Dalmandi Közös Önkormányzati Hivatal jegyzője

1 / 2018.

JEGYZŐI UTASÍTÁS

Iktatószám: D. 334-3/2018.

Dalmandi Közös Önkormányzati Hivatal

7211 Dalmand, Hősök tere 5.

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

érvényes:

2018. június 1.

jóváhagyta:

.....

dr. Foki Csilla jegyző

DALMANDI KÖZÖS ÖNKORMÁNYZATI HIVATAL JEGYZŐJE

Dokumentum története

Verzió	Készült	Változás oka
1.1	2018.05.25	ASP működési rend szabályozása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013 évi L. törvényben (Ibtv.) kapott felhatalmazás alapján, 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 rendeletnek megfelelően az alábbi szabályzatot adom ki:

Informatikai biztonsági szabályzat

Hatálya:

Az Informatikai biztonsági szabályzat ***tárgyi hatálya*** kiterjed a Hivatal tulajdonában, kezelésében lévő valamennyi elektronikus információs rendszerre és azok elemeire, az általa használt alkalmazásokra, adatbázisokra, hálózatokra, hálózati elemekre, kiegészítő informatikai eszközökre, valamint az általa keletkeztetett, feldolgozott, tárolt, továbbított valamennyi adatra és információra, függetlenül azok megjelenési formájától. Idegen vagy vegyes tulajdonú, illetve kezelésű eszközök, rendszerek használata során figyelembe kell venni a külső fél azokra vonatkozó rendelkezéseit és előírásait, illetve az érvényes megállapodásokat.

A szabályzat ***személyi hatálya*** kiterjed a Hivatal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek a Hivatal elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), akik részt vesznek a Hivatalnál keletkező, tárolt, illetve továbbított adatok kezelésében, így:

- a választott tisztségviselőkre (polgármester, alpolgármester, képviselők),
- a közszolgálati jogviszony vagy munkaviszony alapján foglalkoztatott munkatársakra, köztisztviselőkre, ügyintézőkre,
- a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyekre,
- más szervezetek képviseletében a Hivatal munkahelyein tartózkodó személyekre.

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: Dalmandi Közös Önkormányzati Hivatalra, valamint a Szervezeti és Működési Szabályzat szerinti, a 2013. évi L. törvény hatálya alá tartozó szervezeti egységeire, települési és nemzetiségi önkormányzat(ok)ra.

A szabályzat **tárgyi hatálya** kiterjed a kezelt, keletkezett információkra, az informatikai rendszerekben üzemeltetett valamennyi hardver és szoftver elemre, amely felhasználja, feldolgozza, felügyeli, ellenőrzi, tárolja, továbbítja a Hivatalnál keletkező, illetve felhasznált adatokat. Kiterjed továbbá a rendszerelemek dokumentációira

Időbeni hatály: jelen Informatikai biztonsági szabályzat a kiadás napján lép hatályba, mellyel a korábbi Informatikai biztonsági szabályzat és eljárások hatályukat vesztik.

Dalmandi Közös Önkormányzati Hivatal jegyzője

...../2018.

JEGYZŐI UTASÍTÁSA

Dalmandi Közös Önkormányzati Hivatal

7211 Dalmand, Hősök tere 5.

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

érvényes:

.....

jóváhagyta:

.....

Dr. Foki Csilla jegyző

Dokumentum története

Verzió	Készült	Változás oka
1.1	2018.05.25	ASP működési rend szabályozása

Tartalom

Az Informatikai biztonsági szabályzat

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013 évi L. törvényben (a továbbiakban Ibtv.) kapott felhatalmazás alapján A Dalmandi Közös Önkormányzati 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. (VIII. 31.) Korm. rendelettel,
- Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvénnyel.

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 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 megoszlanak a Hivatal és a szolgáltató/üzemeltető között.

A Hivatallal szemben elvárt követelményekkel kapcsolatban figyelembe kell venni a Magyar Állam Kincstár tájékoztatóit (pl. Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről). A Tájékoztató tartalmazza azokat a követelményeket, amelyeket kötelező jelleggel kell megvalósítania 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 információ-biztonsági 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) munkaállomásokra, 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 Dalmandi Közös Önkormányzati Hivatalra, valamint a Szervezeti és Működési Szabályzat szerinti, a 2013. évi L. törvény hatálya alá tartozó szervezeti egységeire, települési és nemzetiségi önkormányzatokra.

Időbeni hatály: jelen Informatikai biztonsági szabályzat a kiadás napján lép hatályba, mellyel a korábbi Informatikai biztonsági szabályzat hatályát veszti.

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 illetéktelenekne nem adhatják tovább.

Szerepkörök, tevékenységek, felelősségek

A Dalmandi Közös Önkormányzati Hivatal szervezeti szintű felépítését a Szervezeti és Működési Szabályzatban (SzMSz) rögzíti. Az elektronikus információs rendszer biztonsága érdekében történő, a Hivatalon belüli együttműködés jelen szabályzat tételes előírásain túl az érintett személyek önkéntes, szabálykövető magatartásán és biztonságtudatos, proaktív viselkedésén is alapul.

Az egyes kontrollfolyamatokban kötelező együttműködési szabályokat az eljárásrendek vonatkozó előírásai részletezik.

Általában minden érintett személy köteles:

- jelen szabályzat és kapcsolódó dokumentumok előírásait megismerni és magára nézve, nyilatkozat keretében kötelezőnek elismerni,
- az információbiztonsági tárgyú belső képzéseken részt venni,
- személyét érintő biztonsági ellenőrzéseket, auditokat tűrni, azokban az ellenőrző személyek kérése szerint részt venni,
- az általa biztonsági eseményként vélelmezett történéseket a felettes vezetőnek és/vagy 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 Hivatal vezetője, 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, 6. rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak, 7. gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről, 8. biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről, 9. ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 10. ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, 11. felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért, 12. megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket, 13. a feladatokért a szervezet vezetője a 9. és I0. 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, 15. együttműködik a hatósággal a hatóság feladatainak elvégzésében, ennek során az Ibtv. 12. § alapján: a) az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt, b) a szervezet Informatikai biztonsági szabályzatát tájékoztatás céljából megküldi, c) az ellenőrzés lefolytatásához szükséges feltételeket biztosítja a hatóság részére.

az elektronikus információs rendszerek biztonságáért felelős személy *(vállalkozási 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. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot. 13. nyilvántartja az elektronikus információs rendszereket 14. nyilvántartást vezet a biztonsági incidensekről 15. nyilvántartást vezet az információbiztonsági és biztonsági eseménykezelési oktatásokról
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.

Megbízott szervezeti egység vezető *(osztály/irodavezetők, hiányukban a Hivatal vezetője)*	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, 4. saját és a felelőssége alá tartozó munkatársak információbiztonsági, informatikai fennakadásról tett észrevételeit jelenti a rendszergazdának
Adatgazda *(szervezeti egység vezető)*	1. meghatározza a hatókörébe tartozó elektronikus információs rendszerekhez, adatokhoz, tevékenységekhez hozzáférők körét, 2. engedélyezi a szükséges jogosultságokat a hatáskörébe tartozó elektronikus információs rendszerek, adatok, tevékenységek tekintetében (nyilatkoztatást követően), 3. 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 *(vállalkozási szerződés alapján külső szakértő)*	1. felelős az elektronikus információs rendszerek felügyeletéért, az alkalmazások, a kiszolgálók és az alapszoftverek, az informatikai hálózat és a munkaállomások 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 (karbantartásinapló), 11. az az elektronikus információs rendszer biztonságáért felelőssel közreműködve, meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket, 12. elvégzi az időszakos mentéseket, szükség szerinti helyreállításokat, visszaállítási teszteket és jegyzőkönyvezi azokat, 13. hiba esetén elvégzi vagy felügyeli az eszközök javítását (a szerződésnek/a jegyző utasításának megfelelően vagy vele egyeztetve),

	14. közreműködik az 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 hatókörében előír, pl.: j) belépésre jogosultak listája (irodákba, hivatali helyiségekbe) k) nyilvántartja a fizikai belépést ellenőrző eszközöket
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. felelőséggel 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 jogszabályba, az informatikai biztonsággal kapcsolatos kiadott utasításba, szabályzatba ütközik, vagy megítélése szerint veszélyeztetné az informatikai biztonságot, 14. köteles az utasítást adó figyelmét felhívni és egyben kérheti az utasítás írásba foglalását, ha az, vagy annak végrehajtása jogszabályba vagy a kiadott informatikai biztonsággal kapcsolatos utasításba ütközne, vagy teljesítése kárt idézhet elő, és a felhasználó a következményekkel számolhat, vagy az utasítás az érintettek jogos érdekeit sérti. Az utasítást adó felettes az utasítás írásba foglalását nem tagadhatja meg.

	15. Az utasítástól való eltérést felettesének azonnal jelezni kell.
Weblap fejlesztő, üzemeltető, tartalom felelős	**Weblap fejlesztő**: 1. a mindenkori 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 közlése (a település bemutatása, aktuális hírek, információk közlése az állampolgárok számára), **A tartalom ellenőrzéséért felelős** (Hivatal által kijelölt vezető vagy munkatárs): 1. a tartalom feltöltése előtt átvizsgálja és rendszeres időközonként ellenőrzi a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolíttatja azokat.
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 szakrendszeri szerepkör(ök)höz rendelése, annak adminisztrációja és karbantartása, b) intézményi kapcsolattartóként az adott tenant felhasználók tanúsítvány igénylésének adminisztrációja és karbantartása, illetve a tanúsítványokat hordozó tokenek csoportos átvétele és felhasználók közötti kiosztása, 2. az önkormányzat szakrendszeri adminisztrátor(ok) feladata a szakrendszer szintű jogosultságkezelés, azaz a szolgáltatást igénybe vevő felhasználók számára a szakrendszeri jogosultságok beállítása, adminisztrációja és karbantartása.

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 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 megfelelőségéért, 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 intézkedés*, 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 megfelelőség 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 Hivatal vezetője megfogalmazza, dokumentálja és 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 Hivatal vezetőjének feladata biztosítani, hogy az Informatikai biztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

1.1.2. Az elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője 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 (Ibtv. 13. §).

A Hivatal vezetője 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 Közszolgálati Egyetem továbbképzésén, éves továbbképzésein 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 szervezetnél 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) részmunkaidőben,
b) a vonatkozó szerződésben meghatározott időtartamban, vagy
c) több érintett szervezetnél.

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

1.1.3. Az intézkedési terv és mérföldkövei

A Hivatal vezetője az informatikai biztonsági követelmények megvalósításához az Ibtv.-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 Hivatal vezetője a vizsgálatot követő 90 napon belül felülvizsgálatot készít, a hiányosság megszüntetése érdekében.

A kitűzött feladatok megvalósulását a Cselekvési tervben a Hivatal vezetője 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, jogosultság adás
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 jog-viszony 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 Hivatal vezetője 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 alapfeladatokat 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 Ibtv. 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 bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt (a 41/2015 [VII.15.] BM rendelet iránymutatása alapján). Az elektronikus információs rendszer biztonsági osztálya alapján kell megvalósítani az előírt védelmi intézkedéseket 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 Hivatal vezetője 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 Hivatal vezetője hagyja jóvá, és felel annak a jogszabályoknak és kockázatoknak való megfelelőségéért, 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 kockázatértékelés 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 Hivatal vezetője - 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 kockázatokat (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 rendszerelemek 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 válaszintézkedéseket 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.

a. 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).

b. Korrekciós kontrollok: A realizálódott, nem kívánt kockázat következményeit korrigálják, úgy, hogy kisegítő 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.

c. 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).

d. 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 vizsgálandó, 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 megszűntetése nem akadályozza az Hivatallal szembeni követelmények teljesítését, csak megszüntethetők az adott tevékenység befejezésével.

Felelősségek

A Hivatal vezetője *(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 kísérési feladatokról
- gondoskodik a kockázatkezelés fontosságának tudatosításáról a teljes szervezetben

A kockázatfelmérésért felelős *(elektronikus információs rendszerek biztonságáért felelős vagy a jegyző által kijelölt személy)*

- felelős a kockázat-felmérési módszertan(ok) kialakításáért, jóváhagyatásáért
- 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 Hivatal vezetőjét 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 a rendszergazdának vagy a nyilvántartásra kijelölt felelősnek haladéktalanul nyilvántartásba kell venni.

Az irodai munkavégzéshez szükséges irodatechnikai eszközök, alkalmazások megfelelő minőségben és mennyiségben történő készletezése (készletezés tervezése) a megbízott szervezeti egység vezető vagy rendszergazda feladata. Ezekből a kellékekből mindig akkora készlettel kell rendelkezni, mely biztosítja a folyamatos üzemvitelt. Azokban az esetekben, amikor a Hivatal olyan elektronikus információs rendszert vesz igénybe, amelynek használatához jogszabályi előírásban kerül meghatározásra a szükséges eszközök beszerzése, 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 határoznia 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, javaslattételi 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 vagy a nyilvántartásra kijelölt felelős nyilvántartja.

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

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

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, megszemélyesítése,
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 visszaállításán túl az, hogy ezt kockázatokkal arányosan lehessen megvalósítani.

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

A folyamat, valamint az ügymenet-folytonosság tervezés és a katasztrófa-visszaállítási terv gazdája az 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 biztosítania 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 újrakezdésének időpontja, az ügymenet-folytonossági terv életbelépését követően, tervezett szolgáltatási szint),
e. a folytonosság biztosításába bevont szerepkörök meghatározása és megszemélyesítése,
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 történjen 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 újrakezdését, 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, vagy a Hivatallal kötött megállapodásban rögzítettek szerint az adott elektronikus információs rendszer üzemeltetője (az ASP esetében a szolgáltató) végzi saját adatmentési és naplózási eljárása körében.

A 466/2017. (XII. 28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról 8. pont 15. § (1) bekezdése alapján, a Hivatal az adattrezor-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 felülbírálhatja, 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 vissza ellenőrzött 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 üzemidő-kiesés, 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 *1.4.1. 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. hálózatbiztonsági incidensek.

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

Az információbiztonsági incidensről, valamint annak életútjáról jegyzőkönyvet kell készíteni, amelyet az elektronikus információs rendszer biztonságáért felelős készít el és jelenti azt a Hivatal vezetője 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 szerveknek (GovCERT-Hungary), amelyek hálózatbiztonsági incidensekből adódnak.

Biztonsági incidensek esetén a Hivatal IBSZ-e szerint kell eljárni, azonban az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a Kormányzati Eseménykezelő Központ mellett (utóbbi esetén az észlelés nem feltétlenül jelentkezik a Hivatalnál, de kizárni sem lehet). A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg. Ennek bejelentési felülete a hibabejelentő rendszer. Az ASP Központ a bejelentéseket fogadja, továbbítja az illetékes terület felé és a jogszabály szerinti lépéseket megteszi.

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

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 hálózatbiztonsági incidenseket (pl. DDOS támadás), amelyeket be kell jelenteni az elektronikus információs rendszerek biztonságának felügyeletét ellátó szerveknek (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 károlhárításhoz, 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 (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 kik kaphatnak 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 igényló 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 munkakor 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, koncentrálóképesség 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 munkatársnak a munkaköri leírásokban, szerződésekben rögzítenie kell.

A humánerőforrás fentebb leírt pontjai nem lehetnek ellentmondásban jelen szabályzattal. 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 Hivatal munkáltatói jogait gyakorló vezető dönt. A jogosultságok megszüntetése során figyelembe kell venni, a felmondás jellegét (felmondás, közös megegyezés, azonnali hatályú felmondás), illetve a szerződésben rögzített felmondási és egyéb határidőket és a jogosultságok visszavonásának ütemezését ehhez kell igazítani.

A jogviszony megszűnésekor az alkalmazottnak, a szerződőknek, harmadik félnek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. A jogosultságok visszavonása 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 vagy a kijelölt felelős megszünteti, vagy visszaveszi a Hivatal által az érintett személynek kibocsátott egyéni hitelesítő eszközeit, beleértve a hitelesítésre szolgáló eszközöket, felhasználói kártyákat (pl. anyakönyvi kártya), a Hivatal területére való belépésre jogosító kártyákat (pl. proximity kártya).

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

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

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

A távozó munkatárs levelezési fiókját, elektronikus információs rendszerhez való hozzáférést az 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 Hivatal vezetője 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. Megelőzi az elektronikus információs rendszert, illetve abban tárolt adatokat érintő, információbiztonsági szabályokat sértő magatartását.

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

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

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 szűntetni az áthelyezés miatt megváltozott hozzáférési engedélyeket.

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

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

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

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

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

A partnernek a Hivatalt haladéktalanul tájékoztatnia kell arról, ha változik a saját 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.

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

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

Az 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.

A külső féllel történő megállapodás megkötését megelőzően a jegyző – az elektronikus információs rendszer biztonságáért felelős személy bevonásával – 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 Hivatal előírja és folyamatosan ellenőrzi a szerződő fél személybiztonsági követelményeknek való megfelelését. Elvárja, hogy a külső fél munkavégzése során:

a. gondoskodjon arról, hogy az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása és az adatvédelem elvei nem sérülhetnek,
b. gondoskodjon arról, hogy a hozzáférési jogot kapott munkatársai a jogosultságot nem adhatják át más személynek,
c. gondoskodjon arról, hogy a hozzáférési azonosítókat és az ezekhez kapcsolódó fizikai eszközöket bizalmasan kezelje, és biztosítsa, hogy azokhoz illetéktelen személyek ne férhessenek hozzá,
d. gondoskodjon arról, hogy ha olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik a Hivatal elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést a Hivatalnak;
e. garantálja az elektronikus információs rendszerek és infokommunikációs eszközök megfelelő védelmét, a szükséges és elégséges hozzáférés elvének betartását, fizikai és logikai védelem kialakítását, rendszerszintű titkosítási eljárások alkalmazását, illetve a biztonsági naplózást,

f. ha távolról éri el a Hivatal hálózatát, illetve valamely elektronikus információs rendszerét, akkor a biztonságos elektronikus adatcsere-kapcsolat érdekében köteles a Hivatal által előírt információbiztonsági megoldásokat megvalósítani mindazon saját eszközein, amelyekről a távoli elérés lehetséges.
g. Bizalmas adatforgalom a Hivatal és a külső fél között csak titkosított kommunikációs csatorna biztosításával történhet.
h. Az elektronikus információs rendszerhez kapcsolódó rendszergazdai feladatok ellátásáért az üzemeltetést végző külső fél felel.
i. A külső fél által megállapodás alapján nyújtott szolgáltatásainak megfelelőségét a Hivatal vezetője és a rendszergazda – szükség esetén az elektronikus információs rendszer biztonságáért felelőssel együttműködve – folyamatosan ellenőrzi.

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.

A Hivatal vezetője belső eljárási rend szerint fegyelmi eljárást kezdeményez az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben. Amennyiben az elektronikus információbiztonsági szabályokat nem a Hivatal személyi állományába tartozó személy sérti meg, érvényesíti a vonatkozó szerződésben meghatározott következményeket, megvizsgálja és szükség szerint alkalmazza az egyéb jogi lépéseket.

1.6.8. Belső egyeztetés

A Hivatal 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 internethasználattal 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 haszonszerzésre irányuló tevékenység (pl. piramisjáték), szerzői jogok megsértése (pl. szoftver nem jogszerű terjesztése);
b. egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám;
c. a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
d. a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat 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. fájlcserélő 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 elérhetőek, vagy a szakfeladatokhoz szükséges adatok, dokumentumok tárolására kerül sor, csak a munkavégzéshez közvetlenül szükséges weboldalak használata engedélyezett;
b. technikai intézkedésekkel tiltani kell a szakfeladatokhoz nem szükséges weboldalak elérését. A munkavégzéshez engedélyezett weboldalakat a felhasználókkal való egyeztetést követően 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 (vezetéknev.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 igyekezzen azt beazonosítani, gyanús esetben törölje az üzenetet, illetve jelezze ezt felettesének vagy a rendszergazdának. Amennyiben a megnyitás szükséges annak megállapítására, hogy mi az üzenet célja, úgy ezt megfelelő előrelátással (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 alkalmazottaknak tilos más alkalmazottak postafiókjához felhatalmazás nélkül hozzáférniük;
g. a kilépett alkalmazott, megszűnt szerződésű partner levelezési hozzáférését azonnal meg kell szüntetni, az érintett levelezési fiókját a rendszergazda a kilépést követően legalább 30 napig figyeli (vagy ameddig 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 (*lsd. 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. a 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 megjelenni, hírlevelekre feliratkozni;
m. tilos a Hivatal nevében olyan e-mailt küldeni, melyek:
   - bizalmas, kritikus információt tartalmaznak vagy szerződési, illetve jogi következménnyel lehetnek a Hivatalra nézve,
   - a Hivatal hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatja, illetve a Hivatal ügyfeleinek érdekét sértheti,
   - a Hivatal bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki és a felhasználó erre nem lett felhatalmazva, vagy munkakörének nem része az adott területre vonatkozó vélemény nyilvánítása,
   - szerzői jogokat sérthetnek,
   - vírusokkal fertőzhetik meg a Hivatal infrastruktúráját,
   - vallási, etnikai, politikai vagy egyéb másokra nézve potenciálisan sértő, zaklató tevékenység.
n. a felhasználó által küldött elektronikus leveleket a felhasználónak kell aláírnia. Nem használható önállóan csupán a Hivatal neve, vagy annak variációi önálló aláírásként – a felhasználóknak a saját nevüket, és opcionálisan beosztásukat kell használni aláírásként;
o. Amennyiben a felhasználó hivatali hatáskörben a Képviselő-testület vagy szerve nevében és meghatalmazásából jár el, annak a levél aláírásából egyértelműen ki kell tűnnie;
p. a munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából, archiválni szükséges;
q. a csatolt állományok készítéséhez és a partnerekhez való küldéshez a dokumentumokat előzetesen PDF formátumra kell átalakítani, amennyiben nem szükséges azt szerkeszthető formátumban továbbítani.

Az Ibtv. 3. § (2) -(3) bekezdése alapján a külföldi adatkezelést, az egyes elektronikus információs rendszerek Magyarország területén kívül üzemeltetetését 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 értesti az érintetteket, megteszi a szükséges teendőket.

1.7.2. Képzési eljárásrend

A Hivatal vezetőjének 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 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 kísérési 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 biztonság tudatosság képzések elvégzése a kijelölt személy (biztonságért felelős, rendszergazda vagy egyéb szakértő feladata, a képzés elvégezhető e-learning képzési formában).

A képzési felelős (képzési referens vagy a jegyző) kezdeményezi a képzéseket, követi a képzési intézkedések megvalósulását, megőrzi a képzési feljegyzéseket.

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 jogosultságaitat 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.