden érintett szereplővel kapcsolatban, a jelen szabályzatban leírt kommunikációra és rendszervédelemre vonatkozó biztonsági követelmények teljesülését ellenőrizze, ide értve az 1.6.9. *Viselkedési szabályok az interneten* fejezetben leírtakat is.

Jelen szabályozások felülvizsgálata és indokolt esetben történő frissítése az információbiztonsági felelős feladata, legalább évente egyszer.

A szolgáltatónak gondoskodnia kell a biztosított szolgáltatás elvártak szerinti működéséről, ehhez kártékony szoftvereket és illetéktelenek általi behatolásokat elhárító biztonsági határvédelmi megoldásokat, szükség esetén pedig a megfelelő incidenskezelési és analízisre szolgáló eszközöket kell alkalmaznia.

A szolgáltató feladata (ahol értelmezhető):

- a) virtuális gépek alkalmazása esetén a virtuális gépek más gépek felől, a fizikai hosztról és hálózat felől érkező támadások elleni védelem;
- b) nyomon követni a hálózati erőforrásokhoz, alkalmazásokhoz és adatokhoz való hozzáféréseket;
- c) az alkalmazási szintig elérő sebezhetőség esetén az alkalmazás-specifikus védelmi megoldásokat biztosítani (pl. levelezőprogram, spamszűrő, böngésző biztonsági frissítése);
- d) az alkalmazói szoftverek alatti rétegeket érintő sebezhetőségi pontokat megfelelő eszközökkel védeni (tűzfalak, böngészők frissítése stb.);
- e) az alkalmazás biztonságosan futtatható üzemmódra konfigurálása (pl. titkosítás kliens-szerver kommunikációban), és integrálása az alkalmazást igénybe vevő meglévő technikai biztonsági intézkedéseivel (azonosítás, hitelesítés, engedélyezési folyamatok). Az erre szolgáló technikai eszközök a széles körben használt szabványoknak megfelelőek legyenek (SSH, SFTP, SSL/TSL).

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 80 / 89



3.11.2 A határok védelme

Az informatikai hálózati határvédelem során a Hivatal informatikai hálózatában az internetkijárat, valamint minden külső, nem megbízhatónak ítélt hálózat felé történő kommunikáció során a belső hálózat és az ott elhelyezkedő elektronikus információs rendszerek, rendszerelemek és adatok védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni.

Gondoskodni kell a hálózat fizikai elemeinek védelméről, így különösen:

- vezetékek és végpontok illetéktelenek általi hozzáféréseinek megakadályozásáról,
- a vezeték nélküli kapcsolatok megfelelő titkosításáról,
- az eszközhöz való illetéktelen hozzáférés megakadályozásáról.

Az elektronikus információs rendszernek felügyelni és ellenőrizni kell a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban kell elhelyezni, elkülönítve a belső Hivatali hálózattól. Az elektronikus információs rendszer csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódhat külső hálózatokhoz, vagy külső elektronikus információs rendszerekhez.

3.11.3 Kriptográfiai kulcs előállítása és kezelése

Titkosítás használata esetén a szolgáltatónak kriptográfiai kulcsok menedzselésére, védelmére, az azokhoz való hozzáférési szabályokra vonatkozó eljárásrendet kell kidolgoznia és alkalmaznia, igazodva az alkalmazott kulcsok jellegéből következő technikai követelményekhez (pl. nyilvános kulcsú titkosítás esetén a kulcspároknak megfelelő kezelése, szimmetrikus kulcsú titkosításnál a kulcskiosztás bizalmassága, az ezeket garantáló technikai eszközök igénybe vételével).

3.11.4 Kriptográfiai védelem

A specifikus technológiára (például kriptográfia, nyilvános kulcsú infrastruktúrán (PKI) alapuló hitelesítési eljárás) vonatkozó biztonsági intézkedések csak akkor alkalmazandók, ha ezeket a technológiákat használják az elektronikus információs rendszerben, vagy előírják ezek használatát.

A szolgáltató, ha az szükséges, szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

3.11.5 Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszernek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását.

A Hivatal nem alkalmaz a központi szolgáltatású elektronikus információs rendszerben távolról elérhető eszközöket, következésképpen nincs lehetőség távoli aktiválásra.

3.11.6 Elektronikus információs rendszeren keresztüli hangátvitel (ún. VoIP)

Az elektronikus információs rendszerben okozható károk felmérésére, megakadályozására a VoIP technológiákhoz szükség esetén használati korlátozásokat kell bevezetni, megvalósítási útmutatót kell kiadni. Felügyelni és ellenőrizni kell a VoIP használatát az elektronikus információs rendszeren belül.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 81 / 89



3.11.7 A folyamatok elkülönítése

Az elektronikus információs rendszernek elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamatra, vagyis ajánlott a szakrendszeri munkaállomásokat különálló védett hálózatba elhelyezni (vlan), így védve a többi hálózati támadástól.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 82 / 89



4 KAPCSOLÓDÓ MELLÉKLETEK

Melléklet száma	Melléklet megnevezése
1. számú melléklet	Elektronikus információs rendszerek biztonsági osztálya - a Hivatal biztonsági szintje
2. számú melléklet	Titoktartási nyilatkozat
3. számú melléklet	Megismerési nyilatkozat-ITB



5 ALAPFOGALMAK

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

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

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

Adatfeldolgozó: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki/amely az adatkezelő részére adatfeldolgozást végez.

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

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

Adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.

Alapkonfiguráció (baseline): egy adott időpillanatban a konfigurációs elemek jellemzőinek és azok kapcsolatának állapota, amely hivatkozási alapként felhasználható egy későbbi időpontban.

Archiválás: a Hivatali alaptevékenység szempontjából lényeges azon információk és dokumentumok tárolásának célját szolgálja, amelyekre a folyamatban lévő feladatok teljesítéséhez már nincs szükség, de jogi követelmények miatt vagy más célokra bizonyos időpontig (tárolási időtartam) megőrzendők.

Archivált adatok: információk és dokumentumok, amelyek archívumban kerültek elhelyezésre (Az archivált adatokat időállóan és igazolhatóan, alkalmas technológiák segítségével kell tárolni, pl. elektronikus, mágneses, optikai vagy nyomtatott formában.).

Archiválási rendszer: az archiváláshoz felhasznált, hardver- és szoftver-elemekből álló technikai rendszer.

Auditálás: előírások teljesítésére vonatkozó megfeleléségi vizsgálat, ellenőrzés.

Backup (adatmentés): az információknak az esetleges adatvesztéssel szembeni védelmét szolgáló kiegészítő tároló közegen történő mentése (Ily módon biztosítja a backup az információk rendelkezésre állását és integritását.).

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

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 84 / 89



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

Biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

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

Biztonsági szint: a Hivatal felkészültsége az Ibtv. törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

Biztonsági szintbe sorolás: a Hivatal felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

Elektronikus információs rendszer (az Ibtv. alkalmazásában): az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.

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

Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy: állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján, az Ibtv. hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon a feladatok ellátásával megbízott személy.

Elektronikus információs rendszerek védelméért felelős vezető: az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat alapján, az Ibtv. hatálya alá tartozó egyéb szervek esetében munkaköri leírásban vagy egyéb módon kijelölt vezető.

Életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam, az állapotváltozások meghatározott menete, amely jellemző az adott konfigurációs elem típusra.

Észlelés: a biztonsági esemény bekövetkezésének felismerése.

Éves továbbképzés: az elektronikus információs rendszerek védelméért felelős vezető, az információbiztonsági felelős és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy iskolarendszeren kívüli továbbképzése.

Felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre.

Felhasználó-felismerés: a felhasználó-felismerés a hálózatokon vagy alkalmazásokon belül a felhasználó egyértelmű beazonosítására szolgál. A felhasználó-felismeréshez felhasználói jogok hozzárendelésére kerül sor.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 85 / 89



Fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védetségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védetségét, biztonságát.

Fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

Globális kibertér: a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.

Illegális szoftverhasználat: egy számítógépes program jogtalan lemásolása és használata - megsértve a szerzői jogi törvényt, valamint a szerzőnek a szoftver licenz szerződésben leírt feltételeit (aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében büntetőjogi törvénybe ütköző cselekedetet követ el).

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

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

Jogosulatlan másolás: a szoftver licenz szerződés, amennyiben eltérően nem rendelkezik, a vevőnek csak egyetlen "biztonsági" másolat készítését engedélyezi, arra az esetre, ha az eredeti szoftver lemeze meghibásodna, vagy megsemmisülne (Az eredeti szoftver bármely további másolása jogosulatlan másolásnak minősül, és megsérti a szoftvert védő és használatát szabályozó licenz szerződést, valamint a szerzői jogi törvényt.).

Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kibertér megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését.

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

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

Kockázatkezelés: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása, intézkedések kiválasztására és végrehajtására a kockázat csökkentése érdekében.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 86 / 89



Kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

Korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni.

Kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat.

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

Létfontosságú információs rendszerelem: az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt létfontosságú rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.

Logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.

Magas biztonsági követelményű elektronikus információs rendszerek: jelen Informatikai biztonsági szabályzatban használt meghatározás szerint: 3-as vagy magasabb biztonsági osztályba sorolt elektronikus információs rendszerek (nem jogszabályi definíció).

Magyar kibertér: a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarország felé irányulnak, illetve Magyarország érintett benne.

Megelőzés: a fenyegetés hatása bekövetkezésének elkerülése.

Megőrzési időtartam: az azon időtartam, amely azzal a nappal záródik le, amelyen a törvényi vagy egyéb, a megőrzésre vonatkozó követelmény véget ér.

Munkahely: a felhasználók által használt végponti készülék és mobil adathordozó.

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

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

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

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 87 / 89



Sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat.

Sérülékenység vizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása.

Súlyos biztonsági esemény: olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.

Számítógépes eseménykezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)].

Szellemi tulajdon: törvények szerint egy eredeti számítógépes program az azt létrehozó személy vagy vállalat szellemi tulajdona és engedély nélküli másolásuk törvénybe ütköző cselekedet.

Szoftver licenz szerződés: egy adott szoftver esetében a licenz szerződés határozza meg a szerzői jog tulajdonosa által megengedett szoftverhasználat feltételeit (A szoftverhez adott licenz szerződésre külön utalás történik a szoftver dokumentációjában, vagy a program indításakor megjelenő képernyőn is. A szoftver ára tartalmazza a szoftver licenzét, és megfizetése kötelezi a vevőt, hogy a szoftvert kizárólag a licenz szerződésben leírt feltételek szerint használja.)

Tudás alapú hitelesítés: olyan hitelesítési eljárás, mód, mely során a felhasználó az általa mások előtt titokban tartott ismeret alapján hitelesíti a rendszerben magát (például jelszó, PIN kód).

Szervezet: az adatkezelést végző, illetve az adatfeldolgozást végző vagy végeztető jogi személy vagy egyéni vállalkozó, valamint az üzemeltető.

Teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem.

Üzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős.

Üzemzavar: az a helyzet, amelyben az üzleti folyamatok és/vagy üzleti rendszerek nem az előirányzottak szerint működnek. Az ebből adódó potenciális károk csekély mértékűek, mivel a feladat-teljesítés csak lényegtelen mértékben sérül (pl. Üzemzavar a helyi IT rendszerek lokalizált olyan mértékű hibája, amelyet a normál IT support a normál SLA időközön belül elhárítani képes. Az elhárítás ideje előre jelezhető és nem igényli üzleti oldali kényszerintézkedések, speciális eljárások használatát.).

Technikai számlák: a személyhez nem kötött felhasználó-felismeréseket technikai számláknak nevezzük. Elsősorban olyan funkciók és feladatok számára kerülnek bevetésre, amelyek nem igénylik a mindenkori felhasználó interaktív tevékenységét, hanem pl. az IT rendszerek közötti adatcseréhez szükségesek.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 88 / 89



Üzemeltető: az elektronikus információs rendszer vagy annak részeinek működtetését végzi.

Válság: összetett és átláthatatlan helyzet rendkívül magas kárpotenciállal, amely a Hivatal létét veszélyezteti. A meglévő vészhelyzeti tervek csak feltételesen hatékonyak. (A válság eseti, egyedi kezelést és azonnali ad-hoc döntések meghozatalát követelheti a Hivatal vezetésének bevonásával.).

Változat (variant): egy olyan konfigurációs elem, amely alapvetően egy adott konfigurációs elem szerint épül fel, attól csak kis mértékben tér el.

Védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés.

Vészhelyzet: az IT folyamatok, eszközök vagy rendszerek nem az előírásoknak megfelelően működnek és funkcióik nem állíthatóak helyre a szükséges időtartamon belül, és az ügymenet oly mértékben sérül, hogy nagy kárszint állhat elő, a Hivatal alaptevékenységének végzése, azonban nem kerül veszélybe (pl. üzemzavar elhárításának határideje nem látható előre, vagy a várható határidő túlmutat az SLA szerinti vállaláson és az üzemzavar következtében a kár enyhítése üzleti oldali lépések megtételét, rendkívüli intézkedéseket, vészhelyzeti forgatókönyvek aktiválását teszi szükségessé).

Zárt célú elektronikus információs rendszer: jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer.

Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

Bizalmassági besorolás	Oldalszám
Nyilvános	Oldal 89 / 89