

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

érvényes:

.....

Sárospatak Város Önkormányzat Képviselő-testülete

/2018. (V. 25.) határozatával jóváhagyta

Bizalmas, belső használatú dokumentum

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

Tartalom

Az Informatikai biztonsági szabályzat	5
Célok	5
Felülvizsgálat.....	6
Hatály	7
Hatásköri és illetékességi szabályok.....	7
Szerepkörök, tevékenységek, felelősségek	8
Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje	14
ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	16
1.1. HIVATALI SZINTŰ ALAPFELADATOK.....	16
1.1.1. Informatikai biztonsági szabályzat	16
1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy	16
1.1.3. Az intézkedési terv és mérföldkövei.....	17
1.1.4. Az elektronikus információs rendszerek nyilvántartása	17
1.1.5. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	18
1.2. KOCKÁZATELEMZÉS	20
1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend	20
1.2.2. Biztonsági osztályba sorolás	20
1.2.3. Kockázatelemzés	21
1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	24
1.3.1. Beszerzési eljárásrend	24
1.3.2. Erőforrás igény felmérés	25
1.3.3. Beszerzések.....	25
1.3.3.2. A védelem szempontjainak érvényesítése a beszerzés során	27
1.3.6. Külső elektronikus információs rendszerek szolgáltatásai	27
1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE.....	27
1.4.1. Ügymenet-folytonosságra vonatkozó eljárásrend	27
1.4.2. Ügymenet-folytonossági terv informatikai erőforrás kiesésekre.....	28
1.4.2.4. Kritikus rendszerelemek meghatározása	29
1.4.3. A folyamatos működésre felkészítő képzés	29
1.4.5.3. Üzletmenet folytonosság elérhetőség	30
1.4.7. Infokommunikációs szolgáltatások.....	30
1.4.7.2. Szolgáltatás prioritási rendelkezések.....	30
1.4.8. Az elektronikus információs rendszer mentései.....	30
1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása.....	31
1.5. A BIZTONSÁGI ESEMÉNYEK KEZELÉSE	31
1.5.1. Biztonsági eseménykezelési eljárásrend	31
1.5.4. A biztonsági események figyelése	32
1.5.6. A biztonsági események jelentése	32
1.5.7. Segítségnyújtás a biztonsági események kezeléséhez	33
1.5.8. Biztonsági eseménykezelési terv	34
1.5.9. Képzés a biztonsági események kezelésére	35
1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	35
1.6.1. Személybiztonsági eljárásrend	35
1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása.....	35
1.6.3. A személyek ellenőrzése	36
1.6.4. Eljárás a jogviszony megszűnésekor	37
1.6.5. Az áthelyezések, átirányítások és kirendelések kezelése	38
1.6.6. A Hivatallal szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	38
1.6.7. Fegyelmi intézkedések.....	38
1.6.8. Belső egyeztetés	39

1.6.9.	Viselkedési szabályok az interneten	40
1.7.	TUDATOSSÁG ÉS KÉPZÉS	43
1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel	43
1.7.2.	Képzési eljárásrend	43
1.7.3.	Biztonság tudatosság képzés	44
1.7.4.	Belső fenyegetés	45
1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	45
1.7.6.	A biztonsági képzésre vonatkozó dokumentációk	46
	FIZIKAI VÉDELMI INTÉZKEDÉSEK	46
2.1.	FIZIKAI ÉS KÖRNYEZETI VÉDELEM.....	46
2.1.2.	Fizikai védelmi eljárásrend.....	46
2.1.3.	Fizikai belépési engedélyek.....	48
2.1.4.	A fizikai belépés ellenőrzése.....	49
2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhöz.....	50
2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése	50
2.1.7.	A fizikai hozzáférések felügyelete.....	51
2.1.7.2.	Behatolás riasztás, felügyeleti berendezések.....	51
2.1.8.	A látogatók ellenőrzése.....	52
2.1.9.	Áramellátó berendezések és kábelezés	52
2.1.12.	Tűzvédelem	52
2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	52
2.1.15.	Be-és kiszállítás	53
2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése.....	54
2.1.19.	Karbantartók	55
2.1.19.3.	Időben történő javítás	55
	LOGIKAI VÉDELMI INTÉZKEDÉSEK.....	56
3.1.	ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK.....	56
3.1.1.	Engedélyezés	56
3.1.3.	Az elektronikus információs rendszer kapcsolódásai	56
3.1.3.2.	Belső rendszerkapcsolatok.....	56
3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	56
3.1.4.	Személybiztonság.....	56
3.2.	TERVEZÉS	57
3.2.2.	Rendszerbiztonsági terv	57
3.2.3.	Cselekvési terv.....	57
3.2.4.	Személyi biztonság.....	58
3.3.	RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	59
3.3.2.	A rendszer fejlesztési életciklusa.....	59
3.6.	KONFIGURÁCIÓKEZELÉS	60
3.6.1.	Konfigurációkezelési eljárásrend	60
3.6.2.	Alap konfiguráció	61
3.6.7.	Legszűkebb funkcionalitás.....	61
3.6.8.	Elektronikus információs rendszer elem leltár	62
3.1.3.3.	Duplikálás elleni védelem	63
3.6.10.	A szoftver használat korlátozásai	63
3.6.11.	A felhasználó által telepített szoftverek.....	63
3.7.	KARBANTARTÁS	64
3.7.1.	Rendszer karbantartási eljárásrend.....	64
3.7.2.	Rendszeres karbantartás.....	64
3.7.3.2.	Adathordozó ellenőrzés	65
3.7.4.	Távoli karbantartás	65

3.8.	ADATHORDOZÓK VÉDELME	66
3.8.1.	Adathordozók védelmére vonatkozó eljárásrend.....	66
3.8.2.	Hozzáférés az adathordozókhoz	66
3.8.4.	Adathordozók tárolása	66
3.8.5.	Adathordozók szállítása.....	66
3.8.5.2.	Kriptográfiai védelem	68
3.8.6.	Adathordozók törlése	68
3.8.7.	Adathordozók használata	68
3.8.7.2.	Ismeretlen tulajdonos.....	69
3.9.	AZONOSÍTÁS ÉS HITELESÍTÉS	69
3.9.1.	Azonosítási és hitelesítési eljárásrend.....	69
3.9.2.	Azonosítás és hitelesítés (hivatalon belüli felhasználók).....	69
3.9.4.	Azonosító kezelés.....	70
3.9.5.	A hitelesítésre szolgáló eszközök kezelése.....	70
3.9.5.2.	Jelszó (tudás) alapú hitelesítés	71
3.9.5.3.	Birtoklás alapú hitelesítés	72
3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	72
3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	72
3.9.8.	Azonosítás és hitelesítés (hivatalon kívüli felhasználók)	72
3.9.8.	Hitelesítésszolgáltatók tanúsítványának elfogadása	73
3.10.	HOZZÁFÉRÉS ELLENŐRZÉSE	73
3.10.1.	Hozzáférés ellenőrzési eljárásrend.....	73
3.10.2.	Felhasználói fiókok kezelése	74
3.10.3.	Hozzáférés ellenőrzés érvényesítése	75
3.10.5.	A felelőségek szétválasztása.....	75
3.10.6.	Legkisebb jogosultság elve.....	75
3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz.....	76
3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz.....	76
3.10.6.4.	Privilegizált fiókok	76
3.10.10.	A munkaszakasz zárolása	76
3.10.10.2.	Képernyőtakarás	76
3.10.11.	A munkaszakasz lezárása	77
3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	77
3.10.14.	Vezeték nélküli hozzáférés	77
3.10.15.	Mobil eszközök hozzáférés ellenőrzése	77
3.10.15.2.	Titkosítás.....	77
3.10.16.	Külső elektronikus információs rendszerek használata	77
3.10.16.2.	Korlátozott használat.....	78
3.10.16.3.	Hordozható adattároló eszközök.....	78
3.10.17.	Információ megosztás.....	78
3.10.18.	Nyilvánosan elérhető tartalom	78
3.11.	RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG	79
3.11.2.	Rendszer- és információsértetlenségre vonatkozó eljárásrend.....	79
3.11.3.	Hibajavítás	79
3.11.4.	Kártékony kódok elleni védelem	80
3.11.4.3.	Automatikus frissítés.....	81
3.11.5.	Az elektronikus információs rendszer felügyelete.....	81
3.11.6.	Biztonsági riasztások és tájékoztatások	81
3.11.10.	Bemeneti információ ellenőrzés.....	81
3.11.12.	A kimeneti információ kezelése és megőrzése.....	82
3.12.	NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	82
3.12.1.	Naplózási eljárásrend	82
3.12.2.	Naplózható események	82

3.12.3.	Naplóbejegyzések tartalma	83
3.12.8.	Időbélyegek	83
3.12.9.	A naplóinformációk védelme.....	83
3.12.11.	A naplóbejegyzések megőrzése.....	83
3.12.12.	Naplógenerálás.....	83
3.13.	RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM	83
3.13.1.	Rendszer- és kommunikáció védelmi eljárásrend	83
3.13.6.	A határok védelme	84
3.13.10.	Kriptográfiai kulcs előállítása és kezelése	85
3.13.12.	Együttműködésen alapuló számítástechnikai eszközök.....	85
3.13.22.	A folyamatok elkülönítése	86
	Kapcsolódó mellékletek	86
	Alapfogalmak	87

Az Informatikai biztonsági szabályzat

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban Ibtv.) kapott felhatalmazás alapján a Sárospatak Város Önkormányzat költségvetési szerveként működő Sárospataki Polgármesteri Hivatal (továbbiakban Hivatal) Informatikai biztonsági szabályzatát az alábbiakban határozza meg: - meghatározza a célokat, a szabályzat tárgyi és személyi hatályát;

- az elektronikus információbiztonsággal kapcsolatos szerepköröket;
- a szerepkörhöz rendelt tevékenységet;
- a tevékenységhez kapcsolódó felelősséget;
- az információbiztonság hivatalrendszerének belső együttműködését
- az elektronikus rendszerbiztonsággal kapcsolatos főbb területeket.

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

- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel,
- az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet
- az önkormányzati ASP rendszerről szóló 257/2016. (Vili. 31.) Korm. rendelettel,
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvénnyel.

Az önkormányzati ASP rendszerről szóló 257/2016. (Vili. 31.) Korm. rendelet értelmében a Hivatalnak csatlakoznia kell az önkormányzati ASP rendszer szakrendszereihez. A csatlakozás egyik feltétele, hogy a Hivatal teljesíti az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.) meghatározott követelményeket.

Mivel az ASP nem tartozik a hivatal saját hatókörébe, így az azzal kapcsolatos biztonsági követelmények megoszlának a Hivatal és a szolgáltató/üzemeltető között.

A Hivatallal szemben elvárt követelményekkel kapcsolatban figyelembe kell venni a Magyar Állam Kincstár tájékoztatóit (pl. Tájékoztató az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről). A Tájékoztató tartalmazza azokat a követelményeket, amelyeket kötelező jelleggel kell megvalósítani az ASP-hez történő csatlakozással. Ennek megfelelően jelen Informatikai biztonsági szabályzat az ASP csatlakozási projekt kapcsán kapott információk birtokában került felülvizsgálatra/elkészítésre. A jogszabály elvárja az önkormányzati ASP-hez történő csatlakozás után a szabályzat és az eljárásrendek szükség szerinti felülvizsgálatát, ismételt kihirdetését.

Célok

Az Informatikai biztonsági szabályzat célja, hogy a Hivatal számára értéket képviselő információk védelméről történő gondoskodást szabályozza. Az információ védelmének a célja, hogy biztosítsa az információ

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

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

szabályokat.

A szabályzatban szereplő követelményeket, rendelkezéseket és ajánlásokat a hatályos jogszabályok keretei között kell használni.

A szabályozás célja a következő:

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

Jelen szabályzat a Hivatal szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. A hatályos jogszabályokkal, a Hivatal működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek és az azokban kezelt adatok biztonságát. Tartalmazza a Hivatal elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van. Megfogalmazza azokat a biztonsági követelményeket is, amelyeket az önkormányzati ASP-hez való csatlakozással teljesíteni szükséges.

A Hivatal informatikai szolgáltatóival kötött szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen szabályzattal.

A célok elérése érdekében, az elektronikus információs rendszerek legmagasabb osztályba sorolt értékének megfelelően további eljárásrendek, részletszabályozások elkészítését a Hivatal vezetője rendelheti el, az elektronikus információs rendszerek biztonságáért felelős szakmai javaslatára. A részletszabályozásokat az elektronikus információs rendszerek biztonságáért felelős vagy a Hivatal vezetője által kijelölt személy készíti el, a rendszergazdával együttműködve, a Hivatal vezetője lépteti hatályba.

A Hivatal informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen szabályzattal.

Felülvizsgálat

A Hivatal az Informatikai biztonsági szabályzatot és hivatkozott eljárásrendjét folyamatosan fejleszti és tökéletesíti. 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.

A szabályzat felülvizsgálatának, módosításának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy vagy a Hivatal vezetője által kijelölt személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása a Hivatal vezetőjének hatásköre.

Hatály

Az Informatikai biztonsági szabályzat a Hivatal egészére vonatkozik, **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 biztosításával, a hatálya kiterjed a kezelt, keletkezett információkra. A tárgyi hatály kiterjed azokra a hardver és szoftver elemekre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező vagy felhasznált adatokat, azaz a szakrendszerek használatához szükséges felhasználói (önkormányzati) munkaadásokra, szoftverekre, nyomatkészítő eszközökre, kártyaolvasóra, és minden olyan egyéb eszközre, amely a munkavégzéshez szükséges, továbbá a rendszerelemek dokumentációira.

A szabályzat **személyi hatálya** kiterjed a Hivatal valamennyi, a Hivatal informatikai rendszeréhez hozzáféréssel rendelkező munkatársára, szerződéses partnerére (a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre), akik részt vesznek a Hivatalnál keletkező, tárolt, illetve továbbított adatok kezelésében. Harmadik személyekkel szemben a Hivatal a személyi hatályt szolgáltatói, vállalkozási vagy megbízási szerződések keretében érvényesíti.

A szabályzat **szervezeti hatálya** a Hivatal valamennyi olyan szervezeti egységére kiterjed, amely a Hivatal elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz. A szabályzat **területi hatálya** kiterjed a Sárospataki Polgármesteri Hivatalra, melynek tevékenysége kiterjed a településen működő nemzeti önkormányzatokra és Sárospatak és Térsége Önkormányzati Társulásra is.

Időbeni hatály, jelen Informatikai biztonsági szabályzat a Képviselő-testület által történő elfogadást követő napon lép hatályba.

Jelen szabályzat egyes követelményeinek hatályba lépési időpontja megfelel az adott követelményre a Hivatal Cselekvési tervében meghatározott határidőnek, összhangban a 2013. évi L. törvénnyel, a 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, a Hivatalra és az elektronikus információs rendszereire érvényes biztonsági osztályhoz és szinthez előírt határidővel.

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

Hatásköri és illetékességi szabályok

Az Informatikai biztonsági szabályzat és a kapcsolódó eljárásrendek, módszertanok, nyilvántartások kizárólag a Hivatal belső használatú dokumentumai, amelyeket a Hivatal elektronikus információs rendszerének felhasználói (a szabályzat személyi hatálya alá tartozók) kizárólag a rájuk vonatkozó követelmény szerint megismerhetnek, de azokat illetékteleneknek nem adhatják tovább.

Szerepkörök, tevékenységek, felelősségek

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 biztonság tudatos, proaktív viselkedésén is alapul.

Az egyes kontrolifolyamatokban 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 az Elektronikus információs rendszer biztonságáért felelős munkatárs felé jelenteni.

Az Információbiztonsági szabályzat (és kapcsolódó dokumentumai) előírásainak betartása, betartatása, illetve a napi szintű munkavégzés során annak alkalmazása a dokumentum személyi hatálya pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A szabályzat el nem olvasása nem mentesít a felelősség alól.

A Hivatali munkavégzéshez szükséges elektronikus információs rendszereket csak a hozzáférési jogosultság tudomásulvételét és a kapcsolódó szabályok megismerését igazoló nyilatkozat (Felhasználói titoktartási nyilatkozat) aláírása után lehet használatba venni.

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

Szerepkör	Főbb felelősségek, tevékenységek
az elektronikus információs rendszerek védelméért felelős vezető (a jegyző)	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 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, 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 kötelelmként teljesüljenek, 10. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelelmként 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, 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 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,

Szerepkör	Főbb felelősségek, tevékenységek
az elektronikus információs rendszerek biztonságáért felelős személy (szerződés alapján külső szakértő)	1. feladata ellátása során a Hivatal vezetőjének közvetlenül adhat tájékoztatást, jelentést, 2. felel a Hivatalnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért, 3. gondoskodik a Hivatal 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 Hivatal elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, eljárásrendeket, terveket 6. előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását, 7. véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Hivatal e tárgykört érintő szabályzatait és szerződéseit, 8. kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal, 9. a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet, 10. biztosítja a törvényben meghatározott követelmények teljesülését a Hivatal valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők, ha a Hivatal 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. a törvény szerinti feladatai és felelőssége a 10. pont szerinti esetekben más személyre nem átruházható, 12. jogosult az 10. pont szerinti közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni.
Elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (megbízott felelős és/vagy az elektronikus információs rendszer biztonságáért felelős személy)	1. Feladata az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt kielégítő informatikai biztonsági rendszerrel kapcsolatos, a jegyző és az elektronikus információs rendszer biztonságáért felelős szakmai utasításainak megfelelő feladatok elvégzése.

Szerepkör	Főbb felelősségek, tevékenységek
Megbízott szervezeti egység vezető (irodavezetők)	1. együttműködik az elektronikus információs rendszerek biztonságáért 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 elektronikus információs rendszerek biztonságáért felelős által tartott előző pontban megjelölt követelmények teljesülésének ellenőrzése során,
Adatgazda	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. a jogosultságok kiosztásánál törekedni kell a „legkisebb jogosultság” elvének érvényesítésére, vagyis mindenki a munkája elvégzéséhez szükséges jogosultságot kapja meg, 4. közreműködik az információbiztonsági kockázatok elemzésében.
Rendszergazda (megbízott köztisztviselő)	1. felelős az elektronikus információs rendszerek felügyeletéért, az alkalmazások, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaadások működésének folyamatos figyelemmel kísérésért, az üzemeltetéshez szükséges dokumentációk kidolgozásáért, a törvényi előírásoknak megfelelő nyilvántartások vezetéséért és naprakészen tartásáért. 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, a Hivatal Szoftver Etikai Kódexében megfogalmazott elveknek megfelelően, 4. biztosítja a rendszerfelügyeletet, a felhasználói fiókok felügyeletét, 5. felügyeli a fizikai belépést ellenőrző eszközöket 6. az elektronikus információs rendszer biztonságáért felelős személlyel és az adatgazdákkal együttműködve kialakítja és működteti az adatokhoz, rendszerekhez való hozzáférési jogok rendszerét, 7. közreműködik az elektronikus információs rendszer biztonságáért felelőssel és az adatgazdákkal az információbiztonsági kockázatok elemzésében, 8. elvégzik a logok elemzését és jelentést készít róla az elektronikus információs rendszerek biztonságáért felelős felé 9. információbiztonsági incidens észlelése esetén haladéktalanul jelentést tesz az elektronikus információs rendszerek biztonságáért felelős felé, 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 az elektronikus információs rendszer biztonságáért felelőssel közreműködve, meghatározza az információbiztonsági

Szerepkör	Főbb felelősségek, tevékenységek
	14. közreműködik az elektronikus információs rendszer biztonságáért felelőssel a BCP/DRP tervek kidolgozásában és megvalósításában, 15. kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat, 16. az elektronikus információs rendszer biztonságáért felelőssel egyeztetve vezeti az Informatikai biztonsági szabályzatban előírt nyilvántartásokat, vagy számára alap adatokat szolgáltat (a Hivatal vezetőjének utasítása szerint), pl.: a) hardver/ szoftver nyilvántartás b) alapkonfiguráció nyilvántartása c) informatikai szolgáltatást nyújtó szerződött partnerek listája, d) jogosultságok nyilvántartása (eszközökhöz, rendszerekhez, felhasználói fiókok) e) jogosultságigények nyilvántartása f) hordozható eszközök listája, kiadott eszközök nyilvántartása g) karbantartások naplózása, karbantartást végzők listája h) szerverterembe történő belépés logolása i) minden egyéb olyan nyilvántartás, amelyet az elektronikus információs rendszer biztonságáért felelős vezető a
Felhasználók (a szabályzat személyi hatálya alá tartozók a közszolgálati jogviszony, a munkaviszony alapján foglalkoztatott munkatársak, a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek)	1. köteles az információbiztonsági szabályzatban rá vonatkozó szabályokat megismerni, elolvasni 2. betartja végrehajtja az elektronikus információbiztonsági szabályokat, utasításokat, magatartásával segíti a hatékony és biztonságos informatikai biztonság megteremtését, 3. együttműködik a Hivatalt érintő információbiztonsági kérdéskörökben felettesével és az elektronikus információs rendszerek biztonságáért felelőssel 4. haladéktalanul jelenti felettesének vagy a rendszergazdának, ha az informatikai rendszerben fennakadást, leállást, zavart, jogosulatlan hozzáférést észlel, ha információbiztonsági eseményt/incidenst észlel, 5. Információbiztonsági incidens esetén - ha az személyét érinti, vagy felettese erre felkéri - együttműködik a kivizsgálásban, 6. bizalmasan kezeli felhasználói azonosítóját, jelszavait, védett zónákba belépést biztosító kártyáit, kódjaikat, 7. köteles részt venni a Hivatalon belül szervezett információbiztonsági oktatásokon, illetve a jegyző utasítása szerint más külső oktatásokon, 8. a birtokában lévő, vagy tudomására jutott információkat bizalmasan kezeli, 9. felelősséggel tartozik a munkavégzése során az elektronikus információs rendszerben végzett feladatokért, a szakrendszerek szakszerű használatáért, 10. felelősséggel tartozik a munkavégzéséhez szükséges, számára kiadott eszközök megfelelő fizikai, logikai védelméért, 11. elszámoltatható minden olyan tevékenységért, amelyet bárki a számára kiadott azonosítói alapján végzett, 12. valamennyi üzemeltető, pl. az ASP központ működtetője által kiadott felhasználói biztonsági követelményeket köteles követni és betartani, 13. megtagadhatja az utasítást, ha annak végrehajtása

Szerepkör	Főbb felelősségek, tevékenységek az érintettek jogos érdekeit sérti. Az utasítást adó felettes az utasítás írásba foglalását nem tagadhatja meg. 15. Az utasítástól való eltérést felettesének azonnal jelezni kell.
Weblap fejlesztő, üzemeltető, tartalom felelős	Weblap fejlesztő: 1. a mindenkor OWASP top 10-es sérülékenységek ellenőrzése, a nyilvánosságra hozott hibák kijavítása, a weblap motor / telepített modulok folyamatos ellenőrzése, frissítése Üzemeltető: 1. a védekezés külső (belső) támadás ellen, 2. a használt szolgáltatások folyamatos frissítése karbantartása, 3. lehetőség szerint a szolgáltatások verziószámainak elrejtése A tartalom felelős (Hivatal által kijelölt munkatárs): 1. a jogszabályi követelményeknek megfelelően a tartalom ellenőrzéséért felelős által jóváhagyott tartalom feltöltési és karbantartási feladatok ellátása, a Hivatal weboldalán elsősorban hírközlő, információs, tájékoztató jellegű adatok közzétele (a település bemutatása, aktuális hírek, információk közzétele az állampolgárok számára), A tartalom ellenőrzéséért felelős (Hivatal által kijelölt vezető vagy munkatárs): 1. a tartalom feltöltése előtt átvizsgálja és rendszeres időközönként ellenőrzi a nyilvánosan hozzáférhető elektronikus információs
ASP Központ super adminisztrátor	1. az önkormányzat által bérlő fiókonként, tenantonként kijelölt önkormányzati ASP adminisztrátor (tenant adminisztrátor) felvétele, annak adminisztrációja és karbantartása
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 szakrendszerei 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 és felhasználók közötti kiosztása, 2. az önkormányzat szakrendszerei adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást

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

Elektronikus információs rendszerek biztonsági osztályba sorolása, a Hivatal biztonsági szintje

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

Az elektronikus információs rendszerek biztonságáért felelős személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, a Hivatal biztonsági szintjét megállapítsa, *Biztonsági osztályba és szintbe sorolás mellékletben, Rendszerbiztonsági tervben* vagy egyéb dokumentumban rögzítse, szükség esetén jelen Informatikai biztonsági szabályzatot aktualizálja, a hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze. A biztonsági osztályba sorolást, a Hivatal vagy szervezeti egység biztonsági szintbe sorolását, az Informatikai biztonsági szabályzatot a Hivatal vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfeleléseért, a felhasznált adatok teljességéért és időszerűségéért, gondoskodik a módosított szabályzat életbe léptetéséről, az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon.

A biztonsági osztályba sorolás eredményét a kizárólag az érintettek és a Hatóság számára hozzáférhető *dokumentum*, a [NEIH-OVI] *Osztályba sorolás és védelmi* , a szintbe sorolás eredményét a [NEIH-SZVI] *Szintbe sorolás és védelmi intézkedés* űrlapok (illetve XML állományok) tartalmazzák.

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) vagy a tőle kapott tájékoztatás alapján a reá vonatkozó biztonsági követelményeket kell teljesítenie. A Hatóság részére a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés* űrlapot annak megfelelően kell kitöltenie a Hivatalnak, ami a szolgáltatóval kötött megállapodás vagy tájékoztatás alapján rá nézve teljesítendő.

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 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 besorolás alapján a 41/2015. (VII. 15.) BM rendeletben a Hivatalra és az elektronikus információs rendszereire érvényes biztonsági osztályhoz és szinthez rendelt követelményeket és azok megvalósításának módját a következő fejezet tartalmazza (adminisztratív, fizikai és logikai védelmi intézkedések). Az intézkedések és sorszámaik a Hatósági elvárásoknak megfelelően megegyeznek a rendelet követelményeivel.

Ha a Hivatal az elektronikus információs rendszernek csak egyes elemeit vagy funkcióit üzemelteti vagy használja - részben vagy teljesen a rendeletben meghatározott követelményeket ezen elemek és funkciók tekintetében kell teljesíteni.

Külső szolgáltató, illetve jogszabály alapján kijelölt szolgáltató esetében az elektronikus információs rendszer nem tartozik a Hivatal saját hatókörébe, így az azzal kapcsolatos biztonsági követelmények megoszlanak a Hivatal és a szolgáltató/üzemeltető között. A Hivatal számára egységes biztonsági megfelelés van előírva, amely minimalizálja a kliens oldali kockázatokat.

Az ASP szakrendszerekre vonatkozó követelményekhez figyelembe vettük a jogszabály alapján kijelölt szolgáltatót biztonsági osztályba sorolását. Az új elektronikus információs rendszer bevezetése vagy már működő elektronikus információs rendszer fejlesztése során megállapított biztonsági osztályhoz tartozó követelményeket a használatbavételig teljesíteni kell.

Biztonsági osztályba sorolás eredménye:

Biztonsági osztályba és szintbe sorolás melléklet tartalmazza (1. sz. melléklet)

Elektronikus információs rendszerek biztonsági osztálya

Biztonsági szintbe sorolás eredménye:

Biztonsági osztályba és szintbe sorolás melléklet tartalmazza (1. sz. melléklet)

ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

Az ebben a fejezetben leírt adminisztratív védelmi intézkedéseket egységesen, valamennyi elektronikus információs rendszerre vonatkozóan kell megvalósítani.

1.1. HIVATALI SZINTŰ ALAPFELADATOK

1.1.1. Informatikai biztonsági szabályzat

A jegyző megfogalmazza, dokumentálja és a Képviselő-testület döntését követően kihirdeti jelen Informatikai biztonsági szabályzatát. Jelen Informatikai biztonsági szabályzatot és eljárásrendet szükség szerint, de legalább évente egyszer az informatika biztonsági rendszer felülvizsgálata során felülvizsgálja, szükség szerint módosítja. Az informatikai biztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a szabályzatot újra vizsgálja, szükség szerinti módosítja. A módosítás az elektronikus információs rendszerek biztonságáért felelős személy szakmai irányításával történik. A jegyző feladata biztosítani, hogy az Informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

A jegyző az elektronikus információs rendszerek biztonságáért felelős személyt nevez ki vagy bíz meg, aki: ellátja az állami és Hivatali szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott feladatokat (lbtv. 13. §).

A jegyző gondoskodik a biztonságért felelős személy képzettségéről, alvállalkozó esetén szerződésben elvárja azt. Adatszolgáltatási kötelezettsége kiterjed a vonatkozó munka-, megbízási vagy más szerződés hatóság felé megküldésére és a jogosultság igazolására.

Csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki:

büntetlen előéletű (a büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni, a Hivatal vezetője kötelezheti, hogy a fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja), rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel, a Nemzeti Községi Egység továbbképzésén, éves továbbképzéseiben részt vesz, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján.

A 2013. évi L. törvény alapján az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetenél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Az információbiztonság ellenőrzésével és irányításával kapcsolatos feladatait a Szerepkörök, tevékenységek, felelősségek pont tartalmazza.

Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az

információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 11. § alapján az elektronikus információs rendszer biztonságáért felelős személy - ideértve az információbiztonsági szolgáltatást nyújtó vállalkozás tagjait és alkalmazottait is - az érintett szervezet igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja a vonatkozó szerződésben meghatározott időtartamban.

Az elektronikus információs rendszerek védelméért felelős személy az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján képzésre és éves továbbképzésre kötelezett.

A jegyző a Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság számára, az lbtv. 11. § (1) bekezdés c) pontjában meghatározott, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt.

1.1.3. Az intézkedési terv és mérőföldkövei

A jegyző az informatikai biztonsági követelmények megvalósításához az lbtv.-ben meghatározott határidőkkel Intézkedési tervet (*Cselekvési terv*) készít, amennyiben a meghatározott biztonsági osztálynál/szintnél hiányosságot állapít meg, ha valamely védelmi intézkedés nem valósul meg, vagy a bevezetett kontroll hibás, és ezekhez határidőket rendel.

A Cselekvési tervet szükség szerint, de legalább évente egyszer az informatikai biztonsági rendszer felülvizsgálata során (belső audit) felül kell vizsgálni, szükség szerint aktualizálni a kockázatkezelési stratégia és a kockázatokra adott válaszok, tevékenységek prioritása alapján (jellemzően a nagy kockázattal járó hiányosságokat kell előtérbe helyezni). Az informatikai biztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor a Cselekvési tervet újra felül kell vizsgálni, szükség szerinti módosítani. Ha az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál (belső vagy külső vizsgálat során) hiányosság kerül megállapításra, vagy a meghatározott biztonsági szint alacsonyabb, mint az elvárt biztonsági szint akkor a jegyző a vizsgálatot követő 90 napon belül felülvizsgálatot készít, a hiányosság megszüntetése érdekében.

A kitűzött feladatok megvalósulását a Cselekvési tervben a jegyző az elektronikus információs rendszer biztonságáért felelős közreműködésével nyomon követi és dokumentálja.

A jegyző feladata biztosítani, hogy a Cselekvési tervben meghatározott intézkedéseket bevezesse, az azokhoz szükséges erőforrásokról gondoskodjon.

Mivel az intézkedési terv (Cselekvési terv) bizalmas információkat tartalmaz, ezért ezt csak a jegyző, a biztonságért felelős, és az általuk kijelölt személyek, valamint az ellenőrzésre jogosult hatóságok ismerhetik meg.

1.1.4. Az elektronikus információs rendszerek nyilvántartása

Az elektronikus információs rendszer biztonságáért felelősnek az elektronikus információs rendszerekről nyilvántartást kell vezetni, azt szükség szerint aktualizálni.

A nyilvántartásnak tartalmaznia kell:

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

1.1.5. 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

A fizikai és logikai jogosultságok engedélyezése az alábbiakat foglalja magába:

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

Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást (a jogosultságok kiosztását és visszavonását) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza, illetve az engedélyezések a további védelmi intézkedések alatt kerülnek részletezésre {pl. 1.6.4. Eljárás a jogviszony megszűnésekor}.

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 elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért felelős az előterjesztő.

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

Verzió
Készült (dátum)
Változás oka
Jóváhagyta
Hatálybalépés dátuma

Hatósági engedélyezés szükséges, ha 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.

Az Ibtv. 3. § (2) - (5) bekezdése lehetőséget ad arra, hogy a Hivatal egyes elektronikus információs rendszereit Magyarország területén kívül üzemeltesse, illetve azokban külföldön végezzenek adatkezelést. A Hivatal az adatkezelés kezdetét legalább 90 nappal megelőzően írásbeli kérelmet nyújthat be a Hatóságnak. A kérelemhez csatolni kell:

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

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

A jegyző a helyes módszertan szerinti kockázatkezelést és az ehhez kapcsolódó ellenőrzések megvalósítását elősegítő eljárást Kockázatkezelési eljárásrendben határozza meg. A törvényi célok teljesítése, a munkatársak, 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. Valamennyi alapfeladatot ellátandó terület saját felelősséggel bír az általa hasznosított és feldolgozott információk biztonságáért és megfelelő védelméért azok értékének és kockázatának megfelelően, ez a felelősség magában foglalja az egyes személyeknek az információk használatával kapcsolatosan felmerülő elszámoltatási kötelezettségét is.

1.2.2. Biztonsági osztályba sorolás

A Hivatal annak érdekében, hogy az lbtv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen - az elektronikus információs rendszerek biztonságáért felelős személy irányításával - jogszabályban meghatározott szempontok, kockázatelemzés alapján megvizsgálja (alvállalkozó igénybevétele esetén megvizsgáltatja) elektronikus információs rendszereit és meghatározza, hogy azok melyik biztonsági osztályba sorolandók, melynek eredményét a kizárólag az érintettek számára hozzáférhető *Elektronikus információs rendszerek biztonsági osztálya, Rendszerbiztonsági terv* vagy egyéb dokumentum, és a rendszerenként a [NEIH-OVI] *Osztályba sorolás és védelmi intézkedés űrlap-ok* 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 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 bizalmosságának, 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 az adott elektronikus információs rendszerre vonatkozóan.

A jegyző a törvényben meghatározott feltételeknek megfelelő, az elektronikus információs rendszerre irányadó biztonsági osztálynál magasabb, kivételes esetben a hatóság előzetes engedélyével, kockázatokra kiterjedő indoklással ellátva alacsonyabb biztonsági osztályt is megállapíthat az elektronikus információs rendszerre vonatkozóan.

Azokat a kontrollokat, amelyek nem valósulnak meg, kockázatelemzés útján prioritásukat tekintve intézkedési tervben (Cselekvési tervben) kell kezelni.

A biztonsági osztályba és biztonsági szintbe sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni. A soron kívüli biztonsági osztályba és szintbe sorolást az elektronikus információs rendszer biztonságát érintő jogszabályban meghatározott változás vagy új elektronikus információs rendszer bevezetése esetén, ill. a szervezet státuszában, szervezetében, ill. az általa kezelt vagy feldolgozott adatok vonatkozásában bekövetkezett változás esetén szükséges elvégezni.

Az elektronikus információs rendszerek biztonságáért felelős személy vagy a jegyző által megbízott személy feladata, hogy a rendszerek biztonsági osztályba sorolását elvégezze, a Hivatal és szervezeti egységeinek biztonsági szintjét megállapítsa, *Biztonsági osztályba és szintbe sorolás* mellékletben vagy egyéb dokumentumban rögzítse, szükség esetén jelen Informatikai biztonsági szabályzatot aktualizálja, a hatósági adatszolgáltatást előkészítse és a jegyző számára előterjessze.

A Hivatal és szervezeti egységei által használt informatikai rendszerek biztonsági osztályba sorolásait, a Hivatal vagy szervezeti egység biztonsági szintbe sorolását, az Informatikai biztonsági szabályzatot a jegyző hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért, a felhasznált adatok teljességéért és időszerűségéért, gondoskodik a módosított szabályzat hatályba léptetéséről, az érintettekkel való megismertetéséről, az elektronikus információs rendszerek biztonságáért felelős személy közreműködésével az adatszolgáltatás teljesítéséről a Hatóság (Nemzeti Kibervédelmi Intézet Nemzeti Elektronikus Információbiztonsági Hatóság) által előírt módon (feltöltés a NEIH hivatali kapujára vagy tömörített, titkosított/jelszóval védett állomány elküldése).

1.2.3. Kockázatelemzés

Az információbiztonság területén fellépő kockázatokat az elektronikus információs rendszer biztonságáért 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 jelen szabályzat vagy a Kockázatelemzési és kockázatkezelési eljárásrend alapján (ha készül). Ezenkívül, bármilyen változás (fejlesztés, fenyegetések, sebezhetőségek) esetében ismételt kockázatelemzési tevékenységet kell végeznie. Az elektronikus információs rendszer biztonságáért 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 kockázatelemzés eredményeit, illetve az abból származó szükséges intézkedéseket az érintettek felé kommunikálni szükséges, amelyet az elektronikus információs rendszer biztonságáért 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 kockázat-felmérési módszertan és a kockázatmenedzsment rendszer kialakítása során figyelembe vettük az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM. rendelet, informatikai biztonsági szabványok és a kapcsolódó útmutatók előírásait.

A módszertan, menedzsment meghatározásáról a jegyző - a kockázatfelmérésért felelős szakmai javaslata alapján - dönt, figyelembe véve a Nemzeti Elektronikus Információbiztonsági Hatóság és egyéb hatóság

elvárásait, szakmai ajánlásait.

A Hivatal hatókörébe tartozó informatikai rendszerekre vonatkozóan a biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A kockázatelemzés elvégezhető a hatóság által ajánlásként kiadott kockázatelemzési módszertana (segédlete) vagy egyéb, a követelményeket figyelembe vevő saját kockázatelemzési módszertan alapján, melyet eljárásrendben rögzíteni kell. Az elektronikus információs rendszerek besorolását a Rendszerbiztonsági terv vagy egyéb dokumentum tartalmazza. A besorolás és nyilvántartás az elektronikus információs rendszer biztonságáért felelős feladata.

A kockázatok azonosítása és felmérése információs rendszerenként, a kockázatok értékelése a vonatkozó jogszabályok alapján, a valószínűsíthető káresemény (közvetett és közvetlen) nagysága és annak a szervezetre gyakorolt, becsült hatása alapján történik.

Az éves felülvizsgálat, illetve felmérés során számba kell venni a belső eredetű kockázatok (sérülékenységek), a külső okokat (fenyegetések), a bekövetkezés valószínűségét (gyakoriságát), ill. azt, hogy milyen adatok és milyen mennyiségbe sérülhetnek.

Meg kell határozni az okok (sérülékenységek, fenyegetések) nyomán előforduló helyzet, esemény (kockázati esemény) hatásait, következményeit, és ennek nagyságát.

Az alábbi közvetett, vagy közvetlen kárt okozó hatásokat, veszélyeket és károkat kell - a Hivatal jellemzőire tekintettel - figyelembe venni:

1. társadalmi-politikai káros hatásokat, károkat vagy a jogsértésből, kötelezettség elmulasztásából fakadó káros hatásokat, károkat (így pl. alaptevékenységek akadályozása, különösen a létfontosságú információs rendszer elemek működési zavarai, a nemzeti adatvagyon sérülései, jogszabályok és egyéb szabályozások megsértése, jogszabály által védett adatokkal történő visszaélés vagy azok sérülése, a közérdekűség követelményének sérülése, személyiséghez fűződő jogok megsértése, bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben, az ország jogrendjének sérülése, vagy ennek lehetővé tétele);
2. személyeket, csoportokat érintő károk, káros hatások (pl. különleges személyes adatok, banktitkok, üzleti titkok megsértése, szervezet, személyek vagy csoportok jó hírének károsodása, személyi sérülések, vagy haláleset bekövetkeztének - ideértve az elektronikus információs rendszer működésének zavara, vagy információhiány miatt kialakult veszélyhelyzetet - veszélye);
3. közvetlen anyagi károk (az infrastruktúrát, az elektronikus információs rendszert ért károk, és ezek rendelkezésre állásának elvesztése miatti pénzügyi veszteség, adatok sértetlenségének, rendelkezésre állásának elvesztése miatti költségek, dologi kár);
4. közvetett anyagi károk (pl. helyreállítási költségek, elmaradt haszonnal arányos költségek, a környezet biztonságának veszélyeztetése, perköltségek).
5. A veszélyeztetettségnek a bekövetkezés valószínűségének megfelelő kárérték szinteknek megfelelő biztonsági osztályba sorolásakor a bizalmasság, sértetlenség és rendelkezésre állás követelménye külön-külön értékelendő.

A kockázatok kezelése

A Hivatal a feltárt kockázatokra a vonatkozó jogszabályban meghatározott biztonsági intézkedések mielőbbi megvalósításával reagál. A megvalósítandó biztonsági intézkedéseket, és azok megvalósításának sorrendjét a

kívánt biztonsági osztály és biztonsági szint elérésére készített Cselekvési tervben kell meghatározni. Amennyiben a kockázat kezelésére javasolt válasz reakció beruházással jár, a jegyző az egyéb szabályzatokban meghatározott engedélyezési szabályok szerint jár el.

A kockázatokra adott válaszingézkedéseket a következők kockázatkezelési stratégiák alapján lehet kiválasztani:

1. A kockázat elviselése

A Kockázat elviselés a következő esetekben alkalmazható:

- a. ha a kialakult működési rend olyan, hogy napi működése során minden beavatkozás nélkül automatikusan kezeli a kockázatot, ezért a kockázat gazdának nincs szüksége külön beavatkozásra,
- b. tudatos vezetői döntés esetén, amennyiben a kockázat elhárításának költsége magasabb az elhárításból eredő haszonnál, vagy kezelése technikai, időbeli, vagy anyagi korlátba ütközik. Amennyiben a vezetői döntés ilyen kockázat elviseléséről dönt, a válaszreakció helyett, köteles a kockázati tényező bekövetkezése után jelentkező hatások kezeléséről gondoskodni.

2. A kockázat kezelése

A kockázat kezelése akkor alkalmazható, ha a kockázatos tevékenység nem szüntethető meg és nem hárítható át. A kockázat kezelés az alábbi típusú kontroll tevékenységeken keresztül valósítható meg.

- c. Megelőző kontrollok: Korlátozzák egy negatív következménnyel járó kockázat bekövetkezésének lehetőségét, vagyis a megelőző kontrollok a szervezeten belüli belső kontrollok (pl. feladatok szétválasztása, „4 szem elve”, tartalék erőforrások, helyettesítési rendszer, képzések).
- d. Korrekciós kontrollok: A realizálódott, nem kívánt kockázat következményeit korrigálják, úgy, hogy kiegészítő megoldást nyújtanak a kár vagy veszteség csökkentésére. Fontos eleme a folytonossági és katasztrófatervek kidolgozása, illetve az eljárásrendekbe beépítve, váratlan helyzetek kezelésének szabályozása, amellyel a szervezet működésének folytonosságát tudja biztosítani a negatív hatásokkal, veszteséggel járó esemény bekövetkezése esetén.
- e. Iránymutató kontrollok: Egy bizonyos, kívánt eredmény elérését biztosítják. Általában egy tevékenység vagy tevékenységcsoport konkrét lépéseit, időbeni ütemezésüket tartalmazzák. Hasznos lehet a szervezet korábbi, hasonló tevékenységekből nyert tapasztalatainak beépítése az ilyen jellegű kontrollokba, amely ugyancsak biztosítékként szolgálhat a kívánt cél eléréséhez és így a kockázatok elkerüléséhez, csökkentéséhez (pl. eljárásrendek, utasítások, egyéb szabályozások, útmutatók).
- f. Felderítő kontrollok: Azt a célt szolgálják, hogy fényt derítsenek olyan esetekre, amikor nem kívánt események következtek be. Mivel csak az esemény bekövetkezése után fejtik ki hatásukat, ezért csak abban az esetben használhatók, amennyiben lehetőség van a kár vagy veszteség elfogadására (pl. rendszeres ellenőrzések, naplók áttekintése, a monitoring jelentések, folyamatok, projektek áttekintései, a célvizsgálatok, az auditok, stb.).

3. A kockázat átadása

A kockázat átadását esetén a kockázat (sem a valószínűsége, sem hatása) nem csökken, de megváltozik a kockázatviselő (szervezeten kívülre kerül). Tipikus példa a biztosításkötés, illetve a kockázatos művelet átadása olyan (külső vagy belső) partnernek, aki felkészült a kockázat kezelésére. Ilyen megállapodás esetén vizsgálendő, hogy a kockázati esemény bekövetkezése esetén milyen maradványkockázat marad az átadó szervezetnél, illetve a Hivatalnál (pl. reputáció-vesztés).

4. A kockázatos tevékenység befejezése;

A kockázatos tevékenység befejezése akkor alkalmazható, ha a kockázatok nem csökkenthetők elfogadható szintre a tevékenység megszüntethető, és megszüntetése nem akadályozza az Hivatallal szembeni követelmények teljesítését, csak megszüntethetők az adott tevékenység befejezésével.

Felelősségek

Jegyző

- felelős a kockázatkezelési rendszer(ek) kialakításáért, működtetéséért
- felelős a kockázatkezelési kritériumok azonosításáért
- kinevezi a kockázatfelmérésért felelősöket, tevékenységüket felügyeli
- gondoskodik a kockázatkezelési irányelvek betartásáról
- biztosítja a kockázatfelméréshez és -kezeléshez a szükséges erőforrásokat
- dönt a kockázatfelmérés elfogadásáról, kockázatok elfogadásáról, az elfogadható kockázati szintről, a szükséges intézkedésekről, figyelemmel kísérisi feladatokról
- gondoskodik a kockázatkezelés fontosságának tudatosításáról a teljes szervezetben

A kockázatfelmérésért felelős (elektronikus információs rendszerek biztonságáért felelős személy)

- felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyásáért
- kezdeményezi az éves rendszeres felmérés indítását
- koordinálja a kockázat-felmérési tevékenységeket
- javaslatokat tesz kockázatkezelési, javítási intézkedésekre
- gondoskodik a kockázatkezelési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről
- rendszeresen tájékoztatja a jegyzőt a kockázati szint alakulásáról, bekövetkezett kockázati eseményekről
- nyilvántartja a Hivatal információs rendszereit a 41/2015. (VII. 15.) BM. rendelet követelményeinek megfelelően

A szakterület kijelölt képviselője/jegyző vagy az általa kijelölt személy

- a kockázatfelmérésért felelős segítségével azonosítja, felméri, értékeli a területére vonatkozó kockázatokat
- javaslatot tesz a magas kockázatok kezelésére a saját területére vonatkozóan
- intézkedik a saját hatáskörükben kezelhető kockázatok csökkentésére, kezelésére
- felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért
- a kockázatok változása, újak felmerülése esetén aktualizálja a felmérést, tájékoztatja a kockázatfelmérésért felelőst

A munkatársak

- felelősek a közzétett, kiadott kockázatkezelési előírások betartásáért
- feladatuk a nem kezelt, illetve az új vagy változó kockázatok jelzése közvetlen vezetőjüknek és/vagy a kockázatfelmérésért felelősnek.

1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

1.3.1. Beszerzési eljárásrend

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 Hivatal IT fejlesztés és üzemeltetés - az információbiztonság rendelkezésre állás céljait támogató - beszerzéssel kapcsolatos szabályait - ha szükséges - külön szabályzat vagy eljárásrend tartalmazza.

A beszerzési eljárásrendet abban az esetben kötelező bevezetni, ha a Hivatal saját hatókörében informatikai szolgáltatást, vagy eszközöket szerez be, rendszerfejlesztési tevékenységet (ide nem értve a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazásokat, szoftvereket, vagy azokat a hardver beszerzéseket, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából történnek, valamint a javítás, karbantartás céljára történő beszerzéseket) végez, vagy végeztet (nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése).

A beszerzett számítástechnikai eszközöket, szoftvereket (Gazdálkodási Iroda illetékes köztisztviselője) a nyilvántartásra kijelölt felelősnek haladéktalanul nyilvántartásba kell venni.

Az irodai munkavégzéshez szükséges irodatechnikai eszközök, alkalmazások megfelelő minőségben és mennyiségben történő készletezése (készletezés tervezése) a 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, értelemszerűen a követelményeknek megfelelő eszközök beszerzése az elvárt.

1.3.2. Erőforrás igény felmérés

Ha a Hivatal saját hatókörében informatikai szolgáltatást vagy eszközöket szerez be, rendszerfejlesztési tevékenységet végez, vagy végeztet, vagy az erőforrás igény felmérés jogszabály alapján, a külső szolgáltató/jogszabály alapján kijelölt szolgáltató által előírt, akkor az elektronikus információs rendszerre és annak szolgáltatásaira vonatkozó biztonsági követelmények teljesítése érdekében a beruházás tervezés részeként meghatározza, és dokumentálja, valamint biztosítja az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat (eszközöket, szolgáltatásokat, humán erőforrásokat), elkülönítetten kezeli az elektronikus információs rendszerek biztonságát beruházás tervezési dokumentumaiban.

A beruházással járó fejlesztések, módosítások, felújítások során 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.

1.3.3. Beszerzések

Az elektronikus információs rendszer biztonságáért 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. a funkcionális biztonsági követelményeket;
- b. a garanciális biztonsági követelményeket (pl. a biztonságkritikus termékekre elvárt garanciaszint);
- c. a biztonsággal kapcsolatos dokumentációs követelményeket;

- d. a biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket;
- e. 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 elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért felelős (egyeztetve a rendszergazdával) feladata;

- a. a harmadik féllel kapcsolatos kockázatok felmérése,
- b. a vonatkozó biztonsági követelmények azonosítása,
- c. az esetleg szükséges egyedi óvintézkedések meghatározása,
- d. a biztonsági követelmények dokumentálása, jegyző felé történő kommunikálása.

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 lehetőség szerint 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.

1.3.3.2. 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 határozni a fejlesztő, szállító számára, hogy hozza létre és bocsássa rendelkezésére az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

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

1.3.6. Külső elektronikus információs rendszerek szolgáltatásai

A külső elektronikus információs rendszer szolgáltatók értékelése és a szolgáltatási szerződések átvizsgálása (ahol az lehetséges) az elektronikus információs rendszer biztonságáért 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.

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 elektronikus információs rendszer biztonságáért felelős kötelessége. A külső szállítókat/szolgáltatókat/harmadik feleket a rendszergazda nyilvántartja.

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.

1.4. 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:

- a. kritikus erőforrások, funkciók, szolgáltatások azonosítása,
- b. elvárások és prioritások azonosítása,
- c. tervezés - folyamat létrehozása, szerepkörök rögzítése, megismerés,
- d. kommunikáció,

- e. tesztelés,
- f. rendkívüli események bekövetkezése esetén a tervek aktiválása,
- g. 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 visszaállítása, 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 elektronikus információs rendszer biztonságáért felelős, aki a terv kidolgozásába bevonja a rendszergazdát.

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:

- a. alapfeladatok, alapfunkciók, alapfunkciót támogató kritikus rendszerelemek,
- b. definiált alapszolgáltatások fenntartása, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is,
- c. tervezhető rendkívüli helyzetek / katasztrófahelyzetek,
- d. ügymenet-folytonossági célértékek (alapfunkciók, alapszolgáltatás és összes funkció újratelepítésének időpontja, az ügymenet-folytonossági terv életbelépését követően, tervezett szolgáltatási szint),
- e. a folytonosság biztosításába bevont szerepkörök meghatározása és megismerése,
- f. a tervek aktiválási (életbe léptetési) körülményei,
- g. az aktiválásról értesítendő személyek,
- h. a végrehajtásba bevonandó személyek, azok elérhetősége, valamint kapcsolódó feladatok,
- i. incidens (biztonsági események is) kezelési folyamatának integrálása a tervekben,
- j. rendkívüli helyzetek / katasztrófa helyzet kezelési folyamatainak részletei, szabályai, prioritások,
- k. a normál üzletmenetre történő visszaállási eljárásokat (úgy, hogy az nem ronthatja az eredeti ügymenet minőségét),
- l. 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 naprakésszé 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 elektronikus információs rendszer biztonságáért felelős felelőssége.

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:

az elemi kár, az
áramszünet,
a rendszerleállás, szolgáltatásszünetelés, hálózati hiba,
az adatsérülés, az adatvesztés,
információ-feldolgozó eszközök, adattárolók rongálódása, eszközök
megszokottól eltérő működése (hardver hibás működése), futtatási
hiba (program hibás működése), biztonsági események.

1.4.2.4. Kritikus rendszerelemek meghatározása

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

1.4.3. A folyamatos működésre felkészítő képzés

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

Az elektronikus információs rendszer biztonságáért 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.

1.4.5.3. 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).

1.4.7. Infokommunikációs szolgáltatások

A Hivatal - a Nemzeti Távközlési Gerinchálózatra 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 újratekintését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a biztonsági tárolási helyszínen.

1.4.7.2. 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, és 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 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézésről összefüggő adatok biztonságát szolgáló Kormányzati Adattrezzorról 8. pont 15. § (1) bekezdése alapján, a Hivatal az adattrezzor-archiválási kötelezettségének az önkormányzati ASP rendszer útján tesz eleget.

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

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

A rendszergazda az elektronikus információs rendszer biztonságáért felelőssel való egyeztetés után felülbíráhatja, 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.

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 visszaellenőrzött biztonsági mentés törlődjön.

A Hivatal a további, egyedi mentési szabályokat szükség esetén *Mentési eljárásrend* vagy egyéb dokumentumban részletezi, melynek elkészítése és naprakészen tartása az elektronikus információs rendszer biztonságáért felelős és 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 rendszergazda gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően (saját hatókörén belül). 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 szükség esetén helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell továbbá, hogy az üzemidőkiesés, adatsérülés és adatvesztés oly mértékű legyen, amely a Hivatal által meghatározott elfogadható kockázati értéken belül marad.

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.

A 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.

Ennek megfelelően az elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért felelős:

- a. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével,
- b. egyezteti az eseménykezelési eljárásokat az ügymenet-folytonossági tervéhez tartozó tevékenységekkel,
- c. 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 elektronikus információs rendszer biztonságáért felelősnek.

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

A biztonsági eseményre adandó gyors és hatékony megoldások érdekében az elektronikus információs rendszer biztonságáért felelős személy ügymenet-folytonossági tervben határozza meg a váratlan eseményekkel kapcsolatos felelősségeket és eljárásokat (lásd *Ügymenet-folytonosságra vonatkozó eljárásrend*)

1.5.4. A biztonsági események figyelése

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

Az elektronikus információs rendszerek működése során fellépő eseményeket megfelelő részletességgel naplózni kell. Az üzemeltetőknek ezeket a naplóállományokat rendszeresen ellenőrizniük kell, az ellenőrzés eredményéről rendszeresen és szükség esetén időszakosan jelentést kell tenniük az elektronikus információs rendszer biztonságáért felelős személy részére.

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

1.5.6. 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 elektronikus információs rendszer biztonságáért felelősnek. A felhasználó köteles a tapasztalt jelenséget, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul a rendszergazda rendelkezésére bocsátani (pl. feljegyzés, képernyőkép). A jelentési csatornákat biztonságáért 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. hálózatzbiztonsági 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 elektronikus információs rendszer biztonságáért felelős készít el és jelenti azt a jegyző felé.

Az információbiztonsági eseményről készült jegyzőkönyveket megfelelő jogosultsági szinttel kell ellátni.

Az elektronikus információs rendszer biztonságáért felelős a 41/2015 (VII.15.) BM rendelet értelmében jelenti azokat a biztonsági eseményekre vonatkozó információkat az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezeteknek (GovCERT-Hungary), amelyek hálózatzbiztonsági 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.

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendelet (GDPR) előírásai alapján a természetes személyek adatait érintő adatvédelmi incidenseket haladéktalanul jelenteni kell az adatvédelmi tisztviselő felé, akinek legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, jelentési kötelezettsége van az illetékes felügyeleti hatóság felé (kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve). Adatvédelmi incidens az a biztonsági esemény, amely megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

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

1.5.8. Biztonsági eseménykezelési terv

Az elektronikus információs rendszer biztonságáért 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 hálózatzbiztonsági incidenseket (pl. DDOS támadás), amelyeket be kell jelenteni az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezeteknek (Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központnak).

Ezekben az esetekben elsősorban:

- a. az elektronikus információs rendszer biztonságáért 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, felelős: észlelő
- 2) Vizsgálat, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők
 - 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?
- 3) Elszigetelés (az esemény jellegéből adódóan)
- 4) Megszüntetés, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők
 - a) a szükséges intézkedések meghatározása,
 - a) az incidensekre hozott döntéseket, intézkedéseket dokumentáltan szükséges megtenni,
 - b) intézkedések végrehajtása,
 - c) 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.
- 5) Helyreállítás, felelős: elektronikus információs rendszer biztonságáért felelős, rendszergazda, érdekelt munkatársak, kijelölt szakértők
Helyreállítási felelősségek kijelölése:

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

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

1.5.9. 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 elektronikus információs rendszer biztonságáért felelős tartja.

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.

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 (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait.

Az elektronikus információs rendszerek üzemeltetőinek, szolgáltatóknak az emberi erőforrás megbízhatóságának biztosítása érdekében a háttérszolgáltatást biztosító szolgáltatói állomány tekintetében gondoskodnia kell a vonatkozó jogszabályokban rögzített megfelelőségi követelmények teljesítéséről (például érzékeny adatok feldolgozását végző rendszerhez kikaphatnak fizikai és logikai hozzáférést).

1.6.2. Munkakörök, feladatok biztonsági szempontú besorolása

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot biztonsági szempontból besorol, felméri a nemzetbiztonsági ellenőrzés alá eső munkaköröket és feladatokat, rendszeresen felülvizsgálja és frissíti a munkakörök és feladatok biztonság szempontú besorolását. A

besorolásnál figyelembe kell venni a vonatkozó jogszabályok előírásait.

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

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. „normál”,
- b. „közepes”,
- c. „magas”,

biztonsági kategóriákba sorolja.

A biztonsági kategóriákat és az adott kategóriába tartozó munkaköröket a Hivatal a *Munkakörök biztonsági szempontú besorolása* vagy egyéb dokumentum tartalmazza (ha van intézkedést igénylő munkakör).

A nemzetbiztonsági ellenőrzés célja annak vizsgálata, hogy a fontos és bizalmas munkakörre jelölt, illetve az ilyen munkakört betöltő személyek megfelelnek-e az állami élet és nemzetgazdaság jogszerű működéséhez szükséges biztonsági feltételeknek. A biztonsági feltételek vizsgálata azt jelenti, hogy az ellenőrzés alá vont személlyel kapcsolatban felvetődnek-e olyan kockázati tényezők, körülmények, információk, amelyek miatt tevékenysége jogellenes céllal befolyásolhatóvá, illetve támadhatóvá válhat, és ez által a nemzetbiztonságot sértő vagy veszélyeztető helyzet állhat elő. A nemzetbiztonsági ellenőrzés kockázat-vizsgálat, nem annak bizonyítására vagy kizárása irányul, hogy az ellenőrzöttet jogellenesen befolyásolták és ez által a nemzetbiztonság veszélyeztetett, hanem hogy a feltárt tények, körülmények, információk alapján okkal feltételezhető-e, hogy ilyen helyzet kialakulhat. A nemzetbiztonsági ellenőrzésre az érintett tudtával kerülhet sor.

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, koncentrálókéesség 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. sz. melléklet, minta), 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, 2. sz. melléklet, minta)
- d. kötelező képzések elvégzését igazoló feljegyzések (Munka és tűzvédelem, informatikai biztonsági oktatás).

Az elektronikus információs rendszer biztonságáért felelős véleményezi az egyes munkakörökhöz, feladatokhoz tartozó leírásokat és javaslatot tesz annak információbiztonsági kikötéseire, amelyeket a jegyzői jóváhagyás után a jegyző által kijelölt munkatártnak a munkaköri leírásokban, szerződéseknél rögzítenie kell.

A humán erőforrás fentebb leírt pontjai nem lehetnek ellentmondásban jelen szabállyal. Az átvilágítás módját és a szükséges átvilágítási elemeket a Hivatal *Munkakörök biztonsági szempontú besorolása* dokumentuma tartalmazza (ha szükséges készíteni). A besorolási eljárás előkészítése és dokumentálása az elektronikus információs rendszer biztonságáért felelős feladata.

1.6.4. Eljárás a jogviszony megszűnésekor

Az alkalmazás megszűnéséről a jegyző 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 szerződőnek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. A jogosultságok visszavonása szakrendszerek esetén a szervezeti egység vezető, egyéb jogosultságok esetén (pl. felhasználói fiókok, levelezőrendszer) a rendszergazda feladata, az elektronikus információs rendszer biztonságáért felelős a jogosultságok visszavonásáról meggyőződik, hiba esetén intézkedést kezdeményez.

A jogosultság megszűnését a nyilvántartás vezetésével megbízott feladata dokumentálni a rendszeresített dokumentumban vagy elektronikus nyilvántartásban.

A rendszergazda megszünteti, vagy visszaveszi a Hivatal által az érintett személynek kibocsátott egyéni hitelesítő eszközeit, beleértve a hitelesítésre szolgáló eszközöket, felhasználói kártyákat (pl. anyakönyvi kártya).

Az alkalmazás megszűnésekor a kilépő munkatártnak, 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 elektronikus információs rendszer biztonságáért 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 jegyző az érintetteket értesíti a munkatárs, szerződő, harmadik fél jogviszonyának megszűnéséről, és gondoskodik még a jogviszony megszűnése előtt az elektronikus információs rendszerrel és annak biztonságával kapcsolatos feladatok ellátásáról.

Az elektronikus információbiztonsággal kapcsolatos további engedélyezési eljárást (a jogosultságok kiosztását és visszavonását) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza.

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 jegyző 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).

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

A Hivatal más, külső szervezettel történő szerződés létesítésekor megkövetelheti, 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 partnernek a Hivatalt haladéktalanul tájékoztatnia kell arról, ha változik a saját elektronikus információs rendszer biztonságáért 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.

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

Az elektronikus információs rendszer biztonságáért 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.

1.6.7. Fegyelmi intézkedések

Minden alkalmazottnak és külső partnernek (az Informatikai biztonsági szabályzat személyi hatálya alá tartozóknak) be kell tartania a Hivatal információbiztonsági szabályait. Minden ennek megtagadásából származó információbiztonsági incidens fegyelmi eljárást vonhat maga után. A szervezeti egység vezetője - szükség esetén az elektronikus információs rendszer biztonságáért felelős és a rendszergazda bevonásával - a tudomására jutott incidenst mérlegeli annak súlyosságától függően, és jelenti azt a jegyző felé. A fegyelmi

eljárás módját a jegyző szükség esetén az elektronikus információs rendszer biztonságáért felelőssel a rendszergazdával 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 szükség szerint tervezi és egyezteti az elektronikus információs rendszer biztonságát érintő tevékenységeit, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását.

1.6.9. Viselkedési szabályok az interneten

Az internethasználat legbiztonságosabb módjának kialakításáért a rendszergazda gondoskodik, az elektronikus információs rendszer biztonságáért felelőssel együttműködve.

A Hivatal az internethasználat és az elektronikus levelezéssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal, a szabályzat személyi hatálya alá tartozókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelező, vagy tiltott tevékenységeket *Informatikai biztonsági eljárásrendben* vagy egyéb dokumentumban (pl. Oktatási anyagban) részletezi.

A felhasználónak a Hivatal hálózatában tilos:

- a. a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így különösen mások személyiségi jogainak megsértése (pl. rágalmazás), tiltott hasznoszerzésre 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. fájlcsere-lő 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 a Hivatal szakfeladataihoz szükséges elektronikus információs rendszerek elérhetők, 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 a rendszergazda és az elektronikus információs rendszer biztonságáért felelős határozza meg, amelyet jegyzői/szervezeti egység vezetői jóváhagyás után a rendszergazda vagy az ezzel a feladattal

megbízott felelős, szolgáltató 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 (pl. közösségi célból).

A Hivatal a felhasználók által böngészett oldalak listáját 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.

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.

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. 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 (vezetéknév.keresztnev@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 munkaállomásain technikai korlátozásokkal tiltani kell;
- e. ha a felhasználó nem ismeri a külső rendszerből érkező levél feladóját, akkor az üzenet megnyitása előtt igyekezzon 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 (lehetőleg a hivatal belső hálózatától elszeparált, szakfeladathoz nem kapcsolódó dokumentumot nem tartalmazó, informatikai rendszer elérést lehetővé nem tevő számítógépen) tegye, és az esetleges csatolt melléklet megnyitását vírus veszély miatt feltétlenül kerülje, további címzettnek nem küldheti tovább;
- f. az alkalmazottnak 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 indokoltan szükséges) vagy tartalmát más munkatárshoz irányítja, 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 *(Isd. 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 e-mail címmel magánérdekből, publikus rendszerekben regisztrálni, fórumokon megjeleníteni, 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.
- m. 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;
- n. a munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából, archiválni szükséges;
- o. a csatolt állományok készítéséhez és a partnerekhez való küldéshez a dokumentumokat előzetesen PDF formátumra kell átalakítani, amennyiben nem szükséges azt szerkeszthető formátumban továbbítani.

Az lbtv. 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.

Az elektronikus levelekben, vagy azok mellékleteként a csatolt állományokat az informatikai rendszer automatikusan ellenőrzi, és a biztonságos üzemeltetést veszélyeztető állományok esetében a használatot, illetve a küldés/fogadást megakadályozza. Az állományok küldésére és fogadására vonatkozó korlátozás kiterjed a rendeltetésszerű- és az ésszerű használat kereteit meghaladó méretű állományokra is.

Ha a felhasználó saját Hivatali postafiókjára elektronikus levélben vagy annak mellékletében kapott olyan állományt, amely nem munkavégzéshez kapcsolódik, azt haladéktalanul törölnie kell, a Hivatal adathordozóira tilos a munkavégzéshez nem kapcsolódó, személyes adatot tartalmazó dokumentum (beleértve a fényképeket is) mentése. A felhasználónak rendszeresen ellenőriznie kell a hozzárendelt mappák, a rendszergazdának a Hivatal összes adathordozójának adattartalmát. Ha a munkavégzéshez nem kapcsolódó vagy személyes adatot tartalmazó dokumentum észlelésére kerül sor, az észlelőnek fel kell hívni a tulajdonos - ha ismert - figyelmét

erre, fel kell szólítani az észszerű időn belüli végleges törlésre. Ennek elmulasztását jelenteni kell a szervezeti egység vezetője és szükség esetén az adatvédelmi tisztviselő felé. Ha nem azonosítható be egyértelműen a munkavégzéshez nem kapcsolódó vagy személyes adatot tartalmazó dokumentum tulajdonosa, a rendszergazda kötelessége az adott állomány végleges törlése helyreállíthatatlanságot biztosító törlési technika alkalmazásával (beleértve az archivált állományokat is).

A Hivatalnak figyelembe kell venni a vonatkozó jogszabályok előírásait, így a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR).

A felhasználó tudomásul veszi, hogy a Hivatal informatikai hálózatára, eszközeire vonatkozóan a Hivatal ellenőrzési és felelősségre vonási jogosultsága fennáll, a 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 (Ibtv.) 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).

Az Ibtv. alapján a szervezet vezetője köteles együttműködni a hatósággal. Ennek során az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt, az informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

A biztonságáért felelős személy feladata, hogy kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal, a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet. Az információcsere és a Központ kárenyhítő intézkedései során a Hivatal együttműködni köteles.

Az elektronikus információs rendszerek biztonságáért felelős a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel (Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központ). Figyelemmel kíséri a kiadott tájékoztatókat, riasztásokat, a Hivatal informatikai rendszereit érintő események esetén értesíti az érintetteket, megteszi a szükséges teendőket.

1.7.2. Képzési eljárásrend

A jegyző feladata az elektronikus információs rendszerek biztonságáért felelőssel együttműködve az elektronikus információs rendszerhez hozzáféréssel rendelkező személyek (beleértve az elektronikus információs rendszerekkel kapcsolatba kerülő külső személyeket, pl. üzemeltetőket is) folyamatos oktatásának, képzésének elősegítése, az ajánlott elektronikus információbiztonsági eljárások, technikák és technológiák naprakészen tartása. Cél, hogy a felhasználók tudatában legyenek az információbiztonsági elvárásoknak és fenyegetettségeknek, illetve felelősségeiknek (pl. jelentési kötelezettségüknek).

A biztonság tudatosítása a felhasználók esetében oktató anyagok terjesztésével és képzések útján történik,

melyről a jegyző gondoskodik. Az oktatási tematikákat és anyagokat az elektronikus információs rendszer biztonságáért felelős személy készíti, a jegyző véleményezi, szükség szerint a rendszergazda bevonásával. A képzés része az Ügymenet-folytonossági tervvel kapcsolatos tudnivalók oktatása.

1.7.3. Biztonság tudatosság képzés

A Hivatal annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói, vagy ahhoz hozzáféréssel rendelkezők számára.

A képzés szükséges:

- a. az elektronikus információs rendszer újonnan belépő felhasználói számára, a kezdeti képzés részeként (a munkába állást megelőzően),
- b. eltérő munkakörbe kerülés esetén, ha indokolt,
- c. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi,
- d. ismétlődően 3 évente,
- e. amikor a jegyző erre utasítást ad vagy erre vonatkozóan utasítás, elrendelés érkezik (pl. biztonsági fenyegetettségkor, vagy biztonsági esemény bekövetkezését követően).

A jegyző biztosítja, hogy a Hivatal munkavállalói az informatikai biztonsági rendszer követelményeiről és az abban bekövetkezett esetleges változásokról megfelelő képzésben részesüljenek. Felelős a képzési kritériumok meghatározásáért, kinevezi a felelősöket, tevékenységüket felügyeli, gondoskodik a képzési szabályok betartásáról, biztosítja a képzéshez a szükséges erőforrásokat, dönt a képzési szabályok elfogadásáról, a szükséges intézkedésekről, figyelemmel kísérisi feladatokról.

Az elektronikus információs rendszerek biztonságáért felelős feladata az érintettek, felhasználók számára az informatikai biztonsági tudatosság megszerzéséhez, szintentartásához szükséges oktatási anyag összeállítása, naprakészen tartása. Az oktatási anyag része az Ügymenet-folytonossági tervben meghatározott intézkedések tudatosítása (minden alkalmazott ismerje, milyen esetben, és kit kell értesíteni katasztrófa esetén - ezek az információk mindenki számára elérhetőek a belső hálózaton).

Az Ügymenet-folytonossági tervben speciális feladatokat ellátók (pl. döntések meghozataláért felelős vezetők, informatikai alkalmazásokért, hardver, szoftver eszközökért felelősök) külön képzésben részesülnek, melynek keretében egyeztetésre kerülnek az általuk elvégzendő feladatok.

Az oktatási anyagnak kellő mélységű gyakorlati ismereteket is kell tartalmaznia. Az oktatási anyag összeállítása során fel kell használni a rendszergazda rendszerüzemeltetési tapasztalatait (felmerült problémák, informatikai incidensek kezelése, megelőző intézkedések).

Az elektronikus információs rendszerek biztonságáért felelős gondoskodik a képzési intézkedések, kontrollok szabályozásokba, dokumentációs rendszerbe illesztéséről.

A munkatársak felelősek a közzétett, illetve számukra kiadott előírások betartásáért, az oktatásokon átadott ismeretek elsajátításáért, lehetőség szerinti fejlesztéséért önképzéssel. Feladatuk az informatikai biztonság tudatosítása, fejlesztése érdekében javaslatainak eljuttatása felettesei vagy az elektronikus információs rendszerek biztonságáért felelős felé. A belső oktatásokon, illetve a jogszabály vagy hatóság által elrendelt éves továbbképzéseken kötelező a részvétel, amelyről részvételi nyilvántartást kell vezetni.

1.7.4. Belső fenyegetés

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

1.7.5. Szerepkör, vagy feladat alapú biztonsági képzés

A Hivatal szerepkör vagy feladat alapú biztonsági képzést szervez, nyújt vagy biztosít az egyes szerepkörök szerinti, azért felelős személyeknek:

- a. az elektronikus információs rendszerhez való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően;
- b. amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi;
- c. a Hivatal által meghatározott rendszerességgel

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

Az új munkavállalók a betanulási időszak alatt személyre szabott program alapján a szervezeti egység vezető vagy az általa kijelölt személy közreműködésével sajátítják el a szükséges ismereteket. Akkor lehet önálló munkával megbízni, ha a munkavállaló megfelelő gyakorlatot szerzett és a felelős meggyőződött a felkészültségéről. Az új munkavállaló képzése során gondoskodni kell az informatikai biztonsággal kapcsolatos képzéséről, tudatosításáról. Meg kell ismertetni a rá vonatkozó informatikai biztonsággal kapcsolatos előírásokkal, szabályzatokkal.

Az informatikai rendszerekhez felhasználói jogosultságot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal információbiztonsági szabályait. Az új munkavállaló munkaköréhez szükséges felhasználói jogosultságait a vonatkozó eljárásrend kell kiadni.

A felhasználót az azonosító(k) átadását megelőzően oktatásban kell részesíteni a használat feltételeiről és szabályairól, meg kell ismertetni a rá vonatkozó informatikai biztonsággal kapcsolatos előírásokkal, szabályzatokkal. Az oktatás *Oktatási tematika* vagy egyéb dokumentum alapján vagy e-learning módszerrel történhet.

Szakrendszerhez kapcsolódó felhasználói azonosító átadását megelőzően a felhasználót oktatásban kell részesíteni az adott szakrendszer használatáról. Az oktatás, a betanulási időszakban az új munkavállaló szakrendszerben végzett munkájának fokozott ellenőrzése a megbízott szervezeti egység vezető vagy a jegyző által kijelölt felelős feladata. Az új bevezetésű szakrendszerek felhasználóinak (pl. ASP keretrendszer és szakrendszerek) részt kell venni az előírt oktatásokon, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják.

A Hivatal azoknak a munkatársaknak, akiknek az idevonatkozó törvény és jogszabályok előírják, külső képzést biztosít. A képzéseket az erre szolgáló központi alkalmazással tervezni szükséges, melynek felelőse a jegyző vagy az általa megbízott felelős.

Új szabályozás vagy a szabályozás jelentős változása esetén az érintetteket képzésben kell részesíteni, a szabályzatot, szabályozást, az abban foglaltak megismerését, tudomásulvételét, betartását Megismerési nyilatkozaton vagy egyéb feljegyzésen kell dokumentálni.

Az oktatásokat úgy kell szervezni, hogy minimálisan három évente egyszer ismétlő, frissítő ismereteket kapjanak a munkatársak. Az új belépő munkatárs oktatását a munkakörétől függően, a lehető legrövidebb időn belül kell elvégezni. Rendkívüli oktatást kell tartani, ha biztonsági vagy egyéb incidens történik, a rendkívüli

oktatást a jegyző a rendszergazda vagy az elektronikus információs rendszerek biztonságáért felelős javaslata alapján rendeli el.

Az lbtv. által előírt, az elektronikus információs rendszerek biztonságáért felelős vezető, felelős személy(ek), valamint a feladatok ellátásában résztvevő személy(ek) számára a vonatkozó jogszabály kötelező képzést ír elő. A továbbképzéseket (belépő képzések) és az éves továbbképzéseket (ismétlődő képzések) a Nemzeti Községi Egyetem szervezi.

Az elektronikus információs rendszerek védelméért felelős vezető (a jegyző) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet alapján képzésre és éves továbbképzésre kötelezett.

Amennyiben nem megfelelő jogosultsággal rendelkező munkatárs vagy külső szakértő látja el az elektronikus információs rendszerek biztonságáért felelős feladatait, a kijelölt személy beiskolázásáról is gondoskodni kell. A szakirányú továbbképzés beiskolázási feltételeit a rendelet tartalmazza.

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

1.7.6. A biztonsági képzésre vonatkozó dokumentációk

A Hivatal dokumentálja a biztonságtudatosságra vonatkozó alap-, és szerepkör alapú biztonsági képzéseket, a képzésen résztvevőkkel a képzés megtörténtét elismerteti, és ezt a dokumentumot megőrzi. A belső képzésről dokumentum születik, mely tartalmazza a képzés helyét, tárgyát, idejét, stb. és a résztvevők illetve oktató aláírásait. Az oktatásokkal kapcsolatos dokumentumokat a kijelölt képzésért felelős kezeli, tárolja. A belső képzéseken túl a külső képzésekről a részvételi, ill. látogatási igazolást és egyéb dokumentumokat, a kapott bizonyítványokat is archiválja a személyi anyagban, melyet zárt tűzvédtett páncélszekrényben tárol. A képzési dokumentációk megtekintését a Hatóságoknak biztosítani kell.

FIZIKAI VÉDELMI INTÉZKEDESEK

2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

2.1.2. 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 elektronikus információs rendszer biztonságáért felelős a jegyző és a rendszergazda közreműködésével kidolgozta a Hivatal fizikai védelmére vonatkozó eljárásrendet. Az informatika biztonsági rendszer rendkívüli módosításakor, vagy biztonsági esemény bekövetkeztekor, de legalább évente az eljárásrendet újra kell vizsgálni, szükség szerint módosítani.

A fizikai védelemmel kapcsolatos további eljárásokat (pl. egyedi kulcskezelési előírásokat) az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza.

A Hivatalnak figyelembe kell vennie a külső szolgáltató, ill. jogszabály alapján kijelölt szolgáltató által meghatározott biztonsági osztály értékét, és a szolgáltatóval történő megállapodás (szerződés) vagy a tőle

kapott tájékoztatás alapján a rá vonatkozó biztonsági követelményeket teljesítenie kell.

Az eljárásrend kidolgozása és alkalmazása során figyelemmel kell lenni a más jogszabályban meghatározott tűz-, és személyvédelmi, valamint a személyes adatok kezelésére vonatkozó rendelkezésekre (a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR)).

A védelmi eljárásrendnek ki kell terjednie az elektronikus információs rendszerek szempontjából érintett létesítményekre, helyiségekre. Az informatikai infrastruktúra különböző funkcionális területeinek optimális megválasztásával lehetőség van a fizikai biztonságot veszélyeztető fenyegetések csökkentésére. A Hivatal szakfeladataihoz kapcsolódó elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni. Ezen elektronikus információs rendszereknek helyt adó helyiségekre vonatkozóan jogszabályi és hatósági elvárás, hogy legyen kialakítva az objektum védelme beléptető, behatolás védelmi, tűzjelző és lehetőség szerint videó-megfigyelő rendszer. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (szerverhelyiség) szükség esetén biztosítani kell a megfelelő környezeti feltételeket. A bárki által szabadon látogatható, vagy igénybe vehető publikus területekre nem vonatkoznak a fizikai és környezeti biztonsági követelmények.

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

Ha a Hivatal az lbtv.-ben meghatározott határidőkkel nem tudja teljesíteni az informatikai biztonsági követelmények megvalósítását, akkor a hiányosságokról Intézkedési tervet készít és rendelkezik annak megvalósításáról (lásd. *1. 1.3. Az intézkedési terv és mérföldkövei*).

2.1.3. Fizikai belépési engedélyek

A Hivatalhoz tartozó épületek, helyiségek biztonsági zónákhoz történő hozzárendelése lehetővé teszi a belépésvédelemmel kapcsolatos intézkedések hatékony végrehajtását a mindenkori védelmi igény függvényében (összhangban a jogszabályi és a hatósági elvárásokkal).

Az elvárt fizikai védelem érdekében a Hivatal a különböző funkcionális területeit biztonsági zónákba sorolja, melyek elhelyezkedésére a hagymahéj-elv a jellemző. Kívül találhatóak a nyilvános területek, majd az alacsony biztonsági igényű területek. Védett területként ezen belül az informatikai infrastruktúra és más fokozottan védendő helyiségek, majd azon irodai helyiségek, amelyekben lehetőség nyílik bizalmas, nagymennyiségű személyes információkhoz való hozzáféréshez (a központi IT- és ellátó infrastruktúra helyisége(i), irattár(ak)). A zónák között lehetőség szerint biztonsági határvonalak (zárt, ellenőrzött áthaladási pontok, ajtók) helyezkednek el.

A szabályzat magában foglalja a biztonsági zónák definícióját, ami a belépésre jogosult személyek, a belépésvédelemmel szemben támasztott követelmények meghatározásának alapjául szolgál.

Ehhez az alábbi biztonsági zónák kerültek meghatározásra:

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). Belépési jogosultsággal a Hivatal minden munkatársa rendelkezik. Látogatók/ügyfelek csak kíséret és felügyelet mellett.
2. biztonsági zóna	Magas biztonsági követelmények	A Hivatal szakfeladatait támogató elektronikus információs rendszereinek (pl. ASP, anyakönyv, választási, egyéb szakrendszereknek) helyt adó helyiségek 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, NTG hálózati eszközöket). A belépés kizárólag a rendszergazdának, üzemeltetésért felelősnek engedélyezett, egyéb személyek, kizárólag indokolt esetben, felügyelettel léphetnek be és tartózkodhatnak ott.

A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségek (2. biztonsági zóna), illetve az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (3. biztonsági zóna) esetében biztosítani kell a jogszabály és a hatóság által elvárt fizikai védelmet.

A szakrendszerek munkaállomásainak helyiségei védelmére riasztórendszert kell kialakítani, pl.:

A helyiségekbe történő belépést úgy kell szabályozni és lehetőség szerint technikai eszközökkel épületbe lépésnél biztosítani, hogy csak a feljogosított személyek léphessenek be.

A jegyző a szervezeti egységek vezetőivel együttműködve meghatározza az egyes biztonsági zónákba (helyiségekbe) a belépésre jogosult személyek listáját. A jegyző a jogosultság kiosztását átruházhatja a

szervezeti egység vezetőjére (irodavezető).

Ahhoz, hogy az engedélyezett belépési jogosultságok ellenőrizhetőek legyenek, szükséges a Hivatalnak belépési jogosultságot igazoló dokumentumokat (pl. kitűzők) kell kibocsátania. A kulcsokhoz vagy kódhoz való hozzáfutás csak dokumentált módon történhet, a jogosultság kiosztását követően.

A jegyző, mint az elektronikus információs rendszerek védelméért felelős vezető a biztonságért felelőssel együttműködve meghatározza a kulcsok felvételére és leadására vonatkozó egyedi szabályokat, az illetékeséget, a kulcsok megőrzési rendjét (ha készül, az *Informatikai biztonsági eljárásrend* vagy egyéb dokumentum tartalmazza).

Állandó belépési jogosultságot alapesetben csak a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes személyek (pl. közszolgálati jogviszony, munkaviszony alapján foglalkoztatott munkatársak) kaphatnak. Külső személyek (pl. képviselők, intézményvezetők, projektmunkához foglalkoztatottak, stb.) számára indokolt esetben, meghatározott munkára és/vagy időtartamra szükséges belépési jogosultságot csak a feladat elvégzéséhez helyéhez kötötten (az adott irodai helyiségekre vonatkozóan) lehet kiadni.

A jóváhagyást és átvételt dokumentálni kell. A kulcsot vagy kódot a jegyző vagy az által kijelölt felelős (pl. rendszergazda) adja ki és tartja nyilván. A belépésre jogosultak listáját a jegyző folyamatosan felülvizsgálja. A nyilvántartás vezetésére kijelöltnak az érvénytelen/megszűnt jogosultságokat dokumentálnia kell. Jogosultság-visszavonás esetében gondoskodni kell a Hivatal által kiadott kulcsok, kitűzők visszavonásáról, megsemmisítéséről, törléséről. Új jogosultság igénye esetén a jegyző döntésének megfelelően kell eljárni.

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

2.1.4. 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 kíséretet mellett lehetséges. Ezekre a bejáratokra lehetőség szerint kerüljön felszerelésre proximity kártyás beléptető ajtó vagy kódzár. Ennek hiányában a nem az ügyfélforgalom számára kijelölt 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 kizárólag kísérettel mehetnek be és tartózkodhatnak ott (a fogadónak kell kísérni). A látogatót, ügyfelet fogadó munkatárs felelős a látogatóért, annak minden, az információbiztonságot veszélyeztető tetteért. Elvárás, hogy a szakrendszerek és központi infrastruktúra helyiségeibe történő látogatói, ügyfél belépésekről információkat kell gyűjteni és megőrizni (lásd 2.1.8. *A látogatók ellenőrzése*).

A nyilvános ügyfélterületeken kívüli védett területeken (a szakrendszerek helyiségeiben) felügyelet nélkül tartózkodó, ismeretlen személyeket meg kell szólítani, nem szabad egyedül hagyni, személyesen kell a meglátogatandó személyhez kísérni. Egyedi mérlegelést követően vizsgálatot kell indítani, indokolt esetben felelősségre vonás alkalmazható azzal szemben, aki belépést biztosított/felügyelet nélkül hagyta az ügyfelet, látogatót, vagy a helyiséget.

Azokban az esetekben, amikor az épületbe karbantartási (akár épület, akár eszköz), vagy ellenőrzési célból érkeznek, a szervezeti egység vezető vagy az általa kijelölt személynek (informatikai jellegű esetekben a rendszergazdának) kísérnie kell ezeket a személyeket is és figyelemmel kell követnie a tevékenységüket.

A karbantartó szervezetekről, személyekről folyamatosan aktualizált nyilvántartást kell vezetni (lásd 2.1.19. *Karbantartók*), kizárólag az engedélyezett karbantartók rendelkezhetnek a munkavégzés idejére belépési jogosultsággal.

A Hivatal takarítását végző személyek nem takaríthatnak felügyelet nélkül az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (pl. szerverszoba, NTG hálózati végpont).

Az 1. ép. 2. biztonsági zóna helyiségeinek legalább kulccsal (a kulcs ne legyen a zárban) és 3. biztonsági zóna helyiségeinek 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.

Vészhelyzetek esetére a kulcs vagy kód másodpéldányát a titkárságon vagy portán (ha van) védett helyen, pl. pánccsaszekrényben vagy zárt kulcsszekrényben kell elhelyezni lezárt, hitelesítéssel ellátott borítékban vagy lepecsételhető kulcsdobozban. A kulcsdoboz vagy boríték rendkívüli felnyitásáról a felhasználónak telefonon és írásos feljegyzésben értesítenie kell a szervezeti egység vezetőjét. A hitelesítéssel ellátott boríték felnyitását, a kód használatát követően a kódot meg kell változtatni.

A rendszergazdának vagy a kijelölt felelősnek meghatározott rendszerességgel (minimum éves gyakorisággal) meg kell változtatni 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).

2.1.5. Hozzáférés az adatátviteli eszközökhöz és csatornákhöz

A Hivatal a fizikai védelmi eljárásrend szerint ellenőrzi az elektronikus információs rendszer adatátviteli eszközeinek és kapcsolódási pontjainak helyt adó helyiségekbe történő fizikai belépést.

A fizikai belépések naplózása szükséges az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. szerverszoba) esetében.

A központi IT rendszereket (beleértve az aktív eszközöket, routereket) is felügyelt biztonsági zónában, vagy ha a fizikai adottságok miatt nem lehetséges, akkor folyamatos felügyelettel és vagyonvédelmi rendszerrel (lehetőség szerint kameraképet rögzítő kamerarendszerrel is) védeni kell, valamint folyamatosan zárva tartott (rack-) szekrényben/védett magasságban kell elhelyezni. A (rack-) szekrény kulcs átvételét, leadását az eljárásrendben előírt módon dokumentálni kell (elvárás, hogy a kulcs felvételének, leadásának vagy a helyiségben tartózkodásnak a tényét - az időpont feltüntetésével - a felvételre jogosult/megőrzésre kijelölt/nyilvántartásra kötelezett az erre a célra szolgáló nyilvántartási naplóban aláírásával igazolja).

A helyiségekbe állandó belépéssel, kulcs felvételére jogosultsággal kizárólag a rendszergazda, illetve a karbantartásra jogosultak rendelkeznek (lásd 2.1.19. *Karbantartók*).

2.1.6. 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 illetéktelen hozzáférés megakadályozható (harmadik fél, ügyfél és látogatók részére nem hozzáférhetőek).

Lehetőség szerint úgy kell beállítani a kimeneti eszközöket, hogy a munkafolyamat azonosítható legyen (pl. a nyomtatóknál kód használata). Nyilvános zónában védett nyomtatás beállítása (PIN kóddal védett dokumentum nyomtatása) szükséges.

A szkennelt dokumentumok bizalmasságának védelmére érdekében hitelesítést igénylő FTP kapcsolaton keresztül szükséges megoldani a szkennelést, hitelesítést igénylő megosztott mappa beállítása (jelszóval védett mappába mentés), vagy ha nem lehetséges, akkor a szkennelt mappa tartalmának rendszeres

automatikus törlése szükséges.

Lehetőség szerint alkalmazni kell az „Üres íróasztal - tiszta képernyő” szabályt:

- a. a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
- b. a felhasználó a számítógépét zárolni köteles, ha azt rövidebb időre őrizetlenül hagyja;
- c. hosszabb idejű távoliet esetén a számítógépből ki kell jelentkezni, illetve ki kell azt kapcsolni;
- d. a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a számítógépet;
- e. munkavégzés után minden érzékeny információt tartalmazó anyagot (papír alapú anyagokat, valamint elektronikus adathordozókat) el kell tenni az asztalokról, és zárható irodabútorban kell tárolni;
- f. gondoskodni kell arról, hogy a nyomtatókból, faxokból, fénymásolókból kijövő dokumentumokhoz illetéktelenek ne férjenek hozzá;
- g. ügyelni kell arra, hogy érzékeny információt tartalmazó dokumentumot ne felejtünk a fénymásolóban, a kinyomtatott, faxolt vagy másolt dokumentumokat nem szabad őrizetlenül az eszközökben hagyni;
- h. a hibásan nyomtatott, nem használt dokumentumokat meg kell semmisíteni (pl. iratmegsemmisítő);
- i. be kell tartani a fizikai biztonságra vonatkozó követelményeket (pl. ügyfelet ne hagyjunk felügyelet nélkül az irodában).

2.1.7. A fizikai hozzáférések felügyelete

A rendszergazda vagy a jegyző által kijelölt felelős a 2. és 3. biztonsági zóna szerinti - magas és kritikus biztonsági követelményű - 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.

2.1.7.2. Behatolás riasztás, felügyeleti berendezések

A fizikai behatolás riasztások és a felügyeleti berendezések felügyeletére hatósági engedéllyel rendelkező távfelügyeleti szolgáltatóval kell szerződést kötni. Biztosítani kell, hogy a vagyonvédelmi rendszer behatolás- és műszaki jelzései automatikusan átjelzésre kerüljenek (lehetőség szerint független kommunikációs csatornán, pl. GPRS vagy rádiós átjelzéssel), a távfelügyeleti szolgáltató biztosítsa az intézkedésre jogosultak és szükség esetén a hatóságok értesítését (rendőrség, tűzoltóság). A műszaki felügyelet része a rendszer működését biztosító feltételek (pl. kommunikáció) meglétének folyamatos ellenőrzése.

A vagyonvédelmi rendszereknek (riasztó- és beléptetőrendszereknek) olyan eseménynaplókat kell tárolnia, mely biztonsági esemény bekövetkezése esetén a vizsgálathoz adatot szolgáltat. A riasztórendszer telepítésekor vagy felülvizsgálata során be kell állítani a teljes eseménynaplózást (beleértve a nyitás-zárás naplózást, a beérkező nyitás-zárás jelzések rögzítését, tárolását). A biztonsági rendszerek adatait a jogszabályok által megengedett maximális megőrzési időig archiválni kell.

A vagyonvédelmi rendszerek eseménynaplóit a szervezeti egység vezetőjének utasítására indokolt esetben a kijelölt szakértőnek (rendszergazdának, a riasztórendszer karbantartásával megbízott szakértőnek vagy kiemelt jogosultsággal (mesterkóddal) rendelkező személynek) át kell vizsgálnia. Szükség esetén ki kell kérni a távfelügyeleti szolgáltató által rögzített eseményeket.

A fizikai hozzáférésekről készült naplók meglétét a rendszergazdának vagy a kijelölt személynek az előírt időközönként (minimálisan az éves ellenőrzések alkalmával) ellenőrizni szükséges.

2.1.8. A látogatók ellenőrzése

A Hivatalnak a 2. és 3. biztonsági zóna szerinti helyiségekbe (szakrendszerek és központi infrastruktúra helyiségeibe) történő látogatói, ügyfél belépésekről információkat kell gyűjteni és megőrizni.

A nyilvántartást a jegyző utasításának megfelelően az ügyfél- portaszolgálat munkatársa vagy a látogatót/ ügyfelet fogadó ügyintéző vezeti, a nyilvántartás legalább az alábbiakat tartalmazza:

- a. dátum,
- b. látogató/ügyfél neve,
- c. ügyfajta, vagy ügyintéző neve.

A megőrzési időt a kockázattal arányosan a jegyző határozza meg (eltérő rendelkezés hiányában 3 hónapban), a selejtezésekről jegyzőkönyvet kell készíteni és megőrizni.

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. A Hivatal területén az elektronikus információs rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak a jegyzőnek vagy az erre a feladatra kijelölt felelősnek a tájékoztatása után, annak jóváhagyásával és felügyeletével lehet végezni.

Az elsődleges áramforrás kiesése esetére azokra a rendszerekhez, ahol az indokolt vagy elvárt (pl. szerverfunkciójú számítógépek, adatmentő szerverek, NTG hálózati eszközök), az eszközök szabályos leállításához a tevékenységhez méretezett, rövid ideig működőképes szünetmentes áramellátást kell biztosítani.

2.1.12. Tűzvédelem

A Hivatalnak az elektronikus információs rendszereknek helyt adó irodákban, helyiségekben, szerverszobában (2. és 3. biztonsági zóna szerinti helyiségekben) független áramellátással támogatott észlelő berendezést (füstérzékelőt) szükséges alkalmazni.

A füstérzékelők jelzéseit a vagyonvédelmi rendszer részeként hatósági engedéllyel rendelkező távfelügyeleti szolgáltató felügyeleti rendszerére kell csatlakoztatni (automatikus, lehetőség szerint független kommunikációs csatornán, pl. GPRS vagy URH rádiós átjelzéssel).

A távfelügyeleti szolgáltatónak biztosítani kell tűzjelzés esetén a hatóság (tűzoltóság) és az intézkedésre jogosultak értesítését.

Az informatikai eszközök központi helyiségeibe (elosztó-, szerverhelyiségekbe) és ahol az tűzvédelmi szempontból indokolt, minimális elvárás a tanúsított gázzal oltó (CO²) hordozható, kézi tűzoltó készülék biztosítása (az elektromos tüzek oltására nem megfelelő a porral oltó készülék).

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

A Hivatalnak védenie kell a 2. és 3. biztonsági zónában lévő elektronikus információs rendszereket, rendszerelemeket a csővezeték rongálódásból származó károkkal szemben, biztosítva, hogy a főelzárószelepek hozzáférhetőek, és megfelelően működnek, valamint a kulcsszemélyek számára ismertek.

Lehetőség szerint az informatikai erőforrásokat koncentráltan tartalmazó helyiségek (pl. szerver szoba, NTG végpont) tervezése, elhelyezése során biztosítani kell, hogy az a víz-, és más hasonló kártól védett legyen.

2.1.15. Be-és kiszállítás

A jegyző utasításának megfelelően a szervezeti egység vezető, vagy megbízására a rendszergazda engedélyezi vagy tiltja a Hivatal területére bevitt, onnan kivitt információs rendszerelemeket. Az eszközök igénylését a megbízott szervezeti egység vezetőhöz vagy a rendszergazdához kell benyújtani.

A Hivatal tulajdonában lévő, a Hivatalból kiszállításra engedélyezett eszközökről nyilvántartást (jegyzőkönyvet, átvételi elismervényt) kell írni vagy elektronikus nyilvántartást vezetni, amely egyértelműen tartalmazza a kiadott eszköz jellemzőit és a kiadással járó felelősségeket. Az eszköz visszaszolgáltatásakor a visszavevőnek meg kell győződnie arról, hogy az megfelel a kiadáskori állapotának.

Behozott eszköz esetében az üzem behelyezést megelőzően a rendszergazdának 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 rendszergazda vagy a kijelölt felelős 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, ha szükséges az azonosításhoz),
- 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,
- 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).

Az eszköz szervizbe történő szállítása esetén jegyzőkönyvet kell készíteni, és a rendszergazdának az adathordozókra vonatkozó adatvédelmi szabályoknak megfelelően kell eljárnia (Lásd.3.8 *Adathordozók védelme*). A szerviz által kiadott szállító levelet a hardver nyilvántartásokkal együtt meg kell őrizni.

Az infokommunikációs eszközök használata során tilos:

- a. az eszközt illetéktelen személynek átengedni,
- b. az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni és
- c. az eszközt - hordozható infokommunikációs eszközök kivételével - a telepítési helyéről elmozdítani és elvinni az üzemeltető engedélye és közreműködése nélkül.

A Hivatal más szervezettel adat- és programcserét kizárólag írásos nyilatkozat alapján bonyolíthat, amelyben utalni kell az érzékeny adatok kezelésére is.

A csere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni:

- a. az adatátvitel, -feladás, -fogadás és -átvétel ellenőrzésének és bejelentésének eljárási szabályait,
- b. az adatok biztonságos átvitele előkészítésének és tényleges átvitelének műszaki szabványait,
- c. az adatvesztéssel kapcsolatos kötelezettséget és felelősséget,
- d. az adatátvitel során a biztonságos - szükség esetén titkosított - környezet előírásait minden érintett félnél,
- e. az érzékeny adatok védelméhez szükséges speciális eszközök igénybevételét.

Az adatcsere esetében:

- a. épületen kívüli szállítást csak az önálló szervezeti egység vezetője rendelhet el,
- b. az átadás-átvételtől jegyzőkönyvet kell felvenni,
- c. a szállításhoz egyszerre több személynek kell jelen lennie,
- d. épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell kiválasztani,
- e. tömegközlekedési eszközön adathordozó nem szállítható,
- f. épületen kívüli szállítás esetén megfelelő tárolóeszközt szükséges használni, és
- g. épületen kívüli szállítás esetén az adatokat titkosított formában kell az adathordozóra rögzíteni, és a titkosítás feloldásához szükséges kulcsot külön csatornán kell eljuttatni a címzetthez, elektronikusan rögzített adatokat tartalmazó mágneses adathordozó szállításakor el kell kerülni a nyilvánvalóan erős mágneses tereket,
- h. a szállítás során a vagyonbiztonság érdekében fokozott figyelemmel kell eljárni,
- i. az adathordozót nem lehet őrizetlenül hagyni,
- j. az adathordozókat óvni kell a fizikai sérülésektől,
- k. az adathordozókon a minősítési szintet megváltoztathatatlanul kell feltüntetni.

Rendkívüli esemény esetén a szállítást elrendelő szervezeti egység vezetőjét - szükség esetén a rendőrséget is - értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében szükséges intézkedéseket, valamint ezzel egy időben tájékoztatnia kell az elektronikus információs rendszer biztonságáért felelős személyt az eseményről és a megtett intézkedésekről.

Megfelelő technikai eljárásokkal és ellenőrzőeszközökkel gondoskodni kell a távközlési és adatátviteli eszközökön keresztül kicserélt információk védelméről. Ennek során figyelembe kell venni, hogy a távközlési eszközökben bekövetkező üzemzavar, az eszközök túlterheltsége vagy a kapcsolat kimaradása esetén a folyamatos üzletmenet megszakadhat, valamint illetéktelen személyek is hozzáférhetnek a különböző információkhoz.

2.1.16. Az elektronikus információs rendszer elemeinek elhelyezése

A Hivatal a lehetőségeihez mérten törekszik az elektronikus információs rendszerek elemeinek elhelyezése során arra, hogy a legkisebb mértékre csökkentse a fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét. Ide tartozik a helyiségek átszervezése, ez ügyfélforgalom optimalizálása, a fokozott védelmet igénylő informatikai rendszerek (pl. szerverhelyiségek, ASP, választási, anyakönyvi szakrendszerek) ügyfélforgalomtól elkülönített elhelyezése.

Az irodahelyiségekben az íróasztalokon rendet kell tartani. Csak a munkához felhasznált iratok, adathordozók lehetnek az asztalokon. Munkavégzés után az íróasztalokról az adathordozókat, munkához felhasznált iratokat zárható szekrénybe szükséges elhelyezni. Lásd 2.1.6. *A kimeneti eszközök hozzáférés ellenőrzése.*

Ha a monitoron személyes, 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 táblákon, flipchart-okon hagyott információkat a terem elhagyása előtt törölni kell,
- c. a tárgyalóteremben is alkalmazni kell a "Tiszta asztal" szabályt.

2.1.19. 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 megfogalmazásra 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 jegyző által kijelölt felelősnek (elektronikus információs rendszerek biztonságáért felelősnek vagy rendszergazdának) nyilvántartást kell vezetnie a karbantartó szervezetekről/személyekről, elérhetőségeikről, azok jogosultságairól (szükség szerint a karbantartandó eszközökről), melyet változások esetén aktualizálnia kell.

Amennyiben a harmadik fél logikai hozzáférést kap, további szerződéses követelményt a *Harmadik felekkel szembeni szerződéses követelmények dokumentum* tartalmaz.

2.1.19.3. 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.

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 *Szerepkörök, tevékenységek, felelősségek* fejezetben határozta meg az információbiztonsággal összefüggő szerepköröket, tevékenységeket, felelősségeket. Az elektronikus információbiztonsági engedélyezési folyamatokat kockázatkezelési eljárásban rögzíteni kell, összhangban jelen szabállyal. Felügyelni kell az elektronikus információs rendszer és környezet biztonsági állapotát.

A jogszabály által kijelölt központi adatkezelő informatikai rendszerére vonatkozó engedélyezési szabályok: Központi rendszerekben, pl. az önkormányzati ASP rendszerben fejlesztői, tesztelési, üzemeltetői, működtetői tevékenységet csak a központi adatkezelők vagy a jogszabály által kijelölt szolgáltatók (pl. az önkormányzati ASP rendszerről szóló 257/2016. (Vili. 31.) Korm. rendeletben), említett szereplők végeznek, illetve végeztetnek.

3.1.3. 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.

3.1.3.2. Belső rendszerkapcsolatok

A Hivatal belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását.

3.1.3.3. Külső kapcsolódásokra vonatkozó korlátozások

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.

3.1.4. Személybiztonság

Minden, a személybiztonsággal kapcsolatos eljárás vagy elvárás kiterjed a Hivatal teljes személyi állományára, valamint minden olyan természetes személyre, aki a Hivatal elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülni.

A Hivatal szerződéses partnereivel, harmadik felekkel szembeni elvárásokat, kötelezettségeket a tevékenységet képező, jogviszonyt megalapozó szerződésekben, megállapodásokban kell érvényesíteni. Meg kell ismertetni és el kell fogadtatni a szerződéses partnerekkel, harmadik felekkel a Hivatal szabályzatait, eljárásrendjeit, titoktartási kötelezettségekre vonatkozó feltételeket.

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 is.

A Hivatal minden érintett szervezeti munkakört, vagy a szervezethez kapcsolódó feladatot besorol az 1.6.2 *Munkakörök, feladatok biztonsági szempontú besorolása* fejezetben leírtaknak megfelelően a hozzáférési jogosultság megadása előtt. Az 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.

Amennyiben a harmadik fél logikai hozzáférést kap, további szerződéses követelményt a *Harmadik felekkel szembeni szerződéses követelmények dokumentum* tartalmaz.

3.2. TERVEZÉS

3.2.2. Rendszerbiztonsági terv

A Hivatalnak saját hatáskörébe 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 hatáskörét, 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. 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 elektronikus információs rendszer biztonságáért felelős feladata.

Az elektronikus információs rendszer rendszerbiztonsági tervet 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 feltárássra.

3.2.3. Cselekvési terv

A Hivatal az elektronikus információs rendszer biztonságáért felelőssel együttműködve 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 mérföldkövet 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. 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.

A cselekvési tervnek minimálisan tartalmaznia kell:

- a. megvalósulatlan védelmi intézkedés (meghatározott biztonsági osztályhoz tartozó OVI-úrlapból a „nem valósult meg” sorok), bevezetett hibás/hiányos kontrollok, elektronikus információs rendszer ismert sérülékenységei, lehetőség szerint a kockázatelemzés eredményének sorrendjében,
- b. tervezett intézkedés (szükséges/javasolt feladat),
- c. intézkedés hatóköre (pl. szervezeti egység),
- d. kijelölt felelős,
- e. tervezett határidő.

A cselekvési tervben foglalt, a szükséges védelmi intézkedések bevezetéséhez szükséges erőforrásokat a Hivatalnak biztosítani kell.

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

A védelmi intézkedések megvalósulását a Hatóság számára a *NEIH-OVI Osztályba sorolás és védelmi intézkedés úrlappal* 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 elektronikus információs rendszer biztonságáért felelős, és az általuk kijelölt személyek (beleértve a kitűzött feladatok bevezetéséért felelősöket) 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 elektronikus információs rendszer biztonságáért felelős 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.

3.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

Jelen eljárást abban az esetben kell alkalmazni, ha a Hivatal saját hatókörében informatikai szolgáltatást, vagy eszközöket (elektronikus információs rendszert, rendszerelemet) szerez be, rendszerfejlesztési tevékenységet végez, vagy végeztet. A beszerzésre vonatkozó követelmény alkalmazása szempontjából nem minősül beszerzésnek a jellemzően kis értékű, kereskedelmi forgalomban kapható általában irodai alkalmazások, szoftverek, vagy azok a hardver beszerzések, amelyek jellemzően a tönkrement eszközök pótlása, vagy az eszközpark addigiakkal azonos, vagy hasonló eszközökkel való bővítése céljából, valamint a javítás, karbantartás céljára történnek. Nem minősül fejlesztésnek a kereskedelmi forgalomban kapható szoftverek beszerzése és frissítése.

3.3.2. A rendszer fejlesztési életciklusa

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

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, amelyet az érintettek felé kommunikálni szükséges.

3.6. KONFIGURÁCIÓKEZELÉS

3.6.1. 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.

A elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért felelős végzi, tartja naprakészen. Minden más esetben, legalább évente egyszer felül kell vizsgálni, mind az eljárásrendet, mind pedig a nyilvántartást.

3.6.2. Alap konfiguráció

A rendszergazdának vagy a Hivatal vezetője által kijelölt felelősnek szükség esetén az elektronikus információs rendszerek biztonságáért felelőssel együttműködve az információs rendszerekhez egy-egy alapkonfigurációt szükséges készítenie, amelyet dokumentáltan, bizalmasan naprakészen kell tartani. Az alapkonfiguráció frissítését az elektronikus információs rendszerelemek telepítésének és frissítéseinek szerves részeként kell elvégezni. Az alapkonfiguráció kiterjed valamennyi, hardver és szoftver elemre (beleértve a menedzselhető eszközöket is), valamint telepítő dokumentációkra /leírásra, azok változásaira.

Bármilyen változásnak, ami módosítja a konfigurációs nyilvántartás tartalmát, felügyelet alatt kell lennie, amely a rendszergazda vagy a kijelölt felelős 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.

Biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemeket vagy eszközöket kell biztosítani azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják. Megfelelő biztonsági eljárásokat kell alkalmazni a külső helyszínen használt eszközök belső használatba vonásakor.

Az önkormányzati ASP rendszerről szóló 257/2016. (Vili. 31.) Korm. rendelet 2. melléklete tartalmazza az önkormányzati ASP rendszer szakrendszereinek használatához szükséges felhasználói (önkormányzati) munkaállomásokkal szembeni minimális elvárásokat. Ennek megfelelően kell kialakítani az informatikai infrastruktúra környezetet:

- a. Munkaállomás, laptop (szoftverekkel)
- b. Monitor
- c. Kártyaolvasó
- d. Nyomtató
- e. NTG csatlakozáshoz szükséges, hivatal oldali hálózati eszközök (rack szekrény, szünetmentes tápegység, switch)

Az ASP rendszerhez történő csatlakozáshoz kapcsolódóan el kell végezni a hálózat kiépítését, az eszközök beüzemelését (munkaállomások, nyomtatók, hálózati aktív eszközök), szoftverek telepítése, beállítása (pl. tűzfal).

3.6.7. Legsúlykebb funkcionális

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.

A legsúlykebb funkcionális biztosítása érdekében szükséges feladatok:

- a. szakfeladatokhoz kapcsolódó, engedélyezett internetelési politika kialakítása, szabályozás, szükséges beállítások (fehérlista, szakfeladatok működtetéséhez nem szükséges portok tiltása)

- b. nyitott portok felülvizsgálata, a szükségtelen portok bezárása,
- c. a szükséges portok fokozott felügyelete, naplózása (operációs rendszer, tűzfal, tűzfalport, Router és egyéb eszköz beállítások: a szükséges portokon kívül ne legyen nyitva port, az adott porton honnan fogadjon bejövő és hova engedélyezzen kimenő forgalmat),
- d. tűzfal konfigurálás: a gyakori portok internet irányából történő elérésének korlátozása (csak Magyarországról elérhető, csak megadott IP címekről elérhető, csak bizonyos felhasználó vagy felhasználók számára elérhető),
- e. üzemeltetéshez használt portok (SSH, RDP, Telnet, LDAP, NTP, SMB, stb.) külső hálózatról történő elérésének tiltása,
- f. IP alapú eszközök elkülönített címtartomány beállítása (IP telefonok, IP kamerák, stb.). Ha használatban van IP kamera, akkor IP címének a hivatali hálózatának IP címétől eltérő tartományba állítása szükséges (az eszközök nem használhatják a Hivatali IP cím tartományt). Javasolt dinamikus DNS szolgáltatás igénybevétele.
- g. nélkülözhető szoftverek, futtatói környezet eltávolítása (pl. JAVA)

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

3.6.8. Elektronikus információs rendszerelem leltár

A rendszergazdának vagy a jegyző által kijelölt felelősnek szükséges:

- a. nyilvántartást készítenie az elektronikus információs rendszer(ek) elemeiről,
- b. azt rendszeres időközönként, minimálisan évente felülvizsgálja és frissíti.

A leltár célja, hogy információval szolgáljon a Hivatalnál használt eszközökről, ahol lehetséges ezek alapkonfigurációjáról, a bekövetkezett változásokról, valamint szükségessé válhatnak a Hivatal számára a hatékony személyes anyagi felelősségre vonhatósághoz. 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 az elektronikus információs rendszerekhez vagy felhasználókhoz rendelve.

A leltárt szervezeti egységenként (hivatal, nemzetiségi önkormányzatok) szükséges elkészíteni (tartalmazni kell a rendszerelemek elhelyezési helyét), legalább a következőkre kell kiterjednie:

1. Felhasználói ICT eszközök: felhasználók által használt információs és kommunikációs technológia eszközök és az azokhoz kapcsolódó főbb információk (típus, operációs rendszer, elhelyezkedés, felhasználó).
2. Felhasználói alkalmazások, liszenszek: felhasználó oldali alkalmazások és azok funkciói, egyedi beállítások, liszenszek (szoftver megnevezése, liszensz típusa, liszenszszám).

Az eszközök hálózatra történő illesztéséről készüljön dokumentáció.

A nyilvántartás alapját képező, az elektronikus információs rendszerekhez kapcsolódó hardver és szoftver elemekről rendszerinformációs alkalmazással készített részletes elektronikus vagy papíralapú riportok megőrzése az azt készítő vagy tárolásért kijelölt felelős feladata.

Az elektronikus információs rendszerelem leltárt frissíteni kell az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában. A frissítés elvégzése vagy a változás jelzése a kijelölt felelős felé a

rendszergazda feladata.

3.1.3.3. Duplikálás elleni védelem

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

3.6.10. A szoftver használat korlátozásai

A Hivatal kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a reájuk vonatkozó szerződésbeli elvárásoknak és a szerzői jogi, vagy más jogszabályoknak.

A szoftver használat főbb szabályai a következők:

- a. a telepítések során figyelembe kell venni a konfigurációs változáskezelési folyamatra vonatkozó irányelveket;
- b. a rendszergazda felelőssége a mindenkor ügleti követelményeknek, valamint információbiztonsági követelményeket teljesítő szoftverek, alkalmazások telepítése. Más felhasználók szoftvertelepítési jogot nem kaphatnak;
- c. minden új és meglévő szoftver telepítése/frissítése esetében a kiadott telepítési / frissítési útmutatók az irányadók;
- d. tilos a Hivatal által üzemeltetett munkaállomásokra olyan szoftvert telepíteni, melyhez nincs a Hivatalnak liszensze, vagy (ingyenes liszensz esetén) amelyet a Hivatal nem engedélyez;
- e. a Hivatal által vásárolt szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek tilos, hacsak megfelelő licencszerződés ezt nem szabályozza 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 elektronikus információs rendszer biztonságáért felelős belső auditok keretében ellenőrzi. A Hivatal az elektronikus informatika biztonsággal kapcsolatos szoftverhasználatlaltal kapcsolatos további szabályokat Informatikai biztonsági eljárásrendben vagy egyéb dokumentumban kezelheti.

3.6.11. A felhasználó által telepített szoftverek

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

Az eszközök firmware/driver/szoftverfrissítése a legutolsó stabil változatnak megfelelően történjen meg (kivéve a kompatibilitási problémákat okozó frissítéseket (pl. JAVA).

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.

Azonon 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 jogosultságokra vonatkozó igényléseket, változásjelentőket és levelezéseket a szervezeti egységek vezetői kötelesek másodpéldányban megküldeni a rendszergazdának. A külső fél által biztosított informatikai szolgáltatások használata során az általa kiadott előírások szerint kell eljárni.

A szoftvereket és adatokat arra nem jogosult harmadik fél számára másolni és továbbadni tilos.

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

3.7. KARBANTARTÁS

3.7.1. 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 elektronikus információs rendszer biztonságáért felelős megfogalmazza és dokumentálja a rendszeres karbantartásra vonatkozó kontrollokat, mely szabályozza a rendszeres karbantartási folyamatot és elősegíti annak ellenőrzését.

A Hivatal az elektronikus információbiztonsággal kapcsolatos egyedi karbantartási szabályokat Informatikai biztonsági eljárásrendben vagy egyéb dokumentumban kezelheti.

3.7.2. Rendszeres karbantartás

A rendszeres karbantartásokat csak az arra jogosult személy(ek) végezheti(k) (a 2.1.14 *Karbantartók* fejezet szerint). 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:

- a. ütemezés (pl. előre ütemezett (tervezett), nem tervezett karbantartás),
- b. mikor történ a karbantartást (dátum, idő),
- c. a karbantartás megnevezése (ellenőrzés, javítás, frissítés stb.),
- d. az érintett eszköz/szoftver, rendszer megnevezése,
- e. módszer (pl. szemrevételezés),
- f. karbantartáshoz szükséges eszközök megnevezése,
- g. ki/kik végezte/ték a karbantartást,
- h. mennyi ideig tartott a karbantartás (ha lényeges),
- i. ha volt rendszerleállítás, mennyi ideig tartott,
- j. a karbantartás ellenőrzés tényét (sikeres, sikertelen),
- k. intézkedés megjelölése sikertelen karbantartás esetén,
- l. 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.

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.

3.7.3.2. 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.

3.7.4. 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).

Ha hatóság (pl. NISZ Zrt.) által nem tiltott, vagy technikailag lehetséges, akkor szükséges az engedélyezett hálózatok és hálózati szolgáltatások meghatározása, szükségesség/ engedélyezés esetén a meghatározott végpontok között VPN kapcsolat létrehozása, biztonságos protokollok (pl. üzemeltetési feladatok ellátásához a rendszerek VPN kapcsolaton keresztül történő elérés céljából).

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

- a. jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket,
- b. 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,
- c. hitelesítéseket alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásánál,
- d. lezárja a munkaszakaszt és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik,
- e. nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről.

3.8. ADATHORDOZÓK VÉDELME

3.8.1. 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 (Lásd 2.1.12. *Be- és kiszállítás*). Az adathordozó használatára való igényt a szervezeti egység vezetőjéhez kell benyújtani. A rendeltetésszerű eszközhasználatot a Hivatal elektronikus információs rendszereihez történő csatlakoztatás után, a rendszergazda szűrőpróbaszerűen ellenőrizheti.

Adathordozót, vagy adatot adathordozón/mobil eszközön (laptop, pendrive, floppy, CD stb.) - otthoni munkavégzés és bármilyen más célból - a Hivatalból kijuttatni csak a szervezeti egység vezetője írásos engedélyével szabad az információbiztonsági előírásoknak megfelelően. A Hivatal az adathordozók használatát a Hivatal szakfeladatait támogató szakrendszerek munkaállomásain információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozza, szakrendszerek munkaállomásain kívüli minden előzetes értesítés nélkül figyelheti, monitorozhatja.

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 („tisztasztal” 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.

Bármely adathordozó eltűnését azonnal jelenteni kell a szervezeti egység vezetőjének azzal az információval

együtt, hogy milyen Bizalmas/Szigorúan Bizalmas minősítésű dokumentum kompromittálódott.

Az adathordozók védelme során figyelembe kell venni a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR). Ha személyes adatot tartalmazó, kriptográfiai védelemmel el nem látott adathordozó eltűnése, jogosulatlanokhoz jutása feltételezhető, akkor azonnal jelentést kell tenni az adatvédelmi tisztviselő felé.

3.8.2. Hozzáférés az adathordozókhoz

A megbízott szervezeti egység vezető 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.

3.8.4. Adathordozók tárolása

Az adathordozókat fizikailag ellenőrizni kell és biztonságosan kell tárolni az arra engedélyezett vagy kijelölt helyen, védeni kell mindaddig, amíg jóváhagyott eszközökkel, technikákkal és eljárásokkal nem semmisítik meg, vagy nem törlik a rajtuk tárolt adatokat.

3.8.5. Adathordozók szállítása

Az adathordozók szállítása során az alábbi biztonsági szabályokat szükséges alkalmazni:

- a. a szállításhoz lehetőleg zárható és a káros környezeti hatásoktól védő tokot, dobozt, táskát kell használni;
- b. szállítás közben az adathordozót folyamatosan a munkatárs személyi felügyelete alatt kell tartani;
- c. szállítás során nem szabad az adathordozót másnak átadni, mások felügyeletére bízni,
- d. óvni kell a nagy melegtől, nagy hidegtől, gyors hőmérséklet változástól, közvetlen napsugárzástól, portól, nedvességtől;
- e. ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg szobahőmérsékletre kerül;
- f. a munkatársak kötelesek az általuk szállított fizikai adathordozókkal kapcsolatos minden eseményt (elvesztés, sérülés, lopás) felettesüknek vagy az elektronikus információs rendszer biztonságáért felelősnek haladéktalanul jelenteni;
- g. gépkocsival történő szállítás esetén az információs rendszerelemeket zárt/fedett csomagtartóban kell elhelyezni oly módon, hogy védve legyen a rázkódásból, sérülésből adódó károktól. Az információs rendszerelemeket és adathordozókat tilos (még rövid időre is) az autóban hagyni, a munkatársnak jármű elhagyásakor magával kell azokat vinnie;
- h. 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 Hivatal 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, vagy a szervezeti egység vezető által kijelölt személyek végezhetik.

3.8.5.2. Kriptográfiai védelem

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

A titkosítás elvégzése a rendszergazda feladata, az elektronikus információs rendszerek biztonságáért felelőssel egyeztetett eljárás alkalmazásával.

3.8.6. 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, a hivatali ellenőrzés megszűnte, vagy újrafelhasználásra való kibocsátás 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) lemezmeghajtók 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/eszközkeszlettel, 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.

A törlésre alkalmazott eszközöket és módszereket hatékonyságát a rendszergazdának a szükséges gyakorisággal tesztelni szükséges (visszaállítás megkísérlésével).

A selejtezésről, a hivatali ellenőrzés megszűntéről, vagy újrafelhasználásra való kibocsátásról előtt minden esetben jegyzőkönyvet kell felvenni, melynek tartalmaznia kell a törlés megtörténtét.

3.8.7. Adathordozók használata

A szervezeti egység vezetője engedélyezheti, korlátozhatja vagy tilthatja bizonyos, vagy bármely adathordozó típusok használatát a kijelölt elektronikus információs rendszereken vagy rendszerelemeken működő biztonsági

intézkedések használatával. A Hivatal szakfeladatait támogató szakrendszerek munkaállomásain az adathordozók használatát az engedélyezett jogosultságoknak megfelelően kell beállítani (csak az azonosított, a felügyeletéért felelőshöz rendelt adathordozó használható engedélyezett, az engedélyezett adathordozó használat dokumentálása szükséges). A szakrendszerek munkaállomásain információbiztonsági megfontolásból a nem engedélyezett adathordozó használatát technikai korlátozásokkal, beállításokkal meg kell akadályozni, melynek a felelőse a rendszergazda.

3.8.7.2. Ismeretlen tulajdonos

A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni.

3.9. AZONOSÍTÁS ÉS HITELESÍTÉS

3.9.1. Azonosítási és hitelesítési eljárásrend

A Hivatalnak gondoskodnia kell arról, hogy a felhasználók mindegyike egyedileg legyen azonosítva és hitelesítve, valamint egyedileg legyenek azonosítva és hitelesítve a felhasználók által végzett tevékenységek. Biztosítani kell ezt azért, hogy a tevékenységek és a hozzájuk tartozó felelősségek 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 Hivatal felhasználóinak kiosztott jogosultságokról a nyilvántartás vezetésére kijelölt személynek nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdákkal közösen felül kell vizsgálni, a nyilvántartást frissíteni kell bármilyen módosítást (pl. személyi változást, jogosultság kiosztását, visszavonását, módosítását) követően.

3.9.2. 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 elektronikus információs rendszer biztonságáért 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, elemei:

- 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.

3.9.4. 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 munkaállomáshoz, rendszerelemhez, elektronikus információs rendszerhez, történő hozzáférést biztosító azonosítókat biztosítók:

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

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat - informatikai rendszertől függően - a felhasználó vagy a rendszergazda hozza létre. Az azonosítók ismételt felhasználása tilos. A rendszer által meghatározott idő, vagy 3 hónap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania, az azonosító ismételt engedélyezést követően aktiválható ismét.

3.9.5. A hitelesítésre szolgáló eszközök kezelése

Az ASP rendszer kétfaktoros azonosítást alkalmaz:

- a. jelszó (tudás) alapú hitelesítést,
- b. birtoklás alapú (tokén) hitelesítés (az e-Személyi igazolvánnyal)

Az Önkormányzati ASP Központ a felhasználói azonosításra egységes SSO (Single Sign-On, egyszeri bejelentkezés) szolgáltatást biztosít, melynek célja, hogy a felhasználónak egyszer kell magát azonosítva belépnie a Keretrendszerbe, majd sikeres bejelentkezés után eléri a hozzárendelt szakrendszereket.

Az elektronikus ügyintézéshez szükséges a Központi Azonosítási Ügynökön keresztüli azonosítás:

- a. Ügyfélkapu: olyan azonosítási szolgáltatás, amely lehetővé teszi, hogy a felhasználó biztonságosan léphessen kapcsolatba az elektronikus közigazgatási ügyintézészt nyújtó szervezetekkel
- b. Elektronikus személyazonosító igazolvány, e-Személyi

Amennyiben a felhasználó nem a fenti módon hitelesíti magát, a Hivatal:

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

sértetlenségét,

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

3.9.5.2. Jelszó (tudás) alapú hitelesítés

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

A Hivatal az alábbi elvárásokat érvényesíti a jelszavak kezelésével kapcsolatosan:

- a. a munkaállomások, rendszerelemek, rendszerek hozzáférésehez szükséges jelszavakat a jelszavak erősségének irányelve alapján kell megadni;
- b. a munkaállomásokhoz, rendszerelemekhez, információs rendszerekhez kiadott kezdő jelszavakat kötelező az első bejelentkezés alkalmával megváltoztatni;
- 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, gépnévre vagy a felhasználói névre utalóak vagy általános, szótári 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 szokatlant tapasztaltak a számítógépes rendszerükben (ezt követően értesíteni kell a rendszergazdát és az elektronikus információs rendszer biztonságáért felelős személyt);
- f. a jelszavakat rendszeres időközönként, legalább 3 havonta cserélni kell (lehetőség szerint automatikusan kikényszerítve), illetve az elektronikus információs rendszer által kikényszerített, vagy az üzemeltetők által meghatározott időközönként;
- g. új jelszónak nem szabad az utolsó 5 régebbi közül egyiket sem megadni;
- h. a jelszavakat alapvetően tilos leírni;
- i. nem tehető a jelszó egy automatikus bejelentkezési folyamat részévé;
- j. tilos a felhasználóknak bejelentkezni a Hivatal rendszereibe olyan felhasználónévvel, melyet eredetileg nem nekik bocsátottak ki, és amelyek használatára nem jogosultak;
- k. a felhasználók a személyes azonosítójukkal és jelszavukkal elkövetett cselekedetekért felelősséggel tartoznak;
- l. 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;
- m. ez a jelszó politika érvényes azokra a külső (nem a Hivatal által üzemeltetett) rendszerekre is, amelyeket a felhasználók a munkájukkal kapcsolatosan elérnek.

Szükséges meghatározni a szakrendszerekben a jogosítások kérdését, és a fluktuáció miatt a felhasználók jogosításának időszakos, Hivatali szintű ellenőrzését és esetleges korrekcióját. A folyamatos ügymenet biztosítása érdekében be kell állítani az egyes szakrendszerekben a helyettesítéseket, amennyiben erre lehetőség van, pl. ASP szakrendszerek esetén, vagy biztosítani kell, hogy az egyes szakrendszerekhez több felhasználónak legyen kiosztva jogosultsága.

Törekednie kell a legkisebb jogosultság kiosztásához a felhasználók körében, a 3.10.6. *Legkisebb jogosultság* elve alapján. Valamennyi felhasználó munkavégzése során a szükséges és elégséges hozzáférés elve alapján

kizárólag a feladat ellátásához szükséges hivatali adat, információ megismerésére, továbbá az adat- és rendszerhozzáférésre a munkavégzéséhez szükséges lehető legrövidebb ideig és szükséges legkisebb jogosultsági szint alkalmazásával jogosult.

A központi szolgáltató kötelező elvárásokat érvényesít a jelszó megadásával kapcsolatban. Az ASP Központ egy esetleges biztonsági incidens során a tenant adminisztrátoroknak privilégiumokkal járó jogosultság-kiosztását számon kérheti.

Azon informatikai rendszerei esetén, ahol jogosultság kizárólag egy felhasználó számára osztható ki, ott ezeket a jelszavakat - informatikai rendszerenként és felhasználónként - nyilván kell tartani, azokat zárt, a felhasználó által a lezárás mentén aláírt, dátummal és névvel ellátott, a jegyző által meghatározott, tűzbiztos, megfelelő mechanikai védelemmel ellátott páncélszekrényben kell tárolni. A folyamatos ügymenet biztosítása érdekében, indokolt esetben, a szervezeti vezető által engedélyezett esetekben, dokumentált módon történő felbontást követően a felhasználónak a megismert jelszavakat azonnal meg kell változtatni. Jelszavakat egyéb helyen tilos leírni.

A hitelesítésre vonatkozó követelményeket valamennyi rendszerelemre vonatkozóan érvényesíteni kell. A menedzselhető hálózati aktív eszköz tekintetében az eszköz gyári, alapértelmezett bejelentkezési azonosítói (név, password) kerüljenek megváltoztatásra. Csak előre kijelölt, privilegizált felhasználóknak legyen lehetősége bejelentkezni a kérdéses eszközökbe.

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

3.9.5.3. 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.

A hitelesítésre szolgáló hardver alapú eszközök kiosztását, visszavonását (az E-személyi kivételével) a rendszergazdának, az elektronikus információs rendszerek biztonságáért felelősnek vagy az erre kijelölt felelősnek nyilván kell tartani.

3.9.5.5. 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.

3.9.6. 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. 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.)

3.9.8. Azonosítás és hitelesítés (hivatalon kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítani 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.

3.9.8. Hitelesítésszolgáltatók tanúsítványának elfogadása

A hálózati kapcsolatok titkosításához csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

3.10. HOZZÁFÉRÉS ELLENŐRZÉSE

3.10.1. Hozzáférés ellenőrzési eljárásrend

A jegyző megfogalmazza, dokumentálja és kihirdeti a hozzáférés ellenőrzési eljárásrendet, mely a hozzáférés ellenőrzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. A jogosultság kezelés során figyelembe veszi a központi szolgáltató (a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató) előírásait. Az elektronikus információbiztonsággal kapcsolatos egyedi engedélyezési hozzáférési szabályokat szükség esetén Informatikai biztonsági eljárásrendben kezeli.

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 vagy a kijelölt felelősnek nyilvántartást kell vezetnie, amelyet legalább évente egyszer az adatgazdákkal közösen felül kell vizsgálni. Frissíteni kell továbbá, bármilyen módosítást követően.

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, a magasabb jogosultsággal rendelkező szervezeti egység vezető vagy a központi szolgáltató által kijelölt adminisztrátor végzi.

Az elektronikus információs rendszerekről, eszközökről, jogosultságokról kizárólag a jegyző, az általa kijelölt személy vagy az elektronikus információs rendszerek biztonságáért felelős szolgáltathat adatokat.

3.10.2. Felhasználói fiókok kezelése

A Hivatallal szerződéses jogviszonyban álló szereplők, a szerződésben meghatározott szerepkörökre kaphatnak jogosultságot. Kizárólag csak a 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. Ha az elektronikus információs rendszerek zavartalan működéséhez szükségesek az emelt szintű jogok, a rendszergazdai jogosultságot a rendszergazda javaslatára a szervezeti egység vezető engedélyezheti a szükséges ideig, kizárólag a szakrendszerek használatához, mely nem használható programok telepítésére, beállítások megváltoztatására.

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.

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.

3.10.3. 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.

3.10.5. 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.

3.10.6. Legkisebb jogosultság elve

A hozzáférés biztosításának alapelvei:

- a. 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;
- b. 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;
- c. a Hivatal által használt rendszerekhez, rendszerelemekhez csak a jogosultságkezelési folyamat betartásával adható hozzáférés;
- d. külső partnerek (vállalkozók, hatóságok stb.) vonatkozásában a Hivatal rendszereihez, rendszerelemeihez való hozzáférés csak szerződés alapján biztosítható;
- e. külső partnerek esetén a hozzáférési jog maximum a szerződés lejáratáig adható;
- f. 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;
- g. a hozzáférési jogosultságokkal történő visszaélés gyanúja esetén a Hivatal minden dolgozója és szerződéses partnere köteles értesíteni az információbiztonsági felelőst,
- h. a felhasználó elszámoltatható minden olyan tevékenységért, amelyet a saját felhasználói azonosítójával végzett, vagy végeztek;
- i. az elektronikus információs rendszerekről és eszközökről kizárólag a jegyző, az általa kijelölt személy vagy az elektronikus információs rendszer biztonságáért felelős szolgáltatott adatokat;
- j. jelen szabályzattól eltérni az elektronikus információs rendszer biztonságáért felelős engedélye esetén lehetséges (ilyen esetekben is szükséges a folyamat megfelelő dokumentálása).

A központi szolgáltató rendszereiben szintén törekedni kell a legkisebb jogosultság kiosztásosára a felhasználók körében. Az adminisztrátornak a jogosultságok kiosztásánál javasolt figyelembe vennie a Szervezeti és Működési Szabályzatot, amely nem kerülhet ellentmondásba sem jelen szabályzattal, sem a központi szolgáltató előírásaival.

Az ASP Központ egy esetleges biztonsági incidens során a tenant 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. A jogosultságok kiosztója is felelőssé tehető a gondatlanságból bekövetkezett biztonsági események kapcsán.

3.10.6.2. Jogosult hozzáférés a biztonsági funkciókhoz

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

3.10.6.3. 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.

3.10.6.4. 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. 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;
- b. a rendszergazda az előjogokat biztosító azonosítóját csak a munkavégzéshez feltétlenül szükséges mértékben használja, minden más esetben a normál felhasználói azonosítójával dolgozzon;
- c. mindenképpen kerülni kell olyan rendszerek üzembeállítását, amelyek nem rendszergazda munkakörben dolgozó felhasználók rendszergazdai jogosultságokkal történő felruházását igényelnék;
- d. 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.

3.10.10. 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 meghatározott időtartalom után automatikusan zárolja a munkaállomást. Az időtartamot kockázatelemzést követően a rendszergazda határozza meg, mely a hatóság által elvártaknak megfelelően alapesetben nem lehet több, mint 3 perc.

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

3.10.10.2. 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.

3.10.11. 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.

3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az azonosítás és hitelesítés nélkül végrehajtható felhasználói tevékenységeket dokumentálni kell, indokolni kell a rendszerbiztonsági tervben, vagy más szabályzatban.

A Hivatalban jelenleg nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek.

3.10.14. 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.

Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, nem engedélyezhető vezeték nélküli hozzáférés.

3.10.15. Mobil eszközök hozzáférés ellenőrzése

A Hivatal belső eljárásrendben felhasználási korlátozásokat, konfigurálásra és kapcsolódásra vonatkozó követelményeket, valamint technikai útmutatót ad ki az általa ellenőrzött mobil eszközökre, engedélyhez köti az elektronikus információs rendszereihez mobil eszközökkel megvalósított kapcsolódást.

A mobil eszközök használatát, Hivatalból történő kiszállítását minden esetben előzetes jegyzői vagy szervezeti egység vezetői engedélyezésnek kell megelőznie.

Az igénylést, kiadást, visszavételt, nyilvántartást, javítást, esetleges elvesztésére vagy a selejtezésére vonatkozó szabályokat eljárásrend tartalmazza.

3.10.15.2. Titkosítás

A Hivatal a mobil eszközök adattároló egységein (laptopok, adathordozók, pl. külső HDD) 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).

A Hivatalból kiszállított mobil eszközök esetén teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást kell alkalmazni (pl. Win10 Pro esetén BitLocker, ESET Endpoint Encryption). Kizárólag hardveres titkosítású pendrive használat engedélyezett.

3.10.16. Külső elektronikus információs rendszerek használata

A jegyző a rendszergazda és az elektronikus információs rendszer biztonságáért felelőssel együttműködve 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.).

Az engedélyezett külső rendszerek használatát dokumentálni szükséges.

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).

3.10.16.2. Korlátozott használat

A Hivatal csak abban az esetben engedélyezi jogosult felhasználóknak egy külső elektronikus információs rendszer felhasználását az elektronikus információs rendszerhez való hozzáférésre, az általa ellenőrzött információk feldolgozására, tárolására vagy továbbítására, ha előzetesen ellenőrzi a szükséges biztonsági intézkedések meglétét a külső rendszeren saját eljárásrendjének megfelelő módon, vagy jóváhagyott, biztonságos kapcsolat van az elektronikus információs rendszerek között, vagy megállapodás született a külső elektronikus információs rendszert befogadó szervezettel.

3.10.16.3. Hordozható adattároló eszközök

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

3.10.17. 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.

3.10.18. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Hivatal a publikus weboldalát.

A jegyző 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.

Az elektronikus információs rendszer biztonságáért felelősfeladata, 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.

3.11. RENDSZER- ÉS INFORMÁCIÓ SÉRTETLENSÉG

3.11.2. 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, rendszerelembe bekövetkezett változások úgy, mint: hibajavítás, frissítés, új hardver üzembe helyezése, vagy a rendszerben bekövetkezett bármi nemű módosítás esetén, az információsértetlenséget biztosítani tudja. A felsorolt változtatásokat a Hivatal saját hatókörében kizárólag a rendszergazda végezheti. A rendszergazdának kell gondoskodnia arról, hogy a rendszer működéséhez szükséges alkalmazások, programok mindig naprakészen működjenek. 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.

3.11.3. 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.

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

A verzióváltással járó alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni (Munkalap vagy egyéb feljegyzés alapján az Alapkonfiguráció nyilvántartásban). Ha nem a módosítást elvégző rendszergazda felelős a nyilvántartás aktualizálásáért, akkor a Munkalapot el kell juttatni az elektronikus információs rendszer biztonságáért felelős felé.

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

3.11.4. 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, figyelembe véve, hogy az ingyenes alkalmazások nem teljesítik a követelményeket;
- 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. a vírusvédelmi rendszert úgy kell beállítani, hogy szükség esetén automatikusan riassza a rendszergazdát vagy a meghatározott további személy(ek)e)t
- g. 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;
- h. a kártékony kódok észlelése és megsemmisítése során jelentkező esetleges téves riasztásokat rendszergazda ellenőrzi;
- i. a rendszer konfigurálása a rendszergazda, a vonatkozó házirendek kialakítása, azok megfelelő működésének ellenőrzése és dokumentálása az elektronikus információs rendszer biztonságáért felelősfeladata;
- j. a szolgáltató által kiadott frissítéseket a rendszergazda a konfigurációkezelési eljárásnak megfelelően hajtja végre;
- k. a Hivatal minden munkatársa köteles az általa használt eszközökön a vírusvédelmet használni, azt semmiféle okból ki nem kapcsolhatja;
- l. kártékony kód észlelése esetén a kártékony kódokat azonnal karanténba kell helyezni, és jelezni kell a rendszergazdának;
- m. a rendszergazdának jelentenie kell az elektronikus információs rendszer biztonságáért felelős felé a kártékony kódok jelenlétét a rendszerben;
- n. a kártékony kódok megsemmisítése során, figyelembe kell venni annak, a rendszer rendelkezésre állására való kihatását;
- o. 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 kékretlen őrzenetek támadásaival szemben. Az internethasználatra vonatkozó szabályokat az 1.6.9. *Viselkedési szabályok az interneten* fejezet tartalmazza.

3.11.4.3. Automatikus frissítés

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

3.11.5. Az elektronikus információs rendszer felügyelete

Felelősségi körén belül a rendszergazda vagy a szolgáltató felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat.

A rendszergazda vagy a megbízott felelős, szolgáltató a rendszer megfelelő működése érdekében figyelemmel kíséri az elektronikus információs rendszer, rendszerelemeinek rendelkezésre állását. Meghibásodás/rendszer hibaüzenet esetén meg kell oldania a problémát. Ellenőrzi, és valós esetben javítja a felhasználóktól 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.

Erősíteni kell a rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jel tapasztalható. Meghibásodás/nem megfelelő üzemelés, esetleges támadás esetén közvetlenül az észlelést követően a rendszer felügyeletéből gyűjtött információkat az elektronikus információs rendszer biztonságáért felelős felé kell kommunikálni.

3.11.6. Biztonsági riasztások és tájékoztatások

Az elektronikus információs rendszer biztonságáért felelős folyamatosan figyeli a kormányzati eseménykezelő központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, folyamatosan figyelemmel kíséri a Nemzeti Kibervédelmi Intézet Kormányzati Eseménykezelő Központtól érkező értesítéseket, szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki, illetve a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez.

Kialakítja és működteti a jogszabályban meghatározott esemény bejelentési kötelezettség rendszerét, és kapcsolatot tart az érintett, külön jogszabályban meghatározott szervekkel, megfelelő ellenintézkedéseket és válaszlépéseket tesz. 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 1.5.8. *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. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

Az elektronikus információs rendszer biztonságáért felelős a biztonsági riasztásokat és a kapcsolatos intézkedéseket elektronikus nyilvántartásban vagy egyéb dokumentumban rögzíti.

3.11.10. Bemeneti információ ellenőrzés

Az elektronikus információs rendszer ellenőrzi az információ belépési pontok érvényességét.

3.11.12. 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.

A kimeneti információk (pl.: nyomtatott dokumentumok) kezelésével és szétosztásával kapcsolatban a következők az előírások:

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

A kimeneti információk kezelése során figyelembe kell venni az információ minősítését. A mindenkori biztonsági osztályok függvényében kerülnek meghatározásra a szabályozások arra vonatkozóan, hogy miként kell eljárni a bizonyos adatokkal, dokumentumokkal.

További elvárásokat a 2.16. *A kimeneti eszközök hozzáférés ellenőrzése* és a Hivatal további szabályzatai tartalmazznak.

3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

3.12.1. 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.

3.12.2. Naplózható események

A rendszergazda - az elektronikus információs rendszer biztonságáért felelőssel egyeztetve - meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét. A naplózható események meghatározásakor a rendszergazda lehetőség szerint vegye figyelembe az érintett munkatársak információigényeit is.

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

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.

3.12.3. 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).

3.12.8. 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.

3.12.9. 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.

3.12.11. 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. Amennyiben nem áll rendelkezésre megfelelő méretű tárhely az eseménynaplók 1 évre visszamenő megőrzéséhez, úgy az eseménynaplót a biztonságos működést nem veszélyeztető maximumban kell beállítani.

3.12.12. Naplógenerálás

Az elektronikus információs rendszernek biztosítani kell a naplóbejegyzések előállítási lehetőségeit a 3.12.2 *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 3.12.2 *Naplózható* fejezetben meghatározottak szerinti eseményekre, a 3.12.3 *Naplóbejegyzések tartalma* pontban meghatározott tartalommal.

3.13. RENDSZER- ÉS KOMMUNIKÁCIÓ VÉDELEM

3.13.1. 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 értekeztet(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 elektronikus információs rendszer biztonságáért 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 elektronikus információs rendszer biztonságáért 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 védelme;
- 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).

3.13.6. 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 és adatok védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni.

Gondoskodni kell a hálózat fizikai elemeinek védelméről, így különösen:

- a. vezetékek és végpontok illetéktelenek általi hozzáféréseinek megakadályozásáról,
- b. szükséges nem használt portok tiltásáról/porthasználat szűkítéséről adott ip/ip tartományra, figyelembe véve a 3.3.6.7. *Legszűkebb funkcionalitás követelményeit*
- c. a vezeték nélküli kapcsolatok megfelelő titkosításáról (WPA2/PSK vezeték nélküli titkosítás szükséges)
- d. 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 al-hálózatokban kell elhelyezni, elkülönítve a belső Hivatali hálózattól. A hatósági elvárásoknak megfelelően szükséges a szakrendszereket használó számítógépek, a nyílt internetet használó számítógépek és a nyilvános (vendég-) hálózatot használó számítógépek fizikai (Switch-el történő elszeparálással) vagy logikai elkülönítése (VLAN) külön, átjárhatatlan alhálózatokban.

Az elektronikus információs rendszer csak a Hivatal biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészekon keresztül kapcsolódhat külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

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

- a. megfelelő interfészt kell alkalmazni a Hivatal és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;
- b. a felhasználókat jelszóval megfelelően hitelesíteni kell;
- c. ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

Az informatikai határvédelemmel, tűzfallal kapcsolatos elvárások:

- a. a szervezet internethez való csatlakoztatása a központi tűzfalon keresztül történjen meg
- b. a tűzfal szabályokat szükség esetén egyeztetni kell a központi szolgáltatóval (NISZ Zrt.)
- c. a tűzfal szabályok dokumentálása és azok zárható helyen történő tárolása legyen biztosítva

A rendszergazda feladata:

- a. határvédelmi rendszerek szoftvereinek naprakészen tartása, határvédelmi eszközök feketelistájának frissítése
- d. hálózati nyomtató megosztásának jelszavas védelme, vagy a szkennelt mappa ütemezett törlése
- e. tűzfal logok elemzése

3.13.10. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai eszközök bevezetése esetén ki kell dolgozni az eszközök biztonságos használatát garantáló szabályozást, melynek a következőket kell tartalmaznia:

- a. az eszközök védelmét biztosító előírások;
- b. az eszközök felhasználására vonatkozó követelmények;
- c. a kulcsok generálására, elosztására, tárolására és megsemmisítésére vonatkozó szabályok;

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).

3.13.12. Együttműködésen alapuló számítástechnikai eszközök

Az elektronikus információs rendszernek meg kell gátolnia az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását, kivéve, ha a Hivatal engedélyezte azt, és közvetlen kijelzést nyújt a távoli aktivitásról azoknak a felhasználóknak, akik fizikailag jelen vannak az eszköznél.

A Hivatal nem alkalmaz a központi szolgáltatású elektronikus információs rendszerben távolról elérhető eszközöket, következésképpen nincs lehetőség távoli aktiválásra. A rendszergazda feladata Házirendben a hozzáférések szabályozása, vagy driver-ek eltávolítása, hardvertiltás beállítása.

3.13.22. A folyamatok elkülönítése

Az elektronikus információs rendszernek elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamatra.

Az elektronikus információs rendszernek elkülönített végrehajtási tartományt kell fenntartani minden végrehajtó folyamatra (hálózati támadástól való védelem érdekében a szakrendszerei munkaállomások különálló védett hálózatba elhelyezése (vlan) lásd 3.13.6. *A határok védelme* fejezet.

Kapcsolódó mellékletek

Melléklet száma	Melléklet megnevezése
1. sz. melléklet	Biztonsági osztályba és szintbe sorolás
2. sz. melléklet	Titoktartási és megismerési nyilatkozat minta

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;

adatifeldolgozás: 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;

adatifeldolgozó: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki/amely az adatkezelő részére adatifeldolgozást 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 adatifeldolgozóval 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 kinyomtatott formában.);

archiválási rendszer: az archiváláshoz felhasznált, hardver- és szoftver-elemekből álló technikai rendszer;

auditálás: előírások teljesítésére vonatkozó megfelelőségi 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;

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 lbtv. 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 lbtv. 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 lbtv. 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 lbtv. 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 elektronikus információs rendszer biztonságáért felelős személy 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;

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 csökkenti 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 kibertérrel 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;

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 elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az, az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

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 licenzszerződés: 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 előírányzottak 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;

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem; *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.

SÁROSPATAK VÁROS ÖNKORMÁNYZAT KÉPVISELŐ-TESTÜLETÉNEK

.../2018. (. .)

h a t á r o z a t a

az Informatikai Biztonsági Szabályzat jóváhagyásáról

Sárospatak Város Önkormányzat Képviselő-testülete tárgybani javaslatot megtárgyalta és úgy döntött, hogy az Információ Biztonsági Szabályzatot a javaslat szerinti tartalommal jóváhagyja.

Felelős: jegyző

Határidő: azonnal