Iktatószám: JZI/492-4/2025

Hatályos: 2025.11.2626.

Szerencsi Közös Önkormányzati Hivatal

3900 Szerencs, Rákóczi út 89.

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

jóváhagyta:

.....

Dr. Béni Gyula

jegyző

Dokumentum története

Verzió	Készült	Változás oka
2.0	2025.11.03.	Új kiadás Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény alapján

Bizalmas, belső használatú dokumentum
A szabályzat szerzői jogvédelem alatt áll, bármely részének felhasználása a jogtulajdonos IP Monitoring Kft. írásbeli engedélyével lehetséges.
A szerzői jog nem korlátozza a Hivatalt a szabályzat módosításában, publikálásában a szerzői jogra való hivatkozás megtartása mellett.

Az Információbiztonsági szabályzat ... 6
Célok 6
Felülvizsgálat ... 6
Hatály 7
Hatásköri és illetékességi szabályok ... 8
Szerepkörök, tevékenységek, felelősségek ... 8
Adatosztályozás ... 14
VÉDELMI INTÉZKEDÉSEK ... 15
1. PROGRAMMENEDZSMENT ... 15
1.1. Információbiztonsági szabályzat ... 15
1.2. Elektronikus információs rendszerek biztonságáért felelős személy ... 15
1.3. Információbiztonságot érintő erőforrások ... 16
1.4. Intézkedési terv és mérföldkövei ... 16
1.5. Elektronikus információs rendszerek nyilvántartása ... 17
1.6. Biztonsági teljesítmény mérése ... 18
1.7. Szervezeti architektúra ... 19
1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve ... 19
1.10. Kockázatmenedzsment stratégia ... 19
1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend ... 20
1.11. Engedélyezési folyamatok meghatározása ... 22
1.12. Szervezeti működés és üzleti folyamatok meghatározása ... 22
1.14. Biztonsági személyzet képzése ... 22
1.15. Tesztelés, képzés és felügyelet ... 23
1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás ... 23
1.17. Fenyegetettség tudatosító program ... 23
1.19. Kockázatmenedzsment keretrendszer ... 23
1.20. Kockázatkezelésért felelős szerepkörök ... 23
1.21. Ellátási lánc kockázatmenedzsment stratégiája ... 23
1.22. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói 24
1.23. Folyamatos felügyeleti stratégia ... 24
2. HOZZÁFÉRÉS-FELÜGYELET ... 25
2.1. Hozzáférés-felügyeleti eljárásrend ... 25
2.1.1. Felhasználói fiókok létrehozása, felülvizsgálata, megszüntetése ... 25
2.1.2. Új hozzáférés igénylése ... 26
2.1.3. Hozzáférési jogosultságok módosítása ... 27
2.1.4. Hozzáférés jogosultságok visszavonása ... 28
2.1.5. Felhasználó letiltása/engedélyezése ... 28
2.1.6. Jogviszony megszűnésekor szükséges általános követelmények ... 28
2.1.7. Tartós távollét esetén szükséges intézkedések ... 29
2.1.8. A szerepkörök és jogosultságok ellenőrzése ... 29
2.1.9. A jelszókezelés követelményei ... 30
2.1.10. Fiókokkal és jogosultságokkal kapcsolatos incidensek kezelése ... 30
2.2. Fiókkezelés ... 30
2.15. Hozzáférési szabályok érvényesítése ... 33
2.71. Sikertelen bejelentkezési kísérletek ... 33
2.75. A rendszerhasználat jelzése ... 33
2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek ... 33
2.100. Távoli hozzáférés ... 34
2.108. Vezeték nélküli hozzáférés ... 35
2.108.1. Alkalmazottak vezeték nélküli hozzáférése ... 36
2.108.2. Vendégek vezeték nélküli hozzáférése ... 36
2.113. Mobil eszközök hozzáférés-ellenőrzése ... 36
2.115. Külső elektronikus információs rendszerek használata ... 37
2.124. Nyilvánosan elérhető tartalom ... 37
3. TUDATOSSÁG ÉS KÉPZÉS ... 39
3.1. Képzési eljárásrend ... 39
3.2. Biztonságtudatossági képzés ... 39
3.4. Biztonságtudatossági képzés – Belső fenyegetés ... 40
3.9. Szerepkör alapú biztonsági képzés ... 40
3.13. A biztonsági képzésre vonatkozó dokumentációk ... 41
4. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG ... 42
4.1. Naplózási eljárásrend ... 42
4.2. Naplózható események ... 42
4.3. Naplóbejegyzések tartalma ... 42
4.5. Naplózás tárkapacitása ... 43
4.7. Naplózási hiba kezelése ... 43

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel ... 43
4.24. Időbélyegek ... 43
4.25. Naplóinformációk védelme ... 44
4.38. A naplóbejegyzések megőrzése ... 44
4.40. Naplóbejegyzések létrehozása ... 44
5. ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS ... 45
5.1. Biztonságértékelési eljárásrend ... 45
5.2. Biztonsági értékelések ... 45
5.4. Biztonsági értékelések – Kiberbiztonsági audit ... 45
5.7. Információcsere ... 46
5.10. Az intézkedési terv és mérföldkövei ... 46
5.12. Engedélyezés ... 46
5.15. Folyamatos felügyelet ... 46
5.18. Folyamatos felügyelet – Kockázatmonitorozás ... 47
5.25. Belső rendszerkapcsolatok ... 47
6. KONFIGURÁCIÓKEZELÉS ... 48
6.1. Konfigurációkezelési eljárásrend ... 48
6.2. Alapkonfiguráció ... 48
6.15. Biztonsági hatásvizsgálatok ... 49
6.18. A változtatásokra vonatkozó hozzáférés korlátozások ... 49
6.23. Konfigurációs beállítások ... 49
6.26. Legszűkebb funkcionalitás ... 49
6.36. Rendszerelem leltár ... 49
6.36.1. Hardver nyilvántartás ... 50
6.36.2. Szoftver nyilvántartás ... 50
6.47. A szoftverhasználat korlátozásai ... 51
6.49. Felhasználó által telepített szoftver ... 52
6.49.1. Telepítés nélkül futtatható szoftverek ... 52
6.49.2. Automatizáltan települő szoftverek ... 52
7. KÉSZENLÉTI TERVEZÉS ... 53
7.1. Üzletmenet-folytonosságra vonatkozó eljárásrend ... 53
7.2. Üzletmenet-folytonossági terv ... 53
7.2.1. Informatikai üzletmenet-folytonossági terv (BCP terv) ... 53
7.2.2. Informatikai katasztrófa-elhárítási terv (DRP terv) ... 54
7.10. A folyamatos működésre felkészítő képzés ... 55
7.35. Az elektronikus információs rendszer mentései ... 55
7.35.1. Adatok mentése ... 55
7.35.2. Szoftverek, eseménynaplók, kapcsolódó dokumentációk mentése ... 55
7.35.3. Archiválás ... 56
7.35.4. Adatok hosszú távú megőrzése ... 56
7.35.5. Mentés adathordozók tárolása, kezelése ... 56
7.35.6. A mentési rendszer dokumentálása ... 56
7.43. Az elektronikus információs rendszer helyreállítása és újraindítása ... 57
8. AZONOSÍTÁS ÉS HITELESÍTÉS ... 58
8.1. Azonosítási és hitelesítési eljárásrend ... 58
8.2. Azonosítás és hitelesítés ... 58
8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése ... 58
8.7. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem ... 58
8.14. Azonosító kezelés ... 58
8.21. A hitelesítésre szolgáló eszközök kezelése ... 59
8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés ... 60
8.22.1. Informatikai rendszerek jelszókezelésének követelményei ... 60
8.22.2. Kezdeti jelszavak kezelése ... 60
8.22.3. Jelszavak kiválasztásának követelményei ... 61
8.22.4. Jelszavak rendszeres megváltoztatása ... 61
8.22.5. Felhasználók felelőssége a jelszóhasználat során ... 61
8.22.6. Beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelése ... 62
8.22.7. A többtényezős hitelesítésre szolgáló eszközök, tanúsítványok kezelése ... 62
8.36. Hitelesítési információk visszajelzésének elrejtése ... 63
8.37. Hitelesítés kriptográfiai modul esetén ... 63
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) ... 63
8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata 63
8.43. Újrahitelesítés ... 64
9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE ... 65
9.1. Biztonsági eseménykezelési eljárásrend ... 65
9.2. Képzés a biztonsági események kezelésére ... 65
9.9. Biztonsági események kezelése ... 65

9.25. A biztonsági események nyomonkövetése ... 66
9.27. A biztonsági események jelentése ... 66
9.27.1. A biztonsági esemény jelentése a Hivatal vezetője és az incidenskezelő központ felé ... 67
9.27.2. Természetes személyek adatait érintő adatvédelmi incidens jelentése ... 68
9.31. Segítségnyújtás a biztonsági események kezeléséhez ... 68
9.34. Biztonsági eseménykezelési terv ... 68
10. KARBANTARTÁS ... 69
10.1. Karbantartási eljárásrend ... 69
10.2. Szabályozott karbantartás ... 69
10.11. Távoli karbantartás ... 70
10.18. Karbantartó személyek ... 71
11. ADATHORDOZÓK VÉDELME ... 72
11.1. Adathordozók védelmére vonatkozó eljárásrend ... 72
11.2. Hozzáférés az adathordozókhoz ... 73
11.8. Adathordozók törlése ... 73
11.14. Adathordozók használata ... 74
12. FIZIKAI ÉS KÖRNYEZETI VÉDELEM ... 75
12.1. Fizikai és környezeti védelemre vonatkozó eljárásrend ... 75
12.2. A fizikai belépési engedélyek ... 75
12.2.1. Védett területekhez történő hozzáférés ... 75
12.2.2. Kiemelten védett területekhez történő hozzáférés ... 76
12.2.2.1. Egyedi hálózati rack szekrények védelme ... 76
12.2.3. Belépésre jogosultak listája ... 77
12.2.4. Belépési engedélyek kiadása ... 78
12.2.5. Belépési engedélyek visszavonása ... 79
12.6. A fizikai belépés ellenőrzése ... 79
12.6.1. Munkavállalók belépésének naplózása ... 79
12.6.2. Ügyfelek, külső partnerek, vendégek belépésének naplózása ... 80
12.6.3. Kártyabirtoklással összefüggő feladatok, felelősségek ... 80
12.6.4. Rendellenességek kezelése ... 80
12.6.5. Belépések ellenőrzése ... 81
12.17. A fizikai hozzáférések felügyelete ... 81
12.17.1. A fizikai hozzáférések felügyelete - Behatolásjelző és megfigyelő berendezések ... 81
12.22. Látogatói hozzáférési naplók ... 82
12.31. Vészvilágítás ... 82
12.33. Tűzvédelem ... 82
12.37. Környezeti védelmi intézkedések ... 82
12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem ... 83
12.42. Be- és kiszállítás ... 83
13. TERVEZÉS ... 84
13.1. Biztonságtervezési eljárásrend ... 84
13.2. Rendszerbiztonsági terv ... 84
13.3. Viselkedési szabályok ... 84
13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások ... 85
13.4.1. Az Internet biztonsága ... 85
13.4.2. Az Internet hozzáférések ellenőrzése ... 86
13.4.3. Az elektronikus levelezés biztonsága ... 86
13.4.4. Az elektronikus levelezés ellenőrzése ... 88
13.4.5. Tiszta asztal és tiszta képernyő politika ... 88
13.10. Biztonsági követelmények kiválasztása ... 89
13.11. Biztonsági követelmények testre szabása ... 89
14. SZEMÉLYI BIZTONSÁG ... 90
14.1. Személyi biztonságra vonatkozó eljárásrend ... 90
14.2. Munkakörök biztonsági szempontú besorolása ... 90
14.3. Személyek háttérellenőrzése ... 90
14.5. Személyek munkaviszonyának megszűnése ... 90
14.5.1. Hozzáférési jogosultságok megszüntetése ... 91
14.5.2. Személyi hitelesítő eszközök, vagyontárgyak visszavétele ... 91
14.5.3. Felhasználói adatok mentése ... 91
14.8. Az áthelyezések, átirányítások és kirendelések kezelése ... 92
14.9. Hozzáférési megállapodások ... 92
14.11. Külső személyekhez kapcsolódó biztonsági követelmények ... 92
14.12. Fegyelmi intézkedések ... 93
14.13. Munkaköri leírások ... 93
15. KOCKÁZATKEZELÉS ... 94
15.1. Kockázatelemzési és kockázatkezelési eljárásrend ... 94

15.2. Biztonsági osztályba sorolás ... 94
15.4. Kockázatelemzés ... 95
15.5. Kockázatelemzés – Ellátási lánc ... 95
15.9. Sérülékenységek ellenőrzése ... 95
15.18. Sérülékenységmenedzsment – Sérülékenységi információk fogadása ... 95
15.20. Kockázatokra adott válasz ... 95
16. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS ... 96
16.1. Beszerzési eljárásrend ... 96
16.1.1. A bevezetés kezdeményezése és projektterv készítése ... 96
16.1.2. A beruházás és bevezetés folyamata ... 96
16.1.3. Alkalmazói rendszerek/szoftverek bevezetése ... 97
16.1.4. Alkalmazói rendszerek/szoftverek fejlesztése ... 98
16.1.5. Kiszervezett fejlesztés ... 99
16.1.6. Alkalmazói rendszerek/szoftverek beszerzése ... 99
16.1.7. Dobozos szoftverek vásárlása vagy bérlése ... 99
16.1.8. Szabad szoftverek bevezetése ... 99
16.1.9. Alkalmazói rendszerek/szoftverek módosítása ... 100
16.2. Erőforrások rendelkezésre állása ... 101
16.3. A rendszer fejlesztési életciklusa ... 101
16.7. Beszerzések ... 103
16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai ... 105
16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció ... 105
16.16. Biztonságtervezési elvek ... 105
16.49. Külső elektronikus információs rendszerek szolgáltatásai ... 105
16.99. Támogatással nem rendelkező rendszerelemek ... 105
17. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM ... 107
17.1. Rendszer- és kommunikációvédelmi eljárásrend ... 107
17.12. Szolgáltatásmegtagadással járó támadások elleni védelem ... 107
17.17. A határok védelme ... 107
17.49. Kriptográfiai kulcs előállítása és kezelése ... 108
17.53. Kriptográfiai védelem ... 108
17.54. Együttműködésen alapuló informatikai eszközök ... 108
17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás) ... 109
17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás) ... 109
17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén ... 109
17.108. A folyamatok elkülönítése ... 109
18. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG ... 110
18.1. Rendszer- és információsértetlenségi eljárásrend ... 110
18.2. Hibajavítás ... 110
18.8. Kártékony kódok elleni védelem ... 111
18.8.1. A felhasználók feladatai a vírusfertőzés megelőzése érdekében: ... 111
18.8.2. Levélszemét szűrése ... 113
18.13. Az EIR monitorozása ... 113
18.37. Biztonsági riasztások és tájékoztatások ... 114
18.67. Információ kezelése és megőrzése ... 114
19. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE ... 115
19.1. Ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrend ... 115
19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat ... 115
19.4. Ellátási láncra vonatkozó követelmények és folyamatok ... 115
19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók ... 115
19.13. Beszerzési stratégiák, eszközök és módszerek ... 115
19.19. Értesítési megállapodások ... 115
19.22. Rendszerek vagy rendszerelemek vizsgálata ... 115
19.23. Rendszerelem hitelessége ... 116
19.24. Rendszerelem hitelessége – Hamisítás elleni képzés ... 116
19.25. Rendszerelem hitelessége – Konfigurációfelügyelet ... 116
19.27. Rendszerelem selejtezése, megsemmisítése ... 116
MELLÉKLET ... 117

Az Információbiztonsági szabályzat

A Szerencsi Közös Önkormányzati Hivatal Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban Kiberbiztonsági tv. vagy törvény) 1. § (1) bekezdés a) pontja szerinti, az 1. mellékletben felsorolt, közigazgatási ágazathoz tartozó szervezet. Az 1. § (4) bekezdésének a) pontja alapján - a település által nyújtott szolgáltatásnak az állam, a társadalom, a gazdaság működése szempontjából való kritikussága, valamint a Hivatal mérete alapján - fontos szervezetnek minősül.

A szervezet vezetője, a jegyző a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására elektronikus információs rendszerek biztonságáért felelős személyt nevezett ki, aki elkészítette a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó jelen Információbiztonsági szabályzatot.

A törvényben kapott felhatalmazása alapján a Hivatal Információbiztonsági szabályzatát az alábbiakban határozza meg, mely átfogó képet nyújt a biztonsági követelményekről, valamint a követelményeknek való megfelelés érdekében a működtetett vagy bevezetni kívánt védelmi intézkedésekről. Tartalmazza a Hivatalra vonatkozó, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendeletben meghatározott adminisztratív, logikai és fizikai védelmi intézkedéseket.

A szabályzatot a Hivatal vezetője, a jegyző adja ki, aki felelősséget vállal és elszámoltatható a szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért.

A szabályzat összhangban áll a hatályos jogszabályokkal, köztük az alábbiakkal:

- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvénnyel (Kiberbiztonsági tv.),
- Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelettel (Kiberbiztonsági vhr.)
- A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelettel (MK rendelet).

Célok

Az Információbiztonsági szabályzat célja, hogy:

- szabályozza a Hivatal számára értéket képviselő információk védelméről történő gondoskodást,
- meghatározza a célkitűzéseket (pl. a szervezet értékeinek védelme a jogkövető magatartás és a jó hírnév érdekében, az információbiztonság növelése a tudatosság, szervezettség, hatékonyság és a technikai megoldások használata segítségével, a megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését)
- a ható- és szerepköröket, a felelősségeket,
- a vezetői elkötelezettséget,
- a szervezeten belüli együttműködés kereteit és a
- megfelelőségi kritériumokat.

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)

Felülvizsgálat

A Hivatal az Információbiztonsági szabályzatot és a kapcsolódó közjogi szervezetszabályzó eszközöket, eljárásrendeket, függelékeket folyamatosan fejleszti és tökéletesíti, legalább kétévente vagy a jogszabályban meghatározott esetekben felülvizsgálja. 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 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 a biztonságáért Felelős vagy a jegyző által kijelölt személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása, kihirdetése jegyző hatásköre.

Az Információbiztonsági szabályzatot a nemzeti kiberbiztonsági hatóság a Kiberbiztonsági törvényben meghatározott feladatainak végrehajtása céljából nyilvántartja és kezeli, a szervezet vezetője gondoskodik a hatósági nyilvántartáshoz történő adatszolgáltatásról vagy azzal megbízza a meglévő bejegyzése alapján arra jogosult biztonságért Felelőst.

Hatály

Jelen Információbiztonsági szabályzat területi hatálya kiterjed a Hivatal szervezetén kívül a Szervezeti és Működési Szabályzat szerinti települési önkormányzatára is:

1) **Szerencsi Közös Önkormányzati Hivatal**
2) **Szerencs Város Önkormányzata**
3) **Mád Község Önkormányzata**

Területi hatálya kiterjed a Hivatal székhelyére és minden telephelyére (továbbiakban együttesen: telephely), továbbá mindazon területekre, ahol a Hivatal informatika használatával a tevékenységét kifejti, függetlenül annak geográfiai elhelyezkedésétől. A szabályzat területi hatálya nem terjed ki a Hivatal tulajdonában lévő, de 3. személynek tartós használatra átadott fizikai területre abban az esetben, ha a 3. személy semmilyen módon nem csatlakozik a Hivatal informatikai infrastruktúrájához.

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. Kiterjed a Hivatal informatikai erőforrásainak üzemelési helyszíneire, a külső szolgáltatók által a Hivatalnak nyújtott szolgáltatásban érintett helyszíneire.

A szabályzat **személyi hatálya** kiterjed a Hivatallal munkavégzésre irányuló jogviszonyban álló természetes személyekre. Jelen szabályzat rendelkezéseit kell alkalmazni és alkalmazását megkövetelni azoktól, akik kapcsolatba kerülnek az informatikai rendszereivel (használják, üzemeltetik, fejlesztik, telepítik, javítják stb.):

a) a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek esetében;
b) más szervezetek képviseletében a Szervezet munkahelyein vagy ezek környezetében tartózkodó személyekre;
c) a rendszerek bármely részén karbantartást végző támogató személyzetre.

Az Információbiztonsági szabályzat a Hivatal egészére vonatkozik, **tárgyi hatálya** kiterjed a Hivatal birtokában levő összes olyan eszközre, amelyek az alaprendeltetésből adódó, a Hivatal/Önkormányzat ügyviteli tevékenységével kapcsolatos feladatok ellátását biztosítják. A szabályzat tárgyi hatálya kiterjed a Hivatal informatikai rendszereire, így az informatikai rendszert alkotó

a) környezeti infrastruktúra elemeire;
b) hardver eszközökre, készülékekre, berendezésekre;
c) szoftverekre;
d) adathordozókra;
e) dokumentációkra;
f) az informatikai rendszerekben rögzített, tárolt, feldolgozott vagy továbbított adatokra.

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

Hatásköri és illetékességi szabályok

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

A jegyző feladata gondoskodni arról, hogy az Információbiztonsági szabályzat jogosulatlanok számára ne legyen megismerhető, módosítható.

Szerepkörök, tevékenységek, felelősségek

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

Az egyes kontrollfolyamatokban kötelező együttműködési szabályokat az eljárásrendek előírásai részletezik.

Általában minden érintett személy köteles:

a) jelen szabályzat és kapcsolódó dokumentumok előírásait megismerni és magára nézve, nyilatkozat keretében kötelezőnek elismerni,
b) az információbiztonsági tárgyú belső képzéseken részt venni,
c) személyét érintő biztonsági ellenőrzéseket, auditokon az ellenőrző személyek kérése szerint részt venni,
d) az általa biztonsági eseményként vélelmezett történéseket a felettes vezetőnek és/vagy a biztonságáért Felelős felé jelenteni.

Az Információbiztonsági szabályzat 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
a Hivatal vezetője, a jegyző	1) Az elektronikus információs rendszerek védelme érdekében - szervezeti döntésre nem teljes körű - kockázatmenedzsment keretrendszert hoz létre és működtet, ennek keretében: 1. gondoskodik a Hivatal által használt elektronikus információs rendszerek, központi szolgáltatások felméréséről és nyilvántartásba vételéről; 2. meghatározza a Hivatal rendelkezésében lévő, továbbá a Hivatal használatában lévő elektronikus információs rendszerek védelmével kapcsolatos szerepköröket, felelősöket, feladatokat és az ehhez szükséges hatásköröket, kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt; Az elektronikus információs rendszer biztonságáért felelős személy kijelölését vagy megbízását megelőzően meggyőződik a jogszabályi követelményeknek való megfelelőségéről, megbízását követően nyilvántartásba vétel érdekében bejelenti a nemzeti kiberbiztonsági hatóság részére, egyidejűleg megküldi a bejelentett adatokat igazoló dokumentumokat. A biztonságért Felelős személy büntetlen előéletét igazolja, a felelős személyt kötelezheti, hogy a Hivatallal fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja. 3. gondoskodik a Hivatal rendelkezésében lévő elektronikus információs rendszerben kezelt adatok felméréséről és osztályozásáról;

Szerepkör	Főbb felelősségek, tevékenységek
	4. hatáselemzést és kockázatmenedzsment tevékenységet végez a Hivatal rendelkezésében lévő elektronikus információs rendszerekre és azok környezetére vonatkozóan; 5. meghatározza a Hivatal rendelkezésében lévő elektronikus információs rendszerek biztonsági osztályát; 6. meghatározza a Hivatal rendelkezésében lévő elektronikus információs rendszerek vonatkozásában a kockázatokkal arányos védelmi intézkedéseket; 7. kiadja a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó információbiztonsági szabályzatot, valamint gondoskodik annak legalább kétévente vagy a jogszabályban meghatározott esetekben történő felülvizsgálatáról; 8. biztosítja az elektronikus információs rendszerek védelme vonatkozásában meghatározott védelmi intézkedések teljesülését; 9. gondoskodik – ha releváns – az európai uniós jogi aktusban foglaltak, valamint az informatikáért felelős miniszter rendelete szerint kiválasztott védelmi intézkedések megfelelőségének első biztonsági osztályba sorolás alkalmával történő értékeléséről; 10. rendszeresen, legalább kétévente, a biztonsági osztályba sorolás felülvizsgálatával egyidejűleg gondoskodik a védelmi intézkedések időszakos értékeléséről, ennek keretében legalább kockázatelemzések, ellenőrzések, független és a kiberbiztonsági hatóság által kiadott ajánlás szerinti belső kiberbiztonsági értékelés lefolytatása révén meggyőződik arról, hogy a jogszabályoknak és a kockázatoknak megfelelően meghatározott védelmi intézkedések megfelelően biztosítják-e a szervezet és elektronikus információs rendszerei biztonságát; 11. gondoskodik a biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során feltárt hiányosságok orvoslásáról; 12. a Hivatal belül dönt az elektronikus információs rendszerek használatbavételéről vagy használatának folytatásáról és 13. gondoskodik a kiberbiztonsági hatósági kötelezések teljesítéséről. 2) Az elektronikus információs rendszer védelmének biztosítása érdekében: a) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a Hivatal munkatársainak – az informatikáért felelős miniszter rendeletében meghatározott – kiberbiztonsági képzéséről, továbbképzéséről; b) ha kötelezően előírt, akkor biztosítja a hazai kiberbiztonsági gyakorlatokon történő részvételt, illetve kiberbiztonsági gyakorlat önálló megtartását; c) gondoskodik az elektronikus információs rendszer eseményeinek nyomon-követhetőségéről; d) ha a Hivatal közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a Hivatal elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; e) az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a gyors és hatékony reagálásról, az illetékes kiberbiztonsági incidenskezelő központnak való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról; f) gondoskodik az érintetteknek a kiberbiztonsági incidensekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáról; g) gondoskodik a kiberbiztonsági hatóság és az illetékes kiberbiztonsági incidenskezelő központ ajánlásainak, iránymutatásainak az elektronikus információs rendszer védelmének biztosítása érdekében történő figyelembevételéről; h) köteles törekedni arra, hogy a jelen jogszabályban meghatározott feladatokat a lehető legrövidebb időn belül hajtsa végre; i) gondoskodik arról, hogy a Hivatal által az adott évben informatikai fejlesztésre fordított költségek legalább 5%-ának megfelelő összeget a Hivatal a tárgyév során kiberbiztonsági fejlesztésekre fordítson és

Szerepkör	Főbb felelősségek, tevékenységek
	j) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket. 3) A Hivatal vezetője biztosítja, hogy a biztonságért Felelős: a) valamennyi, az elektronikus információs rendszerek védelmét érintő döntés előkészítésében részt vegyen; b) rendelkezésére álljanak az elektronikus információs rendszer védelmének biztosításához szükséges feltételek, jogosultságok, információk, humán- és anyagi erőforrások; c) hozzáférjen mindazon rendszerekhez, adatokhoz és információkhoz, amelyek az általa ellátandó feladatok végrehajtásához szükségesek.
Az elektronikus információs rendszer biztonságáért felelős személy – Felelős/ biztonságért Felelős *(vállalkozási szerződés alapján külső szakértő)*	1. Feladatát a Hivatal igényeihez igazodva és annak rendelkezése szerint látja el, legalább háromhavonta egy napon, dokumentált módon, fizikai jelenlét mellett. 2. A nemzeti kiberbiztonsági hatóság előtti eljárásra a nemzeti kiberbiztonsági hatóság általi nyilvántartásba vételét követően jogosulttá válik és képviseleti joga megszűnésének bejelentéséig vagy a nemzeti kiberbiztonsági hatóság általi hivatalból való törléséig képviseletre jogosult személynek kell tekinteni. 3. Az elektronikus információs rendszer biztonságáért felelős személy: a) gondoskodik az elektronikus információs rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, b) gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről keretében, c) előkészíti és átadja vagy előzetes egyeztetésnek megfelelően a Hivatal vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a Hivatal információbiztonsági szabályzatát, gondoskodik annak legalább kétévente vagy a jogszabályban meghatározott esetekben történő felülvizsgálatáról d) előkészíti a Hivatal elektronikus információs rendszereinek biztonsági osztályba sorolását, legalább kétévente, vagy az elektronikus rendszer biztonságát érintő, jogszabályban meghatározott változás esetén soron kívül, dokumentált módon felülvizsgálja, e) az elektronikus információs rendszer biztonsági osztálya alapján meghatározza az előírt védelmi intézkedéseket az adott elektronikus információs rendszerre vonatkozóan, f) előkészíti az elektronikus információs rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szerinti osztályozását, g) előkészíti és a Hivatal vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a Hivatal elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat, h) megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket, i) véleményezi az EIR-ek biztonsága szempontjából a Hivatal elektronikus információbiztonságot érintő, számára eljuttatott szabályzatait és szerződéseit, j) folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a Hivatal elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a Hivatal vezetője számára, k) felülvizsgálja, hogy a Hivatal elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a Hivatal belső szabályozóival, l) az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a Hivatal vezetője számára, m) ha az adott elektronikus információs rendszerre vonatkozó biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során hiányosság kerül megállapításra, akkor a vizsgálatot követő 90 napon belül intézkedési tervet készít a hiányosság megszüntetésére, legalább évente megvizsgálja az intézkedési tervet és beszámolót készít a Hivatal vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket, n) kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal, o) a Hivatal bármely elektronikus információs rendszerét érintő incidensről tájékoztatja e rendeletben meghatározott szervet,

Szerepkör	Főbb felelősségek, tevékenységek
	p) a megbízás alatt fenntartja a számára szükséges képzettséget - ideértve az informatikáért felelős miniszter rendeletében meghatározott szakmai képzési, továbbképzési kötelezettség teljesítését is -, gyakorlatot, valamint a büntetlen előélet követelményének való megfelelést. p) szakértői támogatást nyújt a kiberbiztonsági hatóság által az Automatizált Sebezhetőség-detektáló Rendszer (ASR) használatával havonta végzett, a jogosultság nélkül elérhető (black-box) szolgáltatások sérülékenységeinek feltárására irányuló sérülékenység-vizsgálatok eredményének értelmezésében. A feltárt sérülékenységek javításának elvégzése a Hivatal felelőssége.
Az elektronikus információs rendszer biztonságáért felelős személy helyettesítésére jogosult személy/ helyettes Felelős	Az elektronikus információs rendszer biztonságáért felelős személy távolléte vagy akadályoztatása esetén teljeskörűen ellátja az elektronikus információs rendszer biztonságáért felelős személy feladatait.
Adatgazda *(annak a szervezeti egységnek a vezetője, ahová a jogszabály vagy közjogi szervezetszabályzó eszköz az adat kezelését rendeli, illetve, ahol az adat keletkezik)* *- a szervezeti egység vezetője, hiányában a jegyző*	Tisztviselő, aki jogszabályi vagy műszaki szempontú rendelkezési jogkörrel rendelkezik az EIR adatokkal kapcsolatban és felelős a Rendszerbiztonsági tervben az információk létrehozásának, begyűjtésének, feldolgozásának, terjesztésének és megsemmisítésének ellenőrzéséért. 1. meghatározza az adatok kezelésének célját, és meghozza az adatkezelésre vonatkozó döntéseket 2. engedélyezi a külső és belső felhasználók különböző szintű hozzáférését az informatikai rendszerhez 3. engedélyezi a rendszerben végzett változtatásokat, 4. részt vesz a felügyelete alatt álló informatikai rendszerre vonatkozóan mentési követelmények, az Üzletmenet-folytonossági és katasztrófaelhárítási terv követelményeinek meghatározásában, megvalósításában (Adatvesztési tűrés (RPO), Elfogadható helyreállítási idők (RTO) meghatározása, alternatív, tartalék ügymenet intézkedések, alternatív hivatali folyamatokra való átállásban és a normál hivatali folyamatokra való visszaállásban, 5. közreműködik az információbiztonsági kockázatok elemzésében (azonosítja, felméri, értékeli a szakterületére vonatkozó kockázatokat, javaslatot tesz a magas és kritikus kockázatok kezelésére) 6. együttműködik az elektronikus információs rendszer biztonságáért felelőssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárások, szabályok, felelősségek, kötelező vagy tiltott tevékenységek, viselkedési szabályok meghatározásában, 7. részt vesz a fizikai biztonsági követelmények kialakításában és felügyeletében 8. gondoskodik arról, hogy a felelőssége alá tartozó szervezeti egység munkatársai megismerjék és betartsák a rájuk vonatkozó információbiztonsági követelményeket, szabályokat, 9. közreműködik az elektronikus információs rendszer biztonságáért felelős által a követelmények teljesülésének ellenőrzése során, 10. saját és a felelőssége alá tartozó munkatársak információbiztonsági, informatikai fennakadásról tett észrevételeit jelenti a rendszergazdának
Informatikai rendszer kijelölt felelőse / Kulcsfelhasználó	1. Jogosultsági körében eljárva elvégzi vagy a rendszergazdával elvégezteti a saját üzemeltetésű szakági szoftverek esetén az adatbázist, adatváltozást érintő frissítéseket. 2. Vétlen adattörléskor szükség esetén a felettesével való egyeztetést követően elvégzi a helyreállítást vagy együttműködik a rendszergazdával a helyreállításban és ellenőrzésben. 3. Közreműködik az információbiztonsági kockázatok elemzésében. Együttműködik a biztonságáért Felelőssel, az elektronikus információs rendszerhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárások, szabályok, felelősségek, kötelező vagy tiltott tevékenységek, viselkedési szabályok meghatározásában. 4. Közreműködik az elektronikus információs rendszer biztonságáért felelős által a követelmények teljesülésének ellenőrzése során.

Szerepkör	Főbb felelősségek, tevékenységek
Rendszergazda	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 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 a biztonságáért Felelőssel és az adatgazdákkal az információbiztonsági kockázatok elemzésében, 8. elvégzik a logok elemzését és jelentést készít róla a biztonságáért Felelős felé 9. információbiztonsági incidens észlelése esetén haladéktalanul jelentést tesz az biztonságért Felelős felé, a biztonsági esemény elhárítását megkezdi, az eredményéről tájékoztatást nyújt az érintetteknek, 10. saját hatókörében rendszeres fizikai és logikai karbantartásokat végez és dokumentál (karbantartási napló), 11. a biztonságért Felelőssel közreműködve, meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket, 12. az adatgazdákkal és a biztonságáért Felelőssel együttműködve kialakítja az adatmentési rendszert, naprakészen tartja a mentési rendet, elvégzi/felügyelti az előírt gyakoriság szerinti adatmentéseket, 13. elvégzi a szükség szerinti helyreállításokat, visszaállítási teszteket, 14. hiba esetén elvégzi vagy felügyeli az eszközök javítását (a szerződésnek/a jegyző utasításának megfelelően vagy vele egyeztetve), 15. közreműködik a biztonságáért Felelőssel a BCP/DRP tervek kidolgozásában és megvalósításában, 16. kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat, 17. a biztonságáért Felelőssel egyeztetve vezeti jelen szabályzatban előírt nyilvántartásokat, vagy számára alap adatokat szolgáltat (a Hivatal vezetőjének utasítása szerint)
Felhasználók *(a szabályzat személyi hatálya alá tartozók: a közszolgálati jogviszony, a munkaviszony, a közalkalmazotti és egyéb foglalkoztatásra irányuló jogviszony alapján foglalkoztatottak, a Hivatallal szerződéses kapcsolatban álló természetes és jogi személyek) egyes környezetben: munkavállalók*	1. köteles az Információbiztonsági szabályzatban rá vonatkozó szabályokat megismerni, 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 rendszer 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, kódjait, 7. köteles részt venni a Hivatalon belül szervezett információbiztonsági oktatásokon, illetve a jegyző utasítása szerint más külső oktatásokon, 8. a birtokában lévő, vagy tudomására jutott információkat bizalmasan kezeli, 9. felelősséggel tartozik a munkavégzése során az elektronikus információs rendszerben végzett feladatokért, a szakrendszerek szakszerű használatáért, 10. felelősséggel tartozik a munkavégzéséhez szükséges, számára kiadott eszközök megfelelő fizikai, logikai védelméért, 11. elszámoltatható minden olyan tevékenységért, amelyet bárki a számára kiadott azonosítói alapján végzett, 12. valamennyi üzemeltető, pl. az ASP központ működtetője által kiadott felhasználói biztonsági követelményeket köteles követni és betartani,

Szerepkör	Főbb felelősségek, tevékenységek
	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.
Fizikai biztonsági munkatárs	A recepció /portaszolgálat /biztonsági feladatokkal megbízott külső szervezet munkatársa, hiányában helyben dolgozó, a fizikai belépés ellenőrzésével megbízott. Felügyelet alatt tartja a Hivatal telephelyeire, épületeibe történő fizikai be- és kilépéseket a 12.1. Fizikai és környezeti védelemre vonatkozó eljárásrend alapján.
HR szervezet /HR munkatárs	A Hivatal HR feladatokat ellátó szervezeti egysége/munkatársa. Ellátja főként a 14.1. A személyi biztonságra vonatkozó eljárásrend, a 2.1. Hozzáférés-felügyeleti eljárásrend és egyéb eljárásokban leírt feladatokat.
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, 2. a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Automatizált Sebezhetőségdetektáló Rendszere által feltárt weboldallal kapcsolatos sérülékenységek javítása **Üzemeltető:** 1. a védekezés külső (belső) támadás ellen, 2. a használt szolgáltatások folyamatos frissítése karbantartása, 3. lehetőség szerint a szolgáltatások verziószámainak elrejtése, 4. a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Automatizált Sebezhetőségdetektáló Rendszere által feltárt, a szerverrel és a futó szolgáltatásokkal kapcsolatos sérülékenységek javítása **A tartalom felelős** (Hivatal által kijelölt munkatárs): 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 tartalom ellenőrzéséért felelős** (Hivatal által kijelölt vezető vagy munkatárs): A tartalom feltöltése előtt átvizsgálja és rendszeres időközönként ellenőrzi a nyilvánosan hozzáférhető elektronikus információs rendszertartalmat a nem nyilvános információk tekintetében és eltávolíttatja azokat.
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.

Adatosztályozás

Az adatosztályozás a Hivatal rendelkezésében lévő elektronikus információs rendszerekben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából. Célja, hogy a rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szempontjából értékelésre kerüljenek és azok biztonsági súlyának megfelelően kerüljön kialakításra a kockázatarányos védelem. Hozzájárul az elektronikus információs rendszerben kezelt adatok külföldön vagy felhőben történő kezelésének egyértelmű meghatározásához.

A Hivatal a rendelkezésében lévő elektronikus információs rendszerekben kezelt adatok és információk adatosztályozását a biztonsági osztályba sorolás keretében a Kiberbiztonsági vhr. 1. mellékletében meghatározott irányadó szempontokat figyelembe véve végzi el és az EIR nyilvántartásban dokumentál. Az adatosztályozás eredményét a biztonsági osztályba sorolás eredményének bejelentése keretében bejelenti a nemzeti kiberbiztonsági hatóság részére.

Az adatosztályozást a biztonságért Felelős az adatgazdák bevonásával végzi, az adatok bizalmasság szerinti besorolása tekintetében a Hivatal adatvédelmi tisztviselőjének bevonásával. Ennek keretében azonosítják a rendszer által feldolgozott, tárolt és továbbított adatok típusait, majd az adatok és a rendszer tekintetében vizsgálják a bizalmasság, sértetlenség vagy rendelkezésre állás hatásértékét (alap, jelentős, magas). Figyelembe veszik a logikailag együtt, egységben kezelt elektronikus adatok – ideértve az adatbázist, adattárat, egyedi dokumentumot és egyéb adatállományt – együttes biztonsági igényét.

A kezelt adatok fajtája lehet személyes adat vagy különleges személyes adat, az EIR-ben kezelt adatok mennyisége lehet csekély, közepes, nagy vagy jelentős.

A Hivatal nem privát felhőszolgáltatást vagy külföldi adatkezelést kizárólag az adatosztályozás alapján, annak eredményére figyelemmel vehet igénybe, amennyiben más jogszabály a felhőszolgáltatás igénybevételét, vagy a külföldi adatkezelést nem tiltja vagy korlátozza. A tervezett külföldi adatkezelésre vagy nem privát felhőhasználatra irányuló döntést megelőzően költség-haszon elemzést és kilépési tervet szükséges készíteni. A költség-haszon elemzés keretében a szervezet vizsgálja és kimutatja az aktuálisan alkalmazott technológiához képest a nem privát felhőszolgáltatás igénybevételével járó előnyöket és hátrányokat, a kilépési terv keretében megtervezi a felhőszolgáltatás alkalmazásáról a helyi környezetre vagy privát felhő használatára történő visszaállás lépéseit, annak következményeit és költségvonzatát.

A jegyző abban az esetben dönthet a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele mellett, amennyiben a költség-haszon elemzés és a kilépési terv eredményei alapján a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele a Hivatal számára megalapozottan előnyökkel jár.

Az adatosztályozás felülvizsgálata az elektronikus információs rendszerei biztonsági osztályának felülvizsgálata vagy az elektronikus információs rendszerben kezelendő adatok körében bekövetkezett változás esetén szükséges.

VÉDELMI INTÉZKEDÉSEK

A Szerencsi Közös Önkormányzati Hivatal a rendelkezésében lévő elektronikus információs rendszerekre (továbbiakban EIR-ekre vagy rendszerekre) vonatkozóan a követelményeknek való megfelelés érdekében az alábbi intézkedéseket határozta meg a működtetett vagy bevezetni kívánt védelmi intézkedésekről.

Jelen Információbiztonsági szabályzatban szereplő intézkedések a biztonsági osztály meghatározás alapján elvárt „Alap" biztonsági osztályhoz tartozó védelmi intézkedéseknek felelnek meg.

Az intézkedések sorszámozása és követelményei megfelelnek a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (MK rendelet) 2. mellékletében előírt intézkedésekkel.

A más szervezet rendelkezésében, de a Hivatal használatában lévő elektronikus információs rendszerek védelméhez kapcsolódó követelményeket a Hivatal kockázatarányosan alkalmazza, a központi rendszer felett rendelkezési jogot gyakorló szervezet által meghatározott információbiztonsági követelményeket teljesíti.

1. PROGRAMMENEDZSMENT

1.1. Információbiztonsági szabályzat

A Hivatal vezetője az elektronikus információs rendszer biztonságáért felelős szakmai irányításával kidolgozza és kihirdeti jelen Információbiztonsági szabályzatát. A szabályzat, eljárásai kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításért a biztonságért Felelős felel.

A szabályzatot és eljárásrendjeit szükség szerint, de legalább évente az informatika biztonsági rendszer felülvizsgálata során, illetve az információbiztonsági rendszer rendkívüli módosításakor vagy biztonsági esemény bekövetkeztekor felülvizsgálja, szükség szerint módosítani szükséges.

A jegyző felelősséget vállal és elszámoltatható a szervezeti műveletek (beleértve a célkitűzéseket, funkciókat, imázst és hírnevet), a szervezeti eszközök, személyek, más szervezetek szempontjából számottevőnek tartott kockázatokért.

Az Információbiztonsági szabályzatot védeni kell a jogosulatlan megismeréssel és módosítással szemben.

1.2. Elektronikus információs rendszerek biztonságáért felelős személy

A Hivatal vezetője a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására elektronikus információs rendszerek biztonságáért felelős személyt (biztonságért Felelős) és az elektronikus információs rendszer biztonságáért felelős személy helyettesítésére jogosult személyt (helyettes Felelős) nevez ki és biztosítja a célok eléréséhez szükséges erőforrásokat. A helyettesítésre jogosult személy az elektronikus információs rendszerek biztonságáért felelős távolléte vagy akadályoztatása esetén teljeskörűen ellátja az elektronikus információs rendszer biztonságáért felelős személy feladatait. A felelős és a helyettesítésre jogosult személy megállapodás alapján külső szakértő, személyükben nem áll fenn összeférhetetlenség, nem a Hivatal gazdasági vezetői feladatait ellátó személy vagy az a személy, aki a szervezeten belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el, illetve nem tartozik ilyen személy közvetlen alárendeltségébe.

A helyettesítésre jogosultra az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó rendelkezéseket kell alkalmazni. A biztonságáért Felelős és a helyettes Felelős a megbízás alatt fenntartja a számára szükséges képzettséget - ideértve a rendeletekben meghatározott szakmai képzési, továbbképzési kötelezettség teljesítését is -, gyakorlat, valamint a büntetlen előélet követelményének való megfelelést.

A nemzeti kiberbiztonsági hatóság a Kiberbiztonsági törvényben meghatározott feladatainak végrehajtása céljából nyilvántartja és kezeli az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó személy, szervezet azonosítására alkalmas adatokat, valamint a feladatot ténylegesen ellátó természetes személy személyazonosító adatait, közvetlen elérhetőséget biztosító telefonszámát, elektronikus elérhetőségét, végzettségét, szakképzettségét, szakmai tapasztalatát, a hatóság számára be kell jelenteni a nyilvántartásba vett adatokban történt változást.

1.3. Információbiztonságot érintő erőforrások

A Hivatal biztosítja az információbiztonsági célok, jelen szabályzat és az információbiztonsági intézkedési terv végrehajtásához szükséges forrásokat, mely magában foglalja a szükséges anyagi források biztosítását, valamint a szükséges személyi és technikai erőforrások biztosítását. A jegyző az éves költségvetés tervezése során az elektronikus információs rendszer védelmének biztosítása érdekében - a Kiberbiztonsági tv. 6. § (5) bekezdés i) pontja alapján - gondoskodik arról, hogy a szervezet által az adott évben informatikai fejlesztésre fordított költségek legalább 5%-ának megfelelő összeget a szervezet a tárgyév során kiberbiztonsági fejlesztésekre fordítson.

A biztonságért Felelős feladata arról gondoskodni, hogy az információbiztonsági dokumentumok összhangban legyenek a hatályos törvényekkel, végrehajtási rendeletekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.

1.4. Intézkedési terv és mérföldkövei

A Hivatal megfelelő és arányos technikai, operatív és szervezési intézkedéseket hoz annak érdekében, hogy kezelje azokat a kockázatokat, amely a működése, a közfeladatai teljesítése során használt hálózati és információs rendszerek biztonságát fenyegeti, és megelőzze vagy minimalizálja az eseményeknek az ügyfelekre és más szolgáltatásokra gyakorolt hatásait. Biztosítja a hálózati és információs rendszerek biztonságának a felmerülő kockázatoknak megfelelő szintjét. Az intézkedések arányosságának értékelésekor megfelelően figyelembe veszi a kockázatoknak való kitettség mértékét, a Hivatal méretét és az események előfordulásának valószínűségét, valamint azok súlyosságát, beleértve társadalmi és gazdasági hatásukat is.

Ha a biztonsági hibák, hiányosságok, kockázatok, sérülékenységek javítására hozott javító intézkedések nem kerültek azonnal végrehajtásra, Információbiztonsági intézkedési tervet kell készíteni:

a) Az informatikai rendszerek meghatározott biztonsági osztályba alapján megállapított hiányosságok megszüntetésére; Ha a Hivatal nem teljesíti legalább az „alap" biztonsági osztályba tartozó védelmi követelményeket, hiányosságot állapít meg, ha nem tolerálható kockázat, biztonsági hiba került meghatározásra, ha valamely védelmi intézkedés nem valósul meg vagy a bevezetett kontroll hibás akkor a meg a Kiberbiztonsági törvényben meghatározott határidőkkel Intézkedési tervet készít és ezekhez határidőket rendel.
b) A kockázatelemzés során feltárt, nem tolerálható kockázatok kezelésére; A Hivatal az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó szervezeti elektronikus információs rendszerek intézkedési tervei kidolgozása és karbantartása során a 1.10.1. Kockázatelemzési és kockázatkezelési eljárásrendben leírtakat alkalmazza. A Kockázatfelmérésben vagy egyéb dokumentumban (pl. Intézkedési tervben) rögzíteni kell a megvalósítandó intézkedéseket és feladatokat, a feladathoz rendelt felelősöket, valamint a végrehajtási határidőket.
c) Biztonságértékelések és külső biztonsági auditok során feltárt biztonsági hibák javítására;
d) A biztonsági képességek csökkenése esetén a korrekciós intézkedésekhez;
e) A sérülékenységvizsgálatok során feltárt sérülékenységek megszüntetésére vagy kockázatuk csökkentésére;
f) A bejelentett vagy a biztonsági események vizsgálata, illetve jelen szabályzat betartásának ellenőrzése során feltárt biztonsági hibák javítására.

A tervben rögzíteni kell a megvalósítandó intézkedéseket, a feladatok mellé rendelt felelőst és a feladatok végrehajtásának határidejét. A tervet a biztonságért Felelős javaslatai alapján a jegyző irányításával a rendszergazdának és a saját szakterületükre vonatkozóan az adatgazdáknak kell kidolgozniuk a biztonsági kockázatok, hibák vagy hiányosságok feltárását követően 90 napon belül.

Az Intézkedési tervet a jegyző hagyja jóvá, feladata biztosítani, hogy az Intézkedési tervben meghatározott intézkedéseket bevezesse, az azokhoz szükséges erőforrásokról gondoskodjon. Mivel az Intézkedési terv bizalmas információkat tartalmaz, ezért ezt csak a jegyző, a biztonságért Felelős, és az általuk kijelölt személyek, valamint az ellenőrzésre jogosult hatóságok ismerhetik meg.

Az Intézkedési tervet az információbiztonsági rendszer felülvizsgálata során (belső audit) szükség szerinti, legalább éves gyakorisággal felül kell vizsgálni és a változásoknak megfelelően karban kell tartani.

1.5. Elektronikus információs rendszerek nyilvántartása

A Hivatal a biztonságért Felelős közreműködésével gondoskodik az általa használt elektronikus információs rendszerek, központi szolgáltatások felméréséről, nyilvántartásba vételéről és a kiberbiztonsági hatóság felé történő adatszolgáltatásról.

Az elektronikus információs rendszerek nyilvántartása az alábbi bontásban készül:

a) **A Hivatal rendelkezésében lévő elektronikus információs rendszerek, beleértve a támogató rendszereket is** - azon rendszerek, amelyek felett a Hivatal rendelkezik, a rendszerek védelméhez kapcsolódó követelményeket maga határozza meg és gondoskodik azok alkalmazásáról); Ezekre vonatkozóan NBSZ-OVI űrlapot kell kitölteni és rendszerek hatósági nyilvántartásba vételét Elektronikus információs rendszerek biztonsági osztályba sorolása kérelemben kérelmezni kell.

Más szervezet rendelkezésében lévő elektronikus információs rendszerek, amelyeket a Hivatal feladatai ellátásához igénybe vesz, használ, a rendszerek védelméhez kapcsolódó követelményeket nem maga határozza meg, azokat kötelezően betartja:

b) **Központi rendszerek** – az egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszerek, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek.

   A központi rendszer felett a rendelkezési jogot a központi rendszer szolgáltatója gyakorolja; A központi rendszerek azonosítására alkalmas adatokat, valamint a központi rendszerek felett rendelkezési jogot gyakorló szervezetek megnevezését az EIR nyilvántartás tartalmazza. A rendszerek hatósági nyilvántartásba vételét Elektronikus információs rendszerek biztonsági osztályba sorolása kérelemben kérelmezni kell.

c) **Központi szolgáltatások és támogató rendszerek**; az állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal informatikai és elektronikus hírközlési szolgáltatást nyújtó ún. központi szolgáltató által biztosított - jogszabályi kötelezés vagy egyedi megállapodás alapján igénybe vett - szolgáltatások (a rendszer alapműködési céljához kapcsolódó IT funkciók összessége) és **támogató rendszerek** (az alapfeladatok ellátásában közvetlenül nem részt vevő elektronikus információs rendszerek, amelyek szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el);

   A központi szolgáltatások és támogató rendszerek azonosítására alkalmas adatokat, valamint a központi szolgáltatások, illetve támogató rendszerek felett rendelkezési jogot gyakorló szervezetek megnevezését az EIR nyilvántartás tartalmazza. Ezekre vonatkozóan NBSZ-OVI űrlapot kell kitölteni és a központi szolgáltatásokat, támogató rendszerek hatósági nyilvántartásba vételét Elektronikus információs rendszerek biztonsági osztályba sorolása kérelemben kérelmezni kell.

A Hivatalnak a központi rendszer felett rendelkezési jogot gyakorló szervezet által meghatározott elektronikus információbiztonsági követelményeket teljesítenie kell. Központi szolgáltató által nyújtott szolgáltatást vagy támogató rendszert jogszabályi kötelezés vagy egyedi megállapodás alapján vesz igénybe. A központi szolgáltató tájékoztatást köteles adni arról, hogy az általa nyújtott szolgáltatás milyen biztonsági osztály követelményeinek megfelelő szolgáltatásokat tud nyújtani. A szolgáltatás egyedi megállapodás alapján akkor vehető igénybe, ha a Hivatal elektronikus információs rendszere biztonsági osztályának megfelelnek a központi szolgáltató által biztosított védelmi intézkedések.

Támogató rendszernek azon rendszerek minősülnek, amelyek elsődleges célja az ügyviteli, üzleti adatok kezelését végző rendszerek üzembiztos, biztonságos működésének támogatása. Az alkalmazandó biztonsági kontrollokat a támogató rendszer funkcionalitása, valamint a benne kezelt adatok, valamint a támogatott elektronikus információs rendszer biztonsági igényei alapján szükséges meghatározni. Ezen rendszer nem önálló adatkezelési cél érdekében jön létre, hanem azt támogatja. Az alkalmazandó biztonsági kontrollokat a támogató rendszer funkcionalitása, valamint a benne kezelt adatok, valamint a támogatott elektronikus információs rendszer biztonsági igényei alapján kell meghatározni, gondoskodni kell arról, hogy a támogató rendszer is az általa támogatott elektronikus információs rendszernek megfelelő szintű védelemben részesüljön, ha az adott védelmi intézkedések kockázatarányosan alkalmazhatók az érintett támogató rendszer vonatkozásában.

A Hivatal az EIR nyilvántartást egy korlátozottan, csak az érintetteknek hozzáférhető belső elektronikus nyilvántartásban kezeli.

A biztonságért Felelős felelőssége, hogy felmérje és nyilvántartásba vegye a Hivatal informatikai rendszereit, az adatgazdák felelőssége, hogy a felügyelt rendszerek adatait a nyilvántartásba feltöltsék, azokat folyamatosan naprakészen tartsák vagy a biztonságért Felelős számára biztosítsák és legalább kétévente felülvizsgálják.

Az elektronikus EIR nyilvántartás tartalmazza:

1) a rendszer és modulja(i) / alrendszer(ei) megnevezése;
2) a rendszer állapota (tervezett, üzemelő, archív, megszűnt);
3) a rendszer rövid leírása (alapfeladat, biztosítandó szolgáltatások);
4) a rendszerben kezelt adatok;
5) a Hivatal rendelkezésében lévő elektronikus információs rendszerek biztonsági osztálya;
6) a Hivatal rendelkezésében lévő elektronikus információs rendszerek bizalmasság, sértetlenség és rendelkezésre állás szerinti besorolása, az adatosztályozás eredménye;
7) a központi rendszer megnevezése, a rendszer felett rendelkezési jogot gyakorló szervezet megnevezése;
8) a központi szolgáltatás, támogató rendszer megnevezése, a rendszer felett rendelkezési jogot gyakorló szervezet megnevezése;
9) az adatgazdai terület neve/ az adatgazda neve és elérhetősége;
10) az adatgazdai terület részéről a rendszerben kezelt adatokért felelős kulcsfelhasználó neve, elérhetősége.

Az 1. melléklet Elektronikus információs rendszerek nyilvántartása, jegyzői nyilatkozat az 1) - 8) pontokban szereplő főbb adatokat tartalmazza, mely a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet felé szükséges, Elektronikus információs rendszerek biztonsági osztályba sorolása kérelemhez és az NBSZ-OVI űrlapokhoz tartozó adatszolgáltatás része. Az elektronikus EIR nyilvántartást és az 1. melléklet Elektronikus információs rendszerek nyilvántartását az információbiztonsági rendszer felülvizsgálata során (belső audit) éves gyakorisággal a biztonságért Felelősnek felül kell vizsgálni, új rendszer bevezetése, meglévő rendszer kivezetése esetén soron kívül frissíteni kell, vezetését a biztonságért Felelős a Biztonságértékelési terv keretein belül is ellenőrzi (5.2. Biztonsági értékelések).

1.6. Biztonsági teljesítmény mérése

A jegyző a biztonságért Felelőssel és a rendszergazdával közösen meghatározta az elektronikus információs rendszerek biztonsági mérésének rendszerét. A Hivatal az alábbi mérőszámokat határozta meg, melyeket két felülvizsgálat során eltelt összehasonlítható időszakra (egy évre) vonatkozóan mérni szükséges:

Mérőszám	Mérés célja	Mérőszám meghatározása	Elérendő cél
Biztonsági hibák száma	Annak megállapítása, hogy az informatikai rendszerek védelmi intézkedései mennyire megfelelőek	Az adott időszakban megállapított biztonsági hibák száma	Mérőszám < 5
Sérülékenységek száma	Annak megállapítása, hogy az informatikai rendszerek mennyire sérülékenyek.	Az adott időszakban megállapított sérülékenységek száma	Mérőszám < 5
Biztonsági események száma	Annak megállapítása, hogy a biztonsági események mennyire veszélyeztetik az informatikai rendszerek működését	Az adott időszakban megállapított biztonsági hibák száma	Mérőszám < 5

A Hivatal a rendelkezésében lévő elektronikus információs rendszerei tervezésekor a Rendszerbiztonsági tervben is meghatározhatja és nyomon követi a figyelemmel kísért teljesítménymutatókat.

A biztonságért Felelős és a rendszergazda a Biztonsági teljesítmény értékelés során további teljesítmény-mutatókat is meghatározhat. Ha rendelkezésre állnak a kiberbiztonsági hatóság által az Automatizált Sebezhetőségdetektáló Rendszer (ASR) használatával végzett, a jogosultság nélkül elérhető (black-box) szolgáltatások sérülékenységeinek feltárására irányuló sérülékenységvizsgálatok eredményei, jelentései, akkor figyelemmel kell kísérni, hogy az éves felülvizsgálatok közötti időben hány sérülékenység került meghatározásra, azok milyen arányban kerültek javításra az előző időszakhoz képest. A vizsgálat önkéntes, vezetői döntés alapján

havi gyakorisággal történik a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Automatizált Sebezhetőségdetektáló Rendszere által lefuttatott tesztek alapján.

A felügyelt teljesítménymutatók vizsgálata és kiértékelése része az Információbiztonsági rendszer felülvizsgálata során (belső audit) készített legalább éves felülvizsgálati jelentésnek. A Biztonsági teljesítmény értékelésről a jegyzőt tájékoztatni kell.

1.7. Szervezeti architektúra

A Hivatal olyan vállalati architektúrával rendelkezik, amely integráltan kezeli a biztonsági követelményeket és kockázatokat, ezáltal támogatva a meghatározott célok elérését.

A feltárt kockázatok kezelése és dokumentálása a Kockázatelemzésben, a jogszabályi követelmények teljesítésében feltárt hiányosságok, a potenciális veszélyek az Intézkedési tervben kerülnek meghatározásra.

1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

A Hivatal a működése szempontjából kritikus infrastruktúraként a rendelkezésében lévő elektronikus információs rendszereket, azok alrendszereit kezeli, melyeket az Informatikai üzletmenet-folytonossági terv alapján magas vagy kritikus helyreállítási prioritásúnak minősített, ezekre vonatkozóan a 13.2. Rendszerbiztonsági terv pont szerint Rendszerbiztonsági tervet készít.

1.10. Kockázatmenedzsment stratégia

A Hivatal kockázatmenedzsment stratégiája magában foglalja a kockázatelemzés módszertanát, a kockázat-tűrés meghatározását és a kockázatok kezelésének módját. Az elektronikus információs rendszerek információbiztonsági kockázatelemzését, a védelmi intézkedések hatékonyságának folyamatos ellenőrzésére vonatkozó biztonságfelügyeleti stratégiát az 1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend alapján, a lehetséges kockázatok felmérése érdekében az éves felülvizsgálathoz kapcsolódóan működtetjük.

A kockázatkezelésért felelős személy szerepét a jegyző vagy az általa kijelölt személy, a kockázati vezető személyét a jegyző által kijelölt, kijelölés hiányában a biztonságért Felelős tölti be az 1.20. Kockázatkezelésért felelős szerepkörök pontban foglaltak szerint.

A kockázatfelmérést, elemzést, kezelést a kockázati vezető koordinálja, ha nem a biztonságért Felelős van erre a feladatra kijelölve, akkor a Felelős bevonásával. A kockázati vezető irányításával, a rendszergazda és az adatgazdák bevonásával legalább éves gyakorisággal fel kell mérni az elektronikus információs rendszerek működésével, használatával összefüggő, a Hivatal működéséhez, vagyonelemeihez, a szervezethez köthető személyekhez és más szervezetekhez kapcsolódó, illetve a személyes adatok kezeléséből fakadó biztonsági kockázatokat, minimálisan az MK. rendelet, 3. sz. mellékletében felsorolt fenyegetésekre vonatkozóan.

Az adatgazdák a kockázati vezető segítségével azonosítják, felmérik, értékelik a szakterületükre vonatkozó kockázatokat, a saját területére vonatkozóan javaslatot tesznek a magas és kritikus kockázatok kezelésére. A kockázatelemzés során megismert eredményeket, az intézkedéshez javasolt feladatokat, felelősöket, határtűzidőket a kockázati vezető rögzíti és ismerteti meg a jegyzővel, aki jóváhagyja a kockázatelemzés eredményét.

Az eredmény alapján nem elfogadható kockázatokra az 1.4.Intézkedési terv és mérföldkövei pont szerint Intézkedési tervet kell készíteni. A kockázatkezelési Intézkedési tervet a jegyző (vagy ha kijelölt eltérő személyt, akkor a kockázatkezelésért felelős) jóváhagyását követően az abban foglalt ütemezés szerint, dokumentált módon kell végrehajtani. Az adatgazdák feladata intézkedni a saját hatáskörében kezelhető kockázatok csökkentésére, kezelésére, felelős a területére eső kockázatok figyelemmel kíséréséért, kezeléséért. A kockázatok változása, újak felmerülése esetén soron kívül is tájékoztatni kell a kockázatkezelésért felelőst. Bármilyen változás (fejlesztés, fenyegetések, sebezhetőségek) esetén, vagy a rendszerben vagy annak működési környezetében biztonsági hiányosság azonosítása esetén, a rendszer biztonsági állapotát befolyásoló körülmény felmerülése esetén ismételt kockázatelemzési tevékenységet kell végezni.

A kockázatelemzés eredményei és a kockázatkezelésre hozott intézkedések bizalmas információnak minősülnek ezért a hozzáférést korlátozni kell – a kockázatértékelés eredményeit, illetve az abból származó szükséges intézkedéseket az érintettek felé kommunikálni szükséges. A kockázatkezelésért felelős személy feladata biztosítani, hogy kockázatelemzési folyamat során keletkezett információk megosztásra kerüljenek az adatgazdákkal és az arra jogosultak egyéb személyekkel.

1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal a rendszerrel kapcsolatos fenyegetettségből adódó biztonsági kockázatok értékelését és kezelését kockázatkezelést kockázati mátrix módszerrel végzi, amely a kockázatokat valószínűség és a következmények (hatás) alapján csoportosítja. A kockázatok azonosítása és felmérése 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 mennyiségben sérülhetnek. Meg kell határozni az okok (sérülékenységek, fenyegetések) nyomán előforduló helyzet, esemény (kockázati esemény) hatásait, következményeit és ennek nagyságát.

Valószínűség: a rendelkezésre álló információk alapján a feltárt kockázatok bekövetkezésének valószínűsége:

	Megnevezés	Leírás
1	**Ritka** 1-5 % közötti valószínűség	- Valószínűtlen, de nem teljességgel kizárható. - Teljes körű, szabályozott és bizonyítottan működő kontrollrendszer.
2	**Nem valószínű** 6-15 % közötti valószínűség	- A bekövetkezés a közeljövőben nem valószínű, de reális lehetőség. - Főbb területekre kiterjedő, szabályozott és működő kontrollrendszer.
3	**Alkalmankénti** 16-25 % közötti valószínűség	- A bekövetkezés hosszabb távon valószínű. - Főbb területekre kiterjedő, formálisan nem, vagy csak részben szabályozott, esetlegesen működő kontrollrendszer.
4	**Valószínű** 26-50% közötti valószínűség	- A bekövetkezés már a közeljövőben is valószínű. - Informálisan, eseti jelleggel, elszigetelten működő egy-egy kontroll.
5	**Gyakori** 51 % feletti valószínűség	- Rendszeres (mindennapos) megvalósulás vagy annak folyamatosan nyitva álló lehetősége. - Kontrollfunkciók hiánya.

Hatás: a rendelkezésre álló információk alapján a feltárt kockázatok bekövetkezése esetén keletkező károk mértéke, (a bizalmasságot, sértetlenséget és rendelkezésre állást szem előtt tartva:

	Megnevezés	Leírás
1	**Nagyon kicsi**	Ezek a kockázatok elhanyagolható hatással vannak a Hivatalra és általában nem igényelnek speciális figyelmet. Ilyenek lehetnek a minimális rendszerhibák, apróbb szabályszegések vagy elhanyagolható adatvesztések.
2	**Kicsi**	Ezek a kockázatok csak minimális zavart okoznak a Hivatal számára, általában könnyen kezelhetők. Ide tartozhatnak az egyedi felhasználói hibák, kisebb rendszerintézkedések vagy alacsony szintű biztonsági sérülékenységek.
3	**Közepes**	Ezek a kockázatok kisebb mértékű zavart okozhatnak a Hivatal működésében, de továbbra is figyelmet igényelnek. Ilyenek lehetnek az adatvesztések kisebb esetei, részleges szolgáltatások leállása vagy kisebb jogi következmények.
4	**Magas**	Ezek a kockázatok komoly zavart okozhatnak a Hivatal tevékenységében és erőforrásainak kezelésében. Ide tartozhatnak a fontos rendszerek részleges megbénulása, érzékeny információk kiszivárgása vagy jelentős szabályozási problémák.
5	**Nagyon magas**	Ezek a kockázatok rendkívül jelentősek és meghatározóak lehetnek a Hivatal számára, komoly hatással a működésére és hosszú távú stratégiáira. Ilyen lehet például a kritikus infrastruktúra megbénítása, súlyos adatvesztés vagy hatalmas pénzügyi kár.

KOCKÁZATI ÉRTÉK: a valószínűség és a hatás szorzata, négy kockázati kategória került meghatározásra:

1) 1-8 kockázati érték: **Alacsony kockázati kategória** (zöld) - nem szükséges intézkedést meghatározni, a kockázat indoklás nélkül felvállalható
2) 9-14 kockázati érték: **Közepes kockázati kategória** (sárga) - a kockázati vezető / biztonságért Felelős javaslatot tesz, a kockázat felvállalása csak a kockázatkezelésért felelős indoklása mellett lehetséges

3) 15-19 kockázati érték: **Magas kockázati kategória** (narancs) - szükséges a kockázatkezelés, a kockázat felvállalása csak a kockázatkezelésért felelős indoklása és (ha eltérő személy, akkor) a Hivatal vezetőjének az egyedi jóváhagyása mellett lehetséges, kivételes, indokolt – pl. a szükséges erőforrások hiánya – esetekben lehetséges, ezekre vonatkozóan év közi figyelemmel kíséréssel is követni kell a kockázatok esetleges változását, indokolt esetben rendkívüli intézkedéseket is meg kell határozni
4) 20-25 kockázati érték: **Kritikus kockázati kategória** (piros) - kötelező azonnali intézkedéseket meghatározni, a kockázat felvállalása, kockázatcsökkentő intézkedés nélküli elfogadása nem lehetséges.

KOCKÁZATI ÉRTÉK: valószínűség x hatás 4 KOCKÁZATI KATEGÓRIA				HATÁS				
				Nagyon kicsi	Kicsi	Közepes	Magas	Nagyon magas
				1	2	3	4	5
VALÓSZÍNŰSÉG	Ritka	1-5%	1	1 alacsony	2 alacsony	3 alacsony	4 alacsony	5 alacsony
	Nem valószínű	6-15%	2	2 alacsony	4 alacsony	6 alacsony	8 alacsony	10 közepes
	Alkalmankénti	16-25%	3	3 alacsony	6 alacsony	9 közepes	12 közepes	15 magas
	Valószínű	26-50%	4	4 alacsony	8 alacsony	12 közepes	16 magas	20 kritikus
	Gyakori	50-100%	5	5 alacsony	10 közepes	15 magas	20 kritikus	25 kritikus

A Hivatal a feltárt kockázatokra a szükséges biztonsági intézkedések megvalósításával reagál. A biztonságért Felelős és az adatgazdák javaslatot tesznek a kockázatkezelési, javítási intézkedésekre. A Hivatal a kockázati érték meghatározását követően, az intézkedés költségének figyelembevételével rangsorolást végez, hogy a rendelkezésére álló erőforrásait minél hatékonyabban használhassa fel.

Tűréshatárként a 20-as kockázati érték került megállapításra, azokra a kockázatokra, amelyek elérik ezt az értéket, kötelező érvénnyel azonnali intézkedéseket kell eszközölni, szükséges a kockázat csökkentése, ezekre a fenyegetésekre vonatkozóan a kockázat elfogadása nem lehetséges.

A kockázatkezelés eszközei:

1) **Kockázat felvállalás** - a kockázat tudatos, a következmények felmérése alapján történő elfogadása, felvállalása: a Hivatal vállalja az adott kockázat bekövetkezésével járó veszélyeket, az ellen nem tesz védelmi intézkedést. Akkor alkalmazható, ha a kialakult működési rend olyan, hogy a napi működés során minden beavatkozás nélkül automatikusan lehet kezelni a kockázatot, nincs szükség külön beavatkozásra, ill. tudatos vezetői döntés esetén, ha a kockázat elhárításának költsége magasabb az elhárításból eredő haszonnál, vagy kezelése technikai, időbeli, vagy anyagi korlátba ütközik. Kizárólag alacsony kockázati kategória esetén lehetséges az indoklás nélküli felvállalás, magasabb (közepes vagy magas) kockázati kategória esetén a kockázatkezelésért felelős/jegyző indoklása és jóváhagyása mellett lehetséges. Kritikus kockázati kategóriájú kockázat felvállalására nincsen lehetőség.
2) **Kockázat csökkentés** védelmi intézkedések kialakításával és működtetésével - a fenyegetés bekövetkezési gyakorisága vagy hatása megfelelő védelmi intézkedésekkel történő kezelése, csökkentése: A meghozott intézkedésekkel csökkenteni szükséges a kockázat bekövetkezési esélyét és/vagy az általa okozott kár nagyságát, amivel a meghatározott tűréshatár alá csökkenthető a kockázati érték.
3) **Kockázat áthárítás** - a kockázat - biztosítással, beszállítói szerződésekkel stb. történő áthárítása vagy megosztása harmadik felekkel: csökkenthető a kár hatása, bekövetkezési valószínűsége, a kockázatviselő a Hivatalon kívülre kerül. Ilyen megállapodás esetén vizsgálandó, hogy a kockázati esemény bekövetkezése esetén milyen maradványkockázat marad az átadó szervezetnél (pl. reputáció-vesztés).
4) **Kockázat elkerülés** - a kockázatnak az érintett tevékenység felfüggesztése útján való elkerülése. Akkor alkalmazható, ha a kockázatok nem csökkenthetők elfogadható szintre, a tevékenység megszüntethető és megszüntetése nem akadályozza a Hivatallal szembeni követelmények teljesítését, csak megszüntethetők az adott tevékenység befejezésével. Pl. a jegyző az adott információs rendszer vagy annak elemének, funkciójának kivezetését rendeli el.

1.11. Engedélyezési folyamatok meghatározása

A Hivatal a Szerepkörök, tevékenységek, felelősségek fejezetben, valamint a Rendszerbiztonsági tervben határozta meg az információbiztonsággal összefüggő szerepköröket, tevékenységeket, felelősségeket.

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

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, a Hivatal hatókörébe tartozó emberi, fizikai és logikai erőforrásra, eljárási és védelmi szintre és folyamatra. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárást (a jogosultságok kiosztását és visszavonását) a 2.1. Hozzáférés-felügyeleti eljárásrend tartalmazza, illetve az engedélyezések a további védelmi intézkedések alatt kerülnek részletezésre.

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 a biztonságáért Felelős elé terjeszti, aki – a javaslatok mérlegelése és elfogadása után – átvezeti a módosításokat a dokumentumokon.

1.12. Szervezeti működés és üzleti folyamatok meghatározása

A Hivatal szervezeti céljaként elsősorban a közfeladatok ellátásával kapcsolatos jogszabályi előírások betartását, a hatékony és átlátható ügyintézést határozta meg. Feltérképezte folyamatait: az ügyfélkezelés, iratkezelés, pénzügyi műveletek és egyéb önkormányzati tevékenységek kapcsán figyelembe veszi az információbiztonságot, különös tekintettel a kockázatokra, amelyek érinthetik a működési folyamatok hatékonyságát, az eszközöket (informatikai rendszerek, infrastruktúra), az ügyintézők és ügyfelek biztonságát, más szervezetekkel való együttműködést. A szervezeti célokat és az üzleti folyamatokat évente egyszer vagy jelentős változások esetén (pl. jogszabályváltozás, szervezeti átalakulás) felülvizsgálja. A felülvizsgálat során elemzi: a szervezeti célok és üzleti folyamatok hatékonyságát, az információvédelmi követelmények megfelelőségét, a változó környezeti, üzleti és technológiai tényezők hatásait. Az eredmények alapján módosítja és frissíti a szabályzatot és az eljárásrendeket.

A célokból és folyamatokból adódó konkrét információvédelmi igényeket (javasolt védelmi eszközöket és megoldásokat) a kockázatelemzés folyamata szerint, a feltárt kockázatok alapján kell meghatározniuk a kockázatelemzést végzőknek.

1.14. Biztonsági személyzet képzése

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

A biztonságért Felelős a biztonsági személyzet képzése, fejlesztése, a felhasználók információbiztonsági ismereteinek biztosítása, szinten tartása céljából az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásához Oktatási tematikát, Információbiztonsági szabályzat kivonatot készít.

Az elektronikus információs rendszer védelmének biztosítása érdekében az elektronikus információs rendszerek védelmi feladatainak és az azokhoz kapcsolódó felelősségi köröknek az oktatásáról, saját maga és a szervezet munkatársainak kiberbiztonsági képzéséről, továbbképzéséről a jegyző gondoskodik.

Az informatikai rendszerek felhasználóit, a tervek végrehajtásában, a rendkívüli események észlelése és eszkalálási folyamatában érintett munkatársat oktatni szükséges évente legalább egyszer (releváns belépő munkatársat a munkakezdés előtt). A képzés, tudatosítás történhet e-mail tájékoztatás, dokumentum elosztás, valamint jelenléti, online és hibrid formában is.

A biztonságért Felelős, helyettes Felelős és a szervezet vezetője részt vesz a számára előírt tovább-képzéseken a Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szak-képzettségekre, valamint képzésekre és továbbképzésekre vonatkozó követelményekről szóló rendeletnek megfelelően.

1.15. Tesztelés, képzés és felügyelet

A Hivatal nem kötelezett külső szakértővel végzendő biztonsági tesztelésre, jogszabályi kötelezésnek megfelelően szükség esetén a rendelkezésében lévő informatikai rendszereire vonatkozóan biztonsági teszteket végez vagy végeztet. A teszteket a rendszerek bevezetése előtt, illetve azokban történt fejlesztések, változások vagy jelentős frissítések bekövetkezése esetén ismételten el kell végezni. A külső, interneten elérhető szolgáltatások tekintetében (pl. levelezés, weboldal), a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet sérülékenységvizsgálati rendszere a Hivatal rendelkezésére áll.

A biztonságért Felelősnek a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események, valamint azok súlya alapján legalább évente, de kritikus kockázati besorolású biztonsági eseményt követően egy hónapon belül felül kell vizsgálnia. Az elkészült jelentés bizalmas dokumentum, amelyet csak a sérülékenységek kezelésében érintett személyekkel lehet megosztani.

1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás

A Hivatal kapcsolattartása szakmai csoportokkal a biztonságért Felelős segítségével, kommunikációjával valósul meg. A biztonságért Felelős olyan szakmai csoportoknak, levelezőlistáknak a tagja, amelyek információbiztonsággal kapcsolatos információkat osztanak meg. A témakörben megrendezett konferenciákat időről-időre figyelemmel kíséri (akár online térben) és az ott elhangzottakat beépíti az információbiztonsággal kapcsolatos eljárásokba, gyakorlatokba.

1.17. Fenyegetettség tudatosító program

A 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. Figyelemmel kíséri a kiadott tájékoztatókat, riasztásokat, a Hivatal informatikai rendszereit érintő események esetén értesti az érintetteket, megteszi a szükséges teendőket.

A Hatósági szerveken túl a biztonságért Felelős és a Hivatal kapcsolatot tart partnereivel (pl. vírusirtó szolgáltatójával) és egyéb szakemberrel (pl. más információbiztonsági felelőssel, rendszergazdával).

1.19. Kockázatmenedzsment keretrendszer

A Hivatal elektronikus információs rendszereinek információbiztonsági kockázatelemzését, a kockázatkezelést és a kockázatok felügyeletét az 1.10.1.Kockázatelemzési és kockázatkezelési eljárásrend alapján, legalább éves gyakorisággal végzi. Bármilyen változás (fejlesztés, fenyegetések, sebezhetőségek) esetén, vagy a rendszerben vagy annak működési környezetében biztonsági hiányosság azonosítása esetén, a rendszer biztonsági állapotát befolyásoló körülmény felmerülése esetén ismételt kockázatelemzési tevékenységet kell végezni. A biztonságért Felelős a kockázatelemzés során megismert eredményeket, az intézkedéshez szükséges feladatokat, felelősöket, határidőket, valamint maradék kockázatokat rögzíti és megismerteti a jegyzővel, a kockázatelemzés eredményét a jegyző hagyja jóvá. A kockázatmenedzsment keretrendszer szempontrendszerének felülvizsgálatát és frissítését az éves felülvizsgálatok alkalmával kell elvégezni.

1.20. Kockázatkezelésért felelős szerepkörök

A kockázatkezelésért felelős személy szerepét a Szervezet vezetője, a jegyző vagy az általa kijelölt személy tölti be. A kockázatkezelésért felelős személy biztosítja, aki összehangolja az információbiztonság irányítási folyamatait a stratégiai, működési és költségvetési tervezési folyamatokkal.

A kockázati vezető szerepét eltérő kijelölés hiányában a biztonságért Felelős tölti be. A kockázati vezető biztosítja, hogy a kockázatok a Hivatal egészére kiterjedő szemszögből kerüljenek áttekintésre és elemzésre, valamint azt, hogy a kockázatkezelés a Hivatalon belül egységes és következetes legyen.

1.21. Ellátási lánc kockázatmenedzsment stratégiája

A Hivatal információbiztonsági kockázatelemzését az 1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend tartalmazza. Ebben az eljárásrendben integráltan megtalálhatóak az ellátási láncra vonatkozó kockázatok, figyelembe véve az elektronikus információs rendszerek, rendszerelemek és rendszer-szolgáltatások fejlesztésével, beszerzésével, karbantartásával, selejtezésével kapcsolatos biztonsági kockázatokat.

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

A Hivatal a szervezeti céljainak, az ellátási láncnak a biztosításához szükséges kritikus technológiák, termékek és szolgáltatások beszállítóit azonosította, alapesetben a Hivatal által üzemeltetett informatikai rendszereket biztosító rendszerelemek sorolandók ide. Az elektronikus információs rendszerek alapfunkcióit támogató kritikus rendszerelemek azonosítása az üzletmenet-folytonossági tervben történik, felügyeletüket az adatgazdákkal közösen a jegyző látja el.

1.23. Folyamatos felügyeleti stratégia

A folyamatos felügyelet elősegíti, hogy a Hivatalnak folyamatos és valós képe legyen a szervezet biztonsági állapotáról, lehetőség szerint automatikus eszközök és szoftverek használatával (pl. naplóelemző szoftver, vírusirtó központi menedzser felügyelete) vagy manuális ellenőrzéssel (pl. jogosultságkezelés felülvizsgálata). A felügyeleti eredmények hozzájárulnak a védelmi intézkedések hatékonyságának mérésében.

A felügyelt teljesítménymutatók vizsgálata és kiértékelése része az Információbiztonsági rendszer felülvizsgálata során (belső audit) készített legalább éves felülvizsgálati jelentésnek, melyet a biztonságért Felelős készít a jegyző számára.

2. HOZZÁFÉRÉS-FELÜGYELET

2.1. Hozzáférés-felügyeleti eljárásrend

A jogosultságok hozzáférési lehetőséget jelentenek az informatikai rendszerekhez/rendszerelemekhez, a különböző jogosultsággal felruházott felhasználók különböző szinten használhatják a rendszerek funkcióit. Az informatikai rendszerekhez történő hozzáférések ellenőrzése érdekében jelen fejezetben meghatározott hozzáférés-felügyeleti eljárásrendet kell alkalmazni. Alapvetően biztosítani kell, hogy csak azon személyek juthassanak hozzáférési jogosultságokhoz, akik feladatuk teljesítéséhez a szükséges képesítéssel rendelkeznek, a vonatkozó hatályos törvényi, jogszabályi előírásoknak megfelelően.

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

A Hivatal informatikai rendszereihez kizárólag olyan felhasználó kaphat hozzáférést, akinek a munkájához szükséges az informatikai rendszer használata, és aki

a) a munkavégzéshez szükséges feltételekkel a 14.3. Személyek háttérellenőrzése fejezetnek megfelelően rendelkezik, megismerte jelen szabályzatot, a rá vonatkozó rendelkezéseket;
b) a Hivatal vagy önkormányzat munkavállalója;
c) informatikai rendszerüzemeltetési szerződéssel rendelkező cég munkavállalója;
d) megbízási vagy vállalkozási szerződéses kapcsolatban álló magánszemély, egyéni vállalkozó vagy cég munkavállalója;
e) munkát vagy más tevékenységet folytató, érvényes szerződéssel rendelkező hallgató, gyakornok.

Csak valós, aktív munka- vagy szerződéses viszonyban álló személyeket lehet regisztrálni a rendszerekben. A jogosultságok kezelésekor alapelvként kell érvényesíteni, hogy csak a felhasználók feladatellátásához szükséges és elégséges mértékű jogosultságok biztosíthatók.

A szükséges hozzáférési jogok azon feladatokból és tevékenységekből adódnak, amelyeket a dolgozók a hivatali munkájukon belül ellátnak. A mindenkori feladatkörhöz szükséges jogosultságokat a jogosultság kiadásért felelősnek kell kidolgoznia, szerepkörben (munkaköri leírásban) összefoglalnia és dokumentálnia. Ennek során biztosítani kell, hogy különböző dolgozók azonos nemű jogai csoportosításra kerüljenek és azt, hogy ezen csoportosításhoz közös szerepkör kerüljön meghatározásra.

Az elektronikus információs rendszerekhez való bárminemű hozzáférést megelőzően a felhasználónak meg kell ismernie a rá vonatkozó informatikai biztonsági követelményeket, a tudomásul vételről megismerési nyilatkozatot, valamint titoktartási nyilatkozatot kell aláírnia.

A felhasználói fiókok igénylésére, létrehozására, módosítására és törlésére alkalmas eljárás minden esetben engedélyezési folyamatot tesz szükségessé. Ennek az engedélyezési folyamatnak mindenkor nyomon követhetően dokumentáltnak kell lennie oly módon, hogy vizsgálat esetén rövid időn belül és hiánytalanul igazolásokat lehessen felmutatni. Az új hozzáféréseket dokumentáltan kell igényelni és engedélyeznie az adatgazdának/jegyzőnek, pl. a Változás/igénybejelentő lapon vagy egyéb dokumentumban.

A felhasználói fiókok kezelése a rendszergazda felelősségi köréhez tartozik. Felhasználói fiókot csak olyan személyek részére szabad kiadni, akik elfogadják a Hivatal biztonsági szabályait. Az elfogadást írásos úton kell megadni és annak nyomon követően dokumentáltnak kell lennie (aláírt Titoktartási és megismerési nyilatkozat), amely külsős felek esetén a szerződés részét képezheti.

A törlés a szükséges mentéseket követően csak akkor megengedett, ha a működés szempontjából lényeges és megőrzés-köteles adatok ezzel nem mennek veszendőbe és ellenőrzési követelmények ezeket nem tiltják.

2.1.1. Felhasználói fiókok létrehozása, felülvizsgálata, megszüntetése

Jogosultsági csoportok használatáról a Hivatal felhasználói létszámától, szervezeti felépítésétől és egyéb sajátosságától függően a jegyző dönt. Jogosultságcsoportok használata esetén azokat olyan szemlélettel kell kialakítani, hogy megfeleltethető legyen a felhasználók munkaköri feladatellátásának, az informatikai rendszerekben betöltött feladatköröknek. A csoportok kialakítása során biztosítani kell, hogy a csoport csak a feladatkör ellátásához szükséges és elégséges jogosultságokat tartalmazza. A jogosultsági csoportok listáját és a csoportok leírását elektronikus formában a felhasználók rendelkezésére kell bocsátani segítségképpen a hozzáférési jogosultságok (jogosultsági csoportok) igényléséhez.

A jogosultságok kezelésénél érvényesíteni kell, hogy a szoftverek menüpontjaihoz/funkcióihoz, illetve a fájlrendszer mappáihoz/fájljaihoz kapcsolódó elemi jogosultságokat nem közvetlenül kell egy-egy felhasználóhoz kell rendelni, hanem ezekből az elemi jogosultságokból jogosultsági csoportokat kell képezni és a csoportok tagjai közé kell a felhasználókat felvenni. A jogosultsági csoportok alkalmazása áttekinthetőbbé teszi a jogosultságok rendszerét és leegyszerűsíti a hozzáférési jogok igénylését és kiadását (nagyszámú elemi jogosultság helyett, kevesebb jogosultság csoporttal kell foglalkozni). A jogosultsági csoportok elvét egy felhasználó tagú csoport esetén is érvényesíteni lehet, ez alól funkciójuknál fogva kivételt képeznek a felhasználók személyes használatára létrehozott mappái (a felhasználók „home" mappája).

A közvetlen (vagy felettes) munkahelyi vezetők (adatgazdák) feladata, hogy a beosztott munkavállalóikra vonatkozóan megkérjék azokat a hozzáférési jogosultságokat, amelyek az informatikai rendszerek használatához kapcsolódóan a feladatellátáshoz szükségesek. A beosztott munkatársak feladatkörében vagy az informatikai rendszerben bekövetkező változások esetén felül kell vizsgálniuk a hozzáférési jogosultságokat és kezdeményezniük kell a szükségtelen jogosultságok visszavonását, illetve új jogosultságok kiadását.

Az Android és iOS alapú mobil eszközökön (pl. mobiltelefon, PDA, táblagép) az operációs rendszer alapszolgáltatásainak működéséhez regisztrálni kell egy felhasználói fiókot (Google, illetve Apple fiókot). Az alapszolgáltatások működése, így különösen a biztonsági frissítések és az alkalmazások letöltési lehetősége érdekében a Hivatal megengedi, hogy a felhasználók maguk regisztráljanak egy ilyen fiókot és beállítsák azt a használatba kapott mobil eszközön. Ezeket a Google, illetve Apple fiókokat magáncélú fiókként kell tekinteni, mivel nem a Hivatal általi hivatalos előfizetésről, a Hivatal és az operációs rendszer készítője közötti szerződéses kapcsolatról van szó. A magáncélú eszközök használatának tilalma alóli kivitélként az Android és iOS alapú mobil eszközökön megengedett a magáncélú Google és Apple fiókok használata. Ugyanakkor a Google és Apple fiókokhoz tartozó elektronikus levelezési szolgáltatást tilos hivatalos ügyekben használni, illetve az eszközön Hivatali adatokat tárolni, mivel arról nem készül biztonsági mentés.

2.1.2. Új hozzáférés igénylése

A hozzáférési jogosultságokat az adatgazda engedélyezi a hatáskörébe tartozó elektronikus információs rendszerek, rendszerelemek, adatok, tevékenységek tekintetében. Hivatalon kívüli felhasználók esetén a jogosultság igénylést a külső felhasználó munkáját elrendelő adatgazda tölti ki.

Új belépők esetén a belépő szakterületvezetőjével/adatgazdával előzetesen egyeztetett, alapértelmezett hozzáférési jogosultságainak kiadása - azonos munkakörben dolgozó felhasználó alapértelmezett jogosultságai, felhasználó nevéből képzett e-mailcím, felhasználói fiók - egyszerűsített eljárással (űrlap kitöltése és adatgazdai engedélyezés nélkül) történik: ezeket a jogosultságokat a HR szervezet vagy adatgazda tájékoztatása alapján állítja be rendszergazda.

Az informatikai rendszerekhez való, alapértelmezetten felüli hozzáférési jogosultságok igénylését kizárólag írásban, az alábbi három módszer valamelyikével (továbbiakban az alkalmazott módszertől függetlenül: a jogosultság igény kitöltésével) kell kezdeményezni:

a) az erre a célra rendszeresített hozzáférés jogosultság igénylő űrlap kitöltésével;
b) nagy tömegű jogosultság igénylés esetén egyszerűsített, de minden részletezett adatot tartalmazó, egyéb jogosultság igénylő dokumentum kitöltésével;
c) a helyben szokásos módon, minimálisan a rendszergazdának írt e-mailben dokumentáltan

A jogosultság igénylésben az alábbi adatokat kell megadni:

a) a jogosultság alanyának (a beosztott munkatársnak vagy a külső felhasználónak) az adatait;
b) az informatikai rendszert (amelyhez a jogosultságot kérik);
c) az igényelt hozzáférési jogosultságot (a létező jogosultsági csoportok közül választva; vagy ha a létező csoportokkal nem fedhető le a jogosultság és új csoportot szükséges létrehozni, akkor szövegesen megfogalmazva; vagy egy másik, létező felhasználóval azonos jogosultságokat kérve);
d) a jogosultság igény indoklását (a feladatellátás megnevezését, amelyhez a jogosultság szükséges);
e) az időszakot, amelyre a jogosultságot biztosítani kell (ha nincs megadva jogosultság kezdete dátum, az a kiadás dátumától él, ha nincs jogosultság vége dátum, a jogosultság határozatlan időre szól).

A kitöltés után a jogosultság igénylést e-mail-ben meg kell küldeni a munkatársak önmagukra vonatkozó jogosultság igénylése esetén először a munkahelyi vezetőnek, aki változatlan vagy módosított jogosultságokkal engedélyezi, vagy indoklás mellett elutasítja az igénylést. Ezután a jóváhagyott jogosultság igénylést az igénylőnek e-mail-ben a rendszergazdához kell továbbítania.

Az igénylés ellenőrzésének folyamatában a rendszergazdának ellenőriznie kell a jogosultság igénylés előírásoknak való megfelelését és a jogosultság kiadhatóságát. Ha az igényelt jogosultság egyértelműen azonosítható és kiadható, megfelelő a munkahelyi vezető jóváhagyása, az igényelt jogosultság megfelel a fióktípusokra vonatkozó korlátozásoknak (rendszergazdai jogosultságot csak a rendszergazda kaphat), akkor a jogosultság kiosztható. Ha az igény nem egyértelmű, a jogosultság igénylést pontosíttatni kell az igénylővel és/vagy az adatgazdával.

A jogosultságok beállítását adott rendszertől függően a rendszergazda vagy a központi szolgáltató által kijelölt adminisztrátor végzi. Ha a jogosultság igénylés megfelel az előírásoknak, a rendszergazda a kért jogosultságokkal létrehozza a felhasználói fiókot. A felhasználó első belépést lehetővé tévő kezdeti jelszavát a jelszó kiválasztására vonatkozó szabályok betartásával véletlenszerűen kell generálni a kezdeti jelszavak kezelésére vonatkozó eljárás szerint (ld. 8.22.2. Kezdeti jelszavak kezelése). Ez követően a rendszergazda személyesen megadja, vagy a jogosultság igénylésben megadott, a felhasználó személyes használatában lévő e-mail címre és/vagy mobiltelefonra elküldi a belépéshez használatos felhasználói nevet és a kezdeti jelszót, és szükség esetén megadja az informatikai rendszer elérésére és használatára vonatkozó egyéb fontos adatokat.

A rendszergazda vagy a jegyző által kijelölt felelős a hozzáférési jogosultságok nyilvántartásában vezeti, hogy a felhasználó hozzáférési jogosultságot kapott az adott informatikai rendszerhez vagy rendszerelemhez. A nyilvántartásban nem kell a kiadott, részletes jogosultságokat manuálisan rögzíteni, azok megtalálhatók a jogosultság igénylésekben és az informatikai rendszerekben, és túlzott adminisztrációt jelentene a jogosultságok duplikált rögzítése. A jogosultság beállítását végző rendszergazdának a jogosultság igénylésen igazolnia kell a hozzáférési jogosultság kiadását, majd az igénylőt értesíteni kell a jogosultság beállításáról.

Ha az igénylés határozott idejű jogosultságról szólt, a jogosultság vége dátum is meghatározásra került, akkor a rendszergazdának a megadott dátumot követően gondoskodni kell a kiadott jogosultság visszavonásáról.

A kiadott jogosultságok engedélyezéséhez kapcsolódó feljegyzéseket meg kell őrizni.

2.1.3. Hozzáférési jogosultságok módosítása

A hozzáférési jogosultságok módosítása a meglévő felhasználói fiókok jogosultságának módosítására szolgál az alábbi esetekben:

a) A felhasználó belépése az adott feladatkörbe (pl. munkaviszony létesítése, szervezeti egység váltás vagy átszervezés következtében).
b) A felhasználó kilépése az adott feladatkörből (pl. nyugdíjba vonuláskor, szervezeti egység váltás vagy átszervezés következtében).
c) Változtatások a feladatkörben, amelyek következményeként változtatások válnak szükségessé a jogosultságokban, vagy amelyek következményeként jogosultságok kerülnek megszüntetésre.

Az adatgazdának kell valamennyi személyi változást és a jogosultságok ebből eredő változásait a rendszergazda felé a jogosultságok minél korábbi illesztése érdekében dokumentálni, közvetlenül lejelenteni. Ennek során főként azt kell biztosítani, hogy a már nem szükséges jogosultságok bevonásra kerüljenek, azaz amint azokra a mindenkori feladatkörön belüli teljesítéshez már nincs szükség.

A személyi változások vagy a jogosultságok megváltoztatási igénye esetén minden esetben az érintett felhasználó közvetlen felettesének jogosultság igénylő lapon vagy egyéb feljegyzésen történő írásos engedélye alapján lehet eljárni. Az igénylés folyamata megegyezik az Új hozzáférés igénylése pontban leírtakkal annyi eltéréssel, hogy a jogosultság kiadása nem jár új felhasználói azonosító és kezdeti jelszó létrehozásával, illetve a jogosultság beállításához kapcsolódóan nem kell módosítani a hozzáférési jogosultságok nyilvántartását (a nyilvántartásban nem kell manuálisan rögzíteni a részletes jogosultságokat).

2.1.4. Hozzáférés jogosultságok visszavonása

A hozzáférési jogosultságok visszavonása egy adott informatikai rendszerre nézve a felhasználó bizonyos jogosultságainak vagy minden jogosultságának a visszavonását, törlését jelenti.

A hozzáférési jogosultságok megszüntetéséről az alábbi esetekben szükséges intézkedni:

a) dolgozó kilépése esetén,
b) ha a felhasználót szervezeten belül áthelyezték,
c) ha a munkavállaló szervezeti egységen belül marad, de a munkaköre jelentősen megváltozott,
d) ha a külső partner szerződése lejárt vagy megszűnt,
e) tartós betegség, távollét, illetve helyettesítés esetén, a jegyző egyedi döntésére, aki az adatgazdával történő konzultációt követően hoz erről döntést, figyelembe véve a távollét várható idejét és a hozzáférési jog megtartása, visszavonása egyedi kockázatait
f) visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.

A foglalkoztatotti jogviszonyban álló személy jogviszonyának megszűnése, tartós távollét esetén a hozzáférési jogosultság megszüntetését a HR szervezet, más munkakörbe helyezés (szerepkörök vagy jogosultságok megváltozása) esetén a felelős adatgazda kezdeményezi, melyet a Változás/igénybejelentő lapon vagy egyéb módon dokumentál. A jogosultságok visszavonását adott rendszertől függően a rendszergazda vagy a központi szolgáltató által kijelölt adminisztrátor végzi.

2.1.5. Felhasználó letiltása/engedélyezése

A hozzáférési jogosultságok igénylésére rendszeresített űrlap vagy e-mailben történő dokumentálás szolgál egy adott felhasználó fiókjának letiltására vagy egy bármilyen okból (pl. inaktivitás miatt) letiltott felhasználói fiók újra engedélyezésére is. Az igénylés folyamata megegyezik az Új hozzáférés igénylése pontban leírtakkal annyi eltéréssel, hogy: a felhasználó letiltását és újra engedélyezését nem kell az adatgazdával engedélyeztetni, a felhasználó meglévő jogosultságai nem változnak, illetve a felhasználói fiók aktív / letiltott állapotának változását át kell vezetni a hozzáférési jogosultságok nyilvántartásán.

2.1.6. Jogviszony megszűnésekor szükséges általános követelmények

Jogviszony megszűnésekor a felelős adatgazda és a rendszergazda feladata, hogy:

a) megszünteti, vagy visszaveszi a személy egyéni hitelesítő eszközeit (valamennyi munkavállalónak, a szerződőknek és a felhasználó harmadik feleknek információkhoz és információ-feldolgozó eszközökhöz, informatikai rendszerekhez való hozzáférési jogosultságát, a megosztott mappák hozzáférési jogosultságát és a felhasználói fiókokat meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár);
b) tájékoztatja a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető a jogviszony megszűnése után is fennálló kötelezettségekről;
c) visszaveszi a Hivatal elektronikus információs rendszerével kapcsolatos, tulajdonát képező összes eszközt (valamennyi felhasználónak, a szerződőknek és a felhasználó harmadik félnek vissza kell szolgáltatnia a Hivatal valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik);
d) az eszköz leadásakor ellenőrizni kell, hogy a felhasználó a rögzített hardver-, szoftver-specifikációval adja-e vissza az eszközt;
e) megtartja a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és Hivatali információkhoz (a felhasználó elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott adatot menteni, archiválni kell az általa használt informatikai eszközről, szerver tárhelyről, illetve bármely egyéb adathordozóról, az archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve ha szükséges, a megadott idő után törölni a rendszerből);
f) az általa meghatározott módon a jogviszony megszűnéséről értesíti az általa meghatározott szerepköröket betöltő, feladatokat ellátó személyeket;
g) a jogviszonyt megszüntető személy elektronikus információs rendszerrel, vagy annak biztonságával kapcsolatos esetleges feladatainak ellátásáról a jogviszony megszűnését megelőzően gondoskodniuk kell az illetékeseknek;

h) a jogviszony megszűnésekor a jogviszonyt megszüntető személy esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását hatékony és gyors intézkedésekkel meg kell előzi.

A munkaviszony megváltozása esetén a felhasználó hozzáférését a belső rendszerekhez meg kell változtatni, a munkaviszony megváltozása esetén szükséges lépések:

a) Windows helyi-, Windows AD fiók csoporttagságainak aktualizálása.
b) A munkatárs által kezelt adatok hozzáférésének beállítása az adatgazda által kijelölt helyettes számára.
c) A használt számítógép átmozgatása szükség szerint.
d) Nem használt hálózati csatlakozás vagy végpontra való csatlakozás lehetőségének megszűntetése.

A munkaviszony megszűnése vagy végleges áthelyezés esetén a felhasználó hozzáférését a belső rendszerekhez meg kell szüntetni. A jogviszony megszűnésekor szükséges lépések:

a) Windows helyi-, Windows AD fiók megszüntetése.
b) A munkatárs által kezelt adatok hozzáférésének beállítása az adatgazda által kijelölt helyettes számára.
c) A nem használt számítógép elszállítása az erre a célra kijelölt tároló helyiségbe.
d) Nem használt hálózati csatlakozás vagy végpontra való csatlakozás lehetőségének megszűntetése.
e) Az ASP szakrendszerekben a felhasználói fiók fizikai törlése nem lehetséges, a fiók törlésével a felhasználó által elvégzett műveletek nem törlődnek. Amennyiben törlésre kerül egy felhasználó, a törlés után ugyanazzal a felhasználónévvel már nem lehet új felhasználót felvenni. A művelet elvégzése akkor javasolt, ha a felhasználó végérvényesen távozik, vagy helytelenül lett eredetileg rögzítve a felhasználóneve. A felhasználói hozzáférés megvonása a felhasználó zárolásával lehetséges: a zárolást követően a zárolt felhasználónak belépési kísérletét megtagadja a rendszer.

2.1.7. Tartós távollét esetén szükséges intézkedések

Tartós távollét alatt a 3 hónapot meghaladó távollétet értjük, függetlenül annak okától.
A munkatárs tartós távolléte esetén a hozzáférését a belső rendszerekhez szüneteltetni szükséges. A tartós távollét esetén szükséges lépések:

a) Windows helyi-, Windows AD, fiók inaktívvá tétele.
b) A nem használt számítógép elszállítása az erre a célra kijelölt tároló helyiségbe (adatgazda egyedi döntésére).
c) Nem használt hálózati csatlakozás vagy végpontra való csatlakozás lehetőségének megszűntetése.

Amennyiben a rendszerek támogatják a helyettesítések kezelését (pl. ASP), úgy nem a felhasználók közötti helyettesítésre, hanem a felhasználók által birtokolt szerepkörök közötti helyettesítésre kell helyezni a hangsúlyt. Ennek érdekében egy helyettesítés esetén nemcsak a helyettesíthető felhasználót szükséges megadni, hanem azt a szerepkört, szerepköröket, amelyekben a felhasználó helyettesíthető. Amennyiben a rendszer nem támogatja a helyettesítések kezelését, akkor tartós távollét esetén inaktiválni/zárolni vagy törölni kell a fiókot.

2.1.8. A szerepkörök és jogosultságok ellenőrzése

Valamennyi szerepkört és kiadott jogosultságot legalább évente egy alkalommal kell felülvizsgálni. Az adatgazdák kötelesek meggyőződni a meghonosított szerepkörök megfelelőségéről, a szerepkörök hozzá-rendelésének megfelelőségéről és a felhasználók járulékos egyéni jogosultságainak helyességéről. Az eltéréseket jelenteni kell az adatgazdának, akinek feladata a szükséges intézkedés meghatározása annak megszüntetésére (jogosultság dokumentált kiosztása, hozzáférés megszüntetése vagy intézkedés visszavonásra).

A rendszergazdának 3 havonta felül kell vizsgálnia a felhasználói fiókokat, és ellenőriznie kell, hogy minden kilépő munkavállaló hozzáférési jogosultsága megszüntetésre került-e. A felhasználói fiókok felülvizsgálata céljából a HR szervezetnek a rendszergazda számára kell bocsátani vagy elektronikusan hozzáférhetővé kell tenni az aktuálisan dolgozó és kilépett munkavállalók listáját. A hozzáférések kezelésének folyamatát és az előírások betartását, valamint az igényelt és a Hozzáférési jogosultság nyilvántartásában vezetett, illetve az informatikai rendszerben beállított jogosultságok egyezőségét a biztonságért Felelős a Biztonságértékelési tervben foglaltak szerint és szúrópróbaszerűen ellenőrzi.

A jogosultságok szúrópróbaszerű ellenőrzését a rendszergazda, illetve az adatgazda/jegyző és a biztonságáért Felelős végzi a rendszergazda bevonásával éves gyakorisággal. A szerepkörök és jogosultságok ellenőrzése része az éves felülvizsgálatok és karbantartások kötelező feladatainak. Az éves ellenőrzések során az adatgazdák feladata a használt felhasználó-azonosítók felülvizsgálata, évente annak ellenőrzése, hogy az valóban használatban van-e, és hogy az arra jogosult használja-e.

2.1.9. A jelszókezelés követelményei

Minden felhasználói fiókot jelszóval és/vagy PIN kóddal kell védeni az alábbi direktívák szerint (amennyiben ez az adott rendszerben kivitelezhető):

a) A jelszónak minden felhasználó számára bármikor szabadon megváltoztathatónak kell lennie.
b) Az azonosító és a hozzá tartozó jelszó soha nem kerülhet egyszerre dokumentumban, e-mailben kiküldésre.
c) A jelszó minimális hossza felhasználók esetében legalább 10 karakternek kell lennie.
d) A biztonságos jelszónak kisbetűt, nagybetűt, számot és speciális karakter kell tartalmaznia.
e) További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.
f) Ha a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie.
g) A jelszó ne legyen kívülálló számára kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat.
h) A jelszavakat nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen, gondoskodni kell a jelszó biztonságos helyen zárt borítékban történő tárolásáról.
i) A felhasználói munkaállomásokat úgy kell beállítani, hogy azok tétlenség esetén a hivatal által meghatározott időtartam letelte, maximum 30 perc után zárolják a munkaállomást, amit csak jelszóval lehessen feloldani.
j) Mielőtt az ügyintéző elhagyja a munkaállomást, zárolnia kell azt.
k) A munkaállomásokra való bejelentkezést úgy kell konfigurálni, hogy a felhasználóknak meg kelljen adni a felhasználónév jelszó párost (nem egy felhasználói listából kell kiválasztani a usert)
l) A felhasználónak a jelszavakat ne lehessen megváltoztatni 1 napon belül (jelszó min. élettartam 1 nap)
m) A jelszavakat ne tárolják visszafejthető titkosítással
n) A felhasználói jelszavakat kötelezően 90 naponként meg kell változtatni
o) Ne lehessen új jelszóként beállítani az utolsó 3 jelszót (előző jelszavak megőrzése)
p) Öt sikertelen felhasználói bejelentkezés esetén kerüljön zárolásra a felhasználói fiók minimálisan 30 percre (ld. 2.71. Sikertelen bejelentkezési kísérletek).

2.1.10. Fiókokkal és jogosultságokkal kapcsolatos incidensek kezelése

Valamennyi felhasználó kötelessége, hogy információbiztonsági incidens észlelése esetén – különösen a felhasználói fiók illetéktelen hozzáférésének gyanúja esetén – haladéktalanul jelentést tegyen a 9.27. A biztonsági események jelentése eljárása alapján.

2.2. Fiókkezelés

Felhasználói fiók alatt a felhasználó adott informatikai rendszerhez történő hozzáférését reprezentáló adatok összességét: a felhasználói azonosítót, a jelszót, a hozzáférési jogosultságokat és egyéb adatokat, illetve beállításokat értjük. Az adatgazdák/jegyző feladata meghatározni az elektronikus rendszerekben rendszerben engedélyezett felhasználókat, a csoport- és szerepkör tagságokat, tagsági feltételeket, kritériumokat, a felhasználói fiókok hozzáférési jogosultságait, a felhasználói fiókokhoz tartozó jellemzőket. Ők végzik a fiókok létrehozására irányuló kérelmek jóváhagyását.

A felhasználói fiókok kezelését, a munkacsoportokhoz/ szerepkörökhöz tartozó felhasználói feltételeket a rendszergazda vagy a központi szolgáltató által kijelölt adminisztrátor végzi az adatgazdák és/vagy a jegyző utasításainak megfelelően. A meghatározott jogosultságoknak megfelelően dokumentáltan kezelik az elektronikus információs rendszerhez hozzáférési jogosultsággal rendelkezők körét, a munkacsoporthoz/ szerepkörhöz tartozó jogosultságokat, valamint (szükség esetén) a felhasználói fiókok további jellemzőit. Létrehozzák, engedélyezik, módosítják, letiltják és eltávolítják a felhasználói fiókokat a Hivatal, valamint a központi szolgáltató által meghatározott feltételekkel összhangban.

A Hivatallal szerződéses jogviszonyban álló szereplők, a szerződésben meghatározott szerepkörökre kaphatnak jogosultságot. Kizárólag csak a 14.3. Személyek háttérellenőrzése követelményeinek teljesülése esetén lehet jogosultságot kiosztani. Hozzáférést csak a szükséges mértékben és időtartamra lehet engedélyezni, figyelembe véve a szerepkörhöz tartozó feladatokat. Tartományba léptetett eszközök esetén a fiókok automatikus tiltását maximum 5 rontott jelszó, illetve 12 hónap inaktivitást követően kell beállítani (ld. 8.14. Azonosító kezelés).

Kifejezetten tiltott fióktípus a megosztott és vendégfiók, egyedi engedélyezésüket a Rendszerbiztonsági tervben dokumentálni kell.

A rendszergazdát vagy a központi szolgáltató által kijelölt adminisztrátort az adatgazdáknak haladéktalanul, legkésőbb 5 munkanapon belül értesíti kell, ha:

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

A munkaállomásokon a felhasználóknak nem lehet adminisztrátori joguk. Ha az elektronikus információs rendszerek zavartalan működéséhez szükségesek az emelt szintű jogok, a rendszergazdai jogosultságot a rendszergazda javaslatára a jegyző engedélyezheti a szükséges ideig, kizárólag a szakrendszerek használatához, mely nem használható programok telepítésére, beállítások megváltoztatására.

Minden felhasználónak saját felhasználói azonosítóval kell rendelkeznie, az ehhez szükséges jelszavakat az alkalmazott jelszó szabályoknak megfelelően kell képezni. Az első bejelentkezést követően a felhasználóknak meg kell változtatniuk a jelszavukat, a jelszó szabályokat figyelembe véve. Tiltani kell a csoportos felhasználói azonosítók használatát. A több szerepkört betöltő személyek jogosultságai, a szerepköröknek megfelelően külön-külön kell, hogy kialakításra kerüljön.

A rendszergazda meghatározott gyakorisággal (a központi szolgáltató által kijelölt adminisztrátor a központi szolgáltató előírásai alapján), változások esetén, legalább évente felülvizsgálja a felhasználói fiókokat, hozzáféréseket, biztonsági beállításokat, ellenőrzi a fiókaktivitásokat, a fiókkezelési követelményekkel való összhangot, melyet munkalapon vagy egyéb feljegyzésben dokumentál.

Az informatikai rendszerekhez történő hozzáférés szempontjából a következő fióktípusok kerültek megkülönböztetésre:

a) felhasználói fiókok;
b) névre szóló rendszergazdai fiókok;
c) beépített rendszergazdai fiókok;
d) technikai felhasználói fiókok.

A felhasználói fióktípusba tartoznak az informatikai rendszerrel dolgozó, „normál" felhasználók fiókjai. Azonosításuk és hitelesítésük egyedileg, névre szólóan kell, hogy történjen. Jogosultságuk korlátozott, kizárólag az üzleti folyamatokhoz kapcsolódó feladataik elvégzéséhez szükséges jogosultságokkal rendelkezhetnek.

A névre szóló rendszergazdai fiókok az informatikai rendszerek felügyeletére, adminisztrálására (pl.: a rendszer paramétereinek karbantartására, hozzáférési jogosultságok kezelésére, a rendszer működésének felügyeletére, stb.) szolgálnak, amelyhez kiemelt jogosultságok biztosítása szükséges. A fióktípusba kizárólag a rendszergazda szerepkörben dolgozó munkatársak tartozhatnak, akiket egyedileg, névre szólóan kell azonosítani. Amennyiben a rendszergazda felhasználóként is használja a rendszert, úgy a felhasználói tevékenységet külön (nem kiemelt jogosultságú) felhasználói fiók alatt kell végeznie.

A beépített rendszergazdai fiókok alatt a szoftverek és hardver eszközök kiemelt jogosultságú, gyárilag beépített rendszergazdai fiókjait (pl.: admin, administrator, root, superuser, sa, stb.) értjük, amelyek segítségével a rendszerelem felügyelhető, adminisztrálható.

A beépített rendszergazdai fiókok közös használatú fiókoknak számítanak, ezért tilos a használatuk, helyettük a rendszerelemet felügyelő rendszergazdáknak névre szóló rendszergazdai fiókokat kell létrehozni. A beépített rendszergazdai fiókokat nem kell letiltani vagy törölni, mert biztonsági tartalék céljából szükség lehet rájuk.

Az előzőek alól kivételek azok a hardver eszközök (pl. hálózati eszközök), amelyek nem képesek egyedileg azonosítani a felhasználót. Mivel elkerülhetetlen, ezeknél a rendszerelemet felügyelő rendszergazda számára engedélyezett a beépített rendszergazdai fiók használata.

Technikai felhasználói fiókokról beszélünk, amikor egy felhasználói fiók nem személyhez kötődik, hanem egy szoftverhez, szolgáltatáshoz vagy hardver eszközhöz, amely belsőleg használja a fiókot valamely más rendszer szolgáltatásának eléréséhez (pl.: egy alkalmazói szoftver használja adatok tárolásához az adatbáziskezelő szerveren; vagy egy multifunkciós nyomtató szkennelt dokumentumok e-mail-ben történő küldéséhez; stb.). Ezek a fiókok nem igényelnek feltétlenül kiemelt, rendszergazdai jogosultságot, csak ami az adott feladat ellátásához szükséges. A technikai felhasználói fiókok a szoftverek/hardver eszközök belső működésére vannak fenntartva, személyek általi használatuk tilos! Ez alól kivételt képez a technikai felhasználói fiók tesztelése, ami engedélyezett az informatikai rendszer fejlesztői és üzemeltetői számára.

Tilos névre szóló felhasználói vagy rendszergazdai fiókokat technikai felhasználói fiókként használni, mert ha a fiók tulajdonosának jogosultsága megszüntetésre kerül, leáll az a szolgáltatás, amely az adott fiókra épül.

A beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelésére a 8.22.6. Beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelése eljárása vonatkozik. Valamennyi fióktípust a rendszergazdája kezeli (létrehozza, módosítja, megszünteti a fiókokat), viszont a névre szóló és a beépített rendszergazdai fiókok kezeléséhez a jegyző engedélyezése szükséges.

A Hivatal a közös munkavégzéséhez, a közösen használt fájlok, dokumentumok tárolására a kialakított közös hálózati mappákat biztosít a felhasználók részére.

A közös mappák kialakítására és használatára vonatkozóan az alábbiakat kell alkalmazni:

a) A közös mappákat szervezeti egységek (pl.: igazgatóságok, osztályok, csoportok) és közös feladatok (pl. projektek) szerint kell kialakítani.
b) A közös mappákhoz való hozzáférést jogosultságokkal kell szabályozni. A mappák és a jogosultságok kialakításával biztosítani kell, hogy a felhasználók csak a feladatellátásukhoz szükséges mappákhoz rendelkezzenek módosítás jogosultsággal.
c) A központi tárhely takarékos használata érdekében a közös mappákban csak a feltétlenül szükséges, és többek által használt dokumentumokat szabad tárolni. Magánjellegű fájlokat (pl.: fényképeket, zenéket, filmeket) a közös mappákban tárolni tilos!
d) Tilos a közös mappákban futtatható (pl.: .exe, .com kiterjesztésű) fájlokat tárolni és onnan a futtatni, mert egy vírusos munkaállomás a módosítási joga miatt ezeket a fájlokat megfertőzheti és a fertőzés könnyen továbbterjedhet a hálózaton. A fájl kiterjesztés szerint korlátozást a Hivatal technikai eszközökkel is érvényesítheti.
e) A közös mappák felhasználható mérete korlátozott. A korlátok eredményes betartása érdekében a nagyméretű fájlokra (pl.: videókra, fotókra) kell elsősorban figyelni, és a felhasználóknak rendszeresen törölniük kell a munkájukhoz tartozó, már elavult és szükségtelen fájlokat.

A hálózati hozzáféréssel együtt a Hivatal a felhasználók rendelkezésére bocsáthat egy mások által nem elérhető, saját használatú mappát, az ún. „home" mappát, melyek használatára az alábbiak vonatkoznak:

a) A home mappában helyezhetők el a felhasználók saját használatú, a munkavégzéssel kapcsolatos fájljai, dokumentumai, de rendszerektől függően ide kerülhetnek a felhasználói beállítások és a felhasználó által készített listák, lekérdezések is.
b) A home mappák felhasználható mérete korlátozott, ezért ha a korlát túllépésére vonatkozó figyelmeztetést kap a felhasználó, akkor törölnie kell a szükségtelen lekérdezésekből vagy az általa elhelyezett egyéb fájlokból olyan módon, hogy a mappa mérete ne haladja meg a korlátot.

Hivatali, üzleti dokumentumokat tilos mobil adattárolókon (pl. pendrive, külső merevlemez) és egyéb mobil eszközökön (pl. mobiltelefon, PDA, táblagép) tartósan tárolni, mert ezekről nem készül adatmentés. A munkához szükséges dokumentumokat a felhasználónak a számára a rendszergazda által kijelölt tárhelyre kell menteni.

A dokumentumokat elsődlegesen a fájl szerveren kialakított közös hálózati mappákban, a felhasználó saját „home" mappájában kell tárolni (ha elérhető).

2.15. Hozzáférési szabályok érvényesítése

A Hivatalnál csak olyan informatikai rendszer használható, amely képes a kiadott hozzáférési jogosultságokat érvényesíteni, azaz az informatikai rendszerben kezelt adatokhoz, a rendszerelemekhez csak a jogosultsággal rendelkezők férhetnek hozzá.

Az informatikai eszközök, berendezések vezetékes hálózatra való fizikai csatlakoztatását – ezzel összefüggésben az informatikai eszközök másik tárolóhelyre történő áthelyezését csak a rendszergazda végezheti, a csatlakoztatást, az áthelyezést tőle kell igényelni.

A mobil eszközök vezeték nélküli hálózati hozzáférésére 2.108. Vezeték nélküli hozzáférés pontban leírtakat kell alkalmazni. Nem a Hivatal tulajdonában lévő informatikai eszközöket, berendezéseket csatlakoztatni a Hivatal hálózatához -a vendégek számára fenntartott vezeték nélküli Internet hozzáférés kivételével - kizárólag a jegyző tudtával és engedélyével lehet.

2.71. Sikertelen bejelentkezési kísérletek

A Hivatal rendelkezésében lévő rendszerek azon vonatkozásában, melyeknél technikai lehetőség van az alkalmazásra, be kell állítani a fiókok automatikus tiltását maximum 5, egymást követő rontott jelszó megadását követően. A tiltás korlátozódhat egy előzetesen megállapított időre (minimálisan 30 perc fiókzárolás időtartamra), vagy amíg a rendszergazda, rendszer adminisztrátor azt fel nem oldja. Ha beállítható, akkor értesíteni szükséges a rendszergazdát, ha a sikertelen próbálkozások maximális számát túllépték.

Ha a Rendszerbiztonsági tervben nincsen eltérő rendelkezés, akkor az informatikai rendszereknek a következő fiókzárolási házirendet kell alkalmaznia sikertelen bejelentkezési kísérletek esetén:

Szabály megnevezése	Beállított érték	Magyarázat
Fiókzárolás küszöbe	5 sikertelen próbálkozás	A rendszer ennyi hibás jelszó megadása után zárolja a felhasználói fiókot és tagadja meg a rendszerbe történő bejelentkezést.
Fiókzárolás időtartama	30 perc	Ennyi ideig kerül zárolásra a felhasználói fiók.
Fiókzárolási számláló nullázása	30 perc	Ha ennyi percig nem történt sikertelen bejelentkezési kísérlet, a rendszer nullázza a sikertelen bejelentkezések számát.

2.75. A rendszerhasználat jelzése

A Hivatal rendelkezésében lévő azon rendszereknél, melyeknél technikai lehetőség van az alkalmazásra, rendszerhasználati értesítést kell megjeleníteni a képernyőn, ami felhívja a felhasználó figyelmét a Hivatal rendszerének használatára, a rendszerben végzett tevékenység megfigyelésére, rögzítésére, naplózására és arra, hogy a rendszerben végzett jogosulatlan tevékenységek büntető- vagy polgári jogi felelősséggel járnak. A rendszer használatával a felhasználó elfogadja a fenti feltételeket. Ha technikailag megoldható, a rendszer használatához a felhasználónak el is kell fogadnia a képernyőn megjelenő feltételeket, ennek hiányában nem léphet tovább, nem kezdheti meg a rendszer használatát.

Az elektronikus információs rendszerek használatára vonatkozóan általános, hogy a felhasználó tudomásulvételi vagy egyéb nyilatkozaton elfogadja a Hivatal által elvárt, Információbiztonsági szabályzatban rögzített kötelezettségeket, a rendszerbe történő bejelentkezéssel vállalja a betartását.

2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az azonosítás és hitelesítés nélkül végrehajtható felhasználói tevékenységeket dokumentálni kell, indokolni kell a Rendszerbiztonsági tervben, vagy más dokumentumban. A Hivatalban jelenleg nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek, a jelszavas vagy más hitelesítésnek ki kell terjednie a szerverekre, valamint minden hálózaton üzemelő és hálózattól független, egyedi munkaállomásra.

Kivételt képeznek – amennyiben vannak kihelyezve – a szervezeti információk megosztására kihelyezett azon munkaállomások, amelynek operációs rendszerébe bejelentkezéshez technikai felhasználói fiókok használhatók, vagyis nem szükséges egyedi felhasználói azonosítás. Az egyéb informatikai rendszerek (pl. e-learning rendszerű képzés) ezen munkaállomásokról történő hozzáféréséhez viszont már szükséges egyedi felhasználói azonosítás.

2.100. Távoli hozzáférés

Távoli hozzáférésnek minősül minden olyan hozzáférés, amelyben a kommunikáció külső, nem a Hivatal által ellenőrzött hálózaton, pl. Interneten zajlik. Ennek minősül a távoli asztal (Windows beépített távoli asztal kapcsolata, ill. a TeamViewer, AnyDesk), Virtuális magánhálózat (VPN), az FTP és az SSH hozzáférés.

A távoli hozzáférést a jogosultságokhoz hasonlóan engedélyezési eljárás előzi meg, a távoli hozzáférést alapesetben a 2.1. Hozzáférés-felügyeleti eljárásrend szerint kell igényelni. A hozzáférés csak a Hivatal vagy a szerződéses ügyfél, illetve partner kapcsolatban álló cégek tulajdonában lévő eszközökről engedélyezett.

Az informatikai rendszerekhez történő távoli hozzáférés alapesetben az otthoni munkavégzés szabályai szerint otthonról dolgozó felhasználók vagy azok számára biztosítható, akiknek a munkájuk megköveteli, hogy azt sokféle helyszínen, mobil eszközökkel végezzék. A felhasználói körre, a biztonsági előírásokra, a hozzáférés igénylésére és a használható eszközökre vonatkozóan az alapesettől való eltéréseket a jegyző engedélyezheti.

Távoli hozzáférés esetében minimális biztonsági követelmény, hogy a hitelesítés során használt jelszó a hálózaton titkosított formában kerüljön továbbításra, és amennyiben lehetséges a teljes adatforgalmat titkosítani kell (pl. VPN kapcsolattal). Privilegizált felhasználók esetén vagy a jegyző és/vagy a biztonságért Felelős által meghatározott esetekben korlátozni kell azon IP címek körét, ahonnan a távoli hozzáférés engedélyezett. Technikai lehetőség esetén a VPN hozzáférést úgy kell létrehozni, hogy csak a szükséges rendszerelemek legyenek elérhetők a távolról kapcsolódó számítógépekről.

A Hivatal előírásokat állapít meg a távoli hozzáférés biztonságos üzemeltetéséhez, így a távoli hozzáférésre használt eszközökkel kapcsolatban gondoskodni kell:

a) A távoli hozzáférésre használt eszközön gondoskodni kell az operációs rendszer és az egyéb használt szoftverek legújabb biztonsági frissítéseinek telepítéséről.
b) A távoli hozzáférésre használt eszközön naprakész, legalább naponta frissülő vírusadatbázissal rendelkező vírusvédelmi szoftverrel kell rendelkezni.
c) A használt eszközökön bekapcsolt tűzfalat kell alkalmazni.
d) A használt eszközökön a felhasználóknak rendszergazdai jog nem adható.
e) A használt eszköztől való távozáskor vagy a munka befejeztével a felhasználónak ki kell lépni a távolról elért informatikai rendszerekből, valamint a távoli elérést lehetővé tevő távoli asztal és/vagy VPN kapcsolatból.
f) A felhasználó nem teheti lehetővé mások számára – családtagok számára sem -, hogy a nevében a Hivatal informatikai rendszereiben tevékenykedjenek, illetve a rendszerekhez jogosulatlanul hozzáférjenek. Ennek érdekében mindent meg kell tennie a jelszavai titkosságának megőrzése érdekében, továbbá biztosítania szükséges, hogy a többtényezős hitelesítésre szolgáló személyi hitelesítő eszközeit más ne használhassa.
g) Tilos a távoli hozzáférésen keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni. Ennek keretében tilos pl. a rendelkezésre bocsátott dokumentumokat, adatokat idegen (pl. magántulajdonú) eszközre menteni!

A Hivatal távoli hozzáférésre az Internetet használja és az alábbi hozzáférés típusokat alkalmazhatja:

1) **Távoli asztal hozzáférés** – A kliens számítógép egy terminál szerverre csatlakozik és a szerver erőforrásait használja az alkalmazói szoftverek futtatására. A kliens számítógép csak a terminál szerver képernyőjét jeleníti meg és továbbítja a kliensen végzett billentyűzet és egér műveleteket a szervernek.

   A Hivatal távoli asztal hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett a rendszergazda szerepkörben dolgozó munkatársak számára rendszerüzemeltetés céljából, illetve indokolt esetben – az informatikai rendszerek adatgazdáinak engedélyével és a jegyző tudtával – az informatikai rendszerekhez támogatást nyújtó külső partnerek számára.

   A hozzáférés titkosított kapcsolaton keresztül kell, hogy megvalósuljon. Az Interneten keresztüli közvetlen távoli asztal hozzáférést lehetőség szerint kerülni kell, helyette ajánlott egy biztonságosabb VPN kapcsolaton keresztül elérhetővé tenni a távoli asztal szolgáltatást, vagy korlátozni azon IP címek körét, ahonnan a távoli asztal hozzáférés engedélyezett.

2) **Virtuális magánhálózati (VPN) hozzáférés** – egy nyilvános hálózat (pl. Internet) egyes végpontjai között kiépített logikai hálózat, amelyen keresztülmenő adatok nem láthatók az eredeti hálózaton, mivel titkosított adatcsomagokba vannak csomagolva.

   A Hivatal VPN hozzáférést biztosít az alapesetben engedélyezett felhasználók mellett a rendszergazda szerepkörben dolgozó munkatársak számára rendszerüzemeltetés céljából, közvetlen (optikai) adatkapcsolattal nem rendelkező telephelyek és a központi telephely Interneten keresztüli összekötésére (site-to-site VPN), ill. indokolt esetben – az informatikai rendszerek adatgazdáinak engedélyével és a jegyző tudtával – az informatikai rendszerekhez támogatást nyújtó külső partnerek számára.

   A VPN kapcsolat titkosított, így az adatok bizalmasságára nézve biztonságos, de a Hivatal hálózatához távolról kapcsolódó számítógép részévé válik a hálózatnak, és ezzel fenyegetést jelenthet a hálózatra nézve (pl. vírusfertőzést okozhat). A kockázatok csökkentése érdekében biztosítani kell, hogy csak a szükséges rendszerelemek legyenek elérhetők a távolról kapcsolódó számítógépekről, ill. a távoli hozzáférés esetében is ugyanazokat a munkaállomásokra vonatkozó biztonsági előírásokat kell betartani, mint a belső hálózatban használt számítógépek esetén (pl.: telepített biztonsági frissítések, naprakész vírusvédelmi szoftver, korlátozott felhasználói fiók, bekapcsolt tűzfal).

   A telephelyek közötti VPN kapcsolatok a telephely minden felhasználójára érvényesek, a hozzáférést nem kell külön igényelni. A hozzáférés csak asztali és hordozható számítógépekről engedélyezett, egyéb mobil eszközökről (mobiltelefon, PDA, táblagép) nem.

3) **A levelező rendszer mobil eszközről történő elérése** – A Hivatal a levelező rendszer felhasználói számára lehetővé teszi a rendszer a következő mobil eszközökről kliens programok segítségével történő távoli elérését hordozható számítógépekről (ehhez a levelező kliens program olyan módon kerül beállításra, hogy titkosított web-es (HTTPS) protokollal kapcsolódjon a levelező szerverre, és így nemcsak a hálózaton belülről, hanem Interneten keresztül is felépüljön a kapcsolat), valamint egyéb mobil eszközökről (mobiltelefon, PDA, táblagép).

   A hozzáférésre minden esetben titkosított kapcsolatot kell használni. A mobil eszközök levelező kliens programjának beállítása az e-mail postafiók igénylésének részeként történik, az eszközök utólagos beállítását a rendszergazdától kell igényelni. A hozzáférés csak a Hivatal tulajdonában lévő mobil eszközökről engedélyezett.

4) **A levelező rendszer web-es elérése** – A Hivatal web-es felületen keresztüli távoli hozzáférést biztosít a levelező rendszer felhasználói számára. A távoli hozzáférés titkosított (HTTPS) kapcsolaton keresztül kell megvalósítani. A levelező rendszer web-es elérése alapértelmezett része a postafiók használatának, a távoli hozzáférést nem kell külön igényelni.

5) **Egyéb web-es felületű rendszerek elérése** – A Hivatal indokolt esetben lehetővé teheti a web-es felületű informatikai rendszereinek távoli hozzáférését az alapesetben engedélyezett felhasználói kör számára. A távoli hozzáférés titkosított (HTTPS) kapcsolaton keresztül kell, hogy megvalósuljon, a hozzáférést az alapesetben érvényes módon kell igényelni.

6) **FTP hozzáférés** – Az FTP/FTPS protokollok fájlok hálózaton keresztüli cseréjét (le- és felöltését) teszik lehetővé, a protokoll nem támogat titkosított felhasználó azonosítást, ezért távoli hozzáférés esetén helyette a titkosítással kiegészített FTPS protokollt kell használni.

   A Hivatal FTP hozzáférést az alapesetben engedélyezett felhasználói kör számára biztosít és a hozzáférést az alapesetben érvényes módon kell igényelni.

2.108. Vezeték nélküli hozzáférés

A Hivatal a következőkben leírtak szerint elkülönített vezeték nélküli hozzáférést biztosíthat felhasználói és a vendégek számára telephelyeire vonatkozóan. Azokon az eszközökön, amelyeken önkormányzati ASP rendszer van használatban, vagy adat továbbítódik rá, nem engedélyezhető vezeték nélküli hozzáférés.

2.108.1. Alkalmazottak vezeték nélküli hozzáférése

Kizárólag az munkavállalók számára a Hivatal a belső hálózatra történő kapcsolódáshoz IEEE 802.11g/n szabványnak megfelelő (WiFi) vezeték nélküli hozzáférést biztosít a Hivatal tulajdonában levő mobil eszközökön. A belső hálózathoz való vezeték nélküli hozzáférés mobil eszközön történő beállítását a rendszergazdától kell igényelni.

A vezeték nélküli hozzáférésnél az alábbi módon kell gondoskodni az illetéktelen használat megelőzéséről:

a) A vezeték nélküli WiFi eszközön (hozzáférési ponton/routeren) WPA2 (vagy ha az eszköz támogatja WPA3) protokollt kell alkalmazni (a sok esetben alapértelmezett, bizonyítottan könnyen feltörhető WEP protokoll használata kifejezetten tilos).
b) A vezeték nélküli hozzáféréshez legalább 20 karakter hosszú, kisbetűt, nagybetűt, számot és speciális karaktert tartalmazó, a felhasználói jelszó kiválasztására vonatkozó szabályoknak megfelelő véletlenszerűen generált hozzáférési kulcsot kell beállítani.
c) A hozzáférési kulcsokat a rendszergazdának legalább kétévente meg kell változtatnia és Munkalapon vagy egyéb feljegyzésen kell dokumentálnia.
d) A hozzáférési kulcsokat a felhasználók nem ismerhetik, a kulcsokat a rendszergazda a beépített adminisztrátori jelszavakkal megegyező módon tárolja.
e) A kulcsok kezelésére a fenti eltéréssekkel a 8.22. A hitelesítésre szolgáló eszközök kezelése pontban szabályozott felhasználói jelszavakra vonatkozó előírások és biztonsági intézkedések vonatkoznak.
f) A közös használatú hozzáférési kulcsok helyett ajánlott nagyobb biztonságot nyújtó felhasználó szintű hitelesítési módot használni. Ebben az esetben értelemszerűen nem kell alkalmazni a hozzáférési kulcsok kezelésére vonatkozó fenti szabályokat.
g) A WiFi eszközön le kell tiltani a WiFi Protected Setup (WPS) használatát, amely a hozzáférési kulcs ismerete nélkül is lehetővé tenné az eszközökhöz való kapcsolódást.
h) A WiFi eszköz web-es adminisztrálási felületének eléréséhez tikosított (HTTPS) kapcsolatot kell alkalmazni.

2.108.2. Vendégek vezeték nélküli hozzáférése

A Hivatal a vendégei számára az Internet elérését 802.11g/n/ac/ax szabványnak megfelelő (WiFi) vezeték nélküli hozzáféréssel biztosítja. A vendégek Internet eléréséhez szükséges kulcsot a rendszergazdától kell igényelni. A hozzáférési kulcs a vendégek és munkavállalók számára megosztható (pl. az Intraneten). A munkavállalók és vendégek WiFi hozzáférésére vonatkozó védelmi intézkedések beállítása a rendszergazda feladata.

A vendégek biztonságos vezeték nélküli kapcsolódása érdekében a következőkről kell gondoskodni:

a) Külön a vendégek számára fenntartott, és a kapcsolódó eszközök számára láthatóvá tett (broadcast-olt) WiFi hálózati nevet (SSID) kell létrehozni.
b) A vendég WiFi forgalmát fizikai vagy VLAN (virtuális helyi hálózat) szeparációs technológia alkalmazásával el kell különíteni a belső hálózattól.
c) A WiFi eszközön WPA2 (vagy ha az eszköz támogatja WPA3) protokollt kell alkalmazni, a WEP protokoll használata kifejezetten tilos.
d) A vezeték nélküli hozzáféréshez legalább 12 karakter hosszú, kisbetűt, nagybetűt, számot és speciális karaktert tartalmazó, a felhasználói jelszó kiválasztására vonatkozó szabályoknak megfelelő hozzáférési kulcsot kell beállítani.
e) A WiFi eszközön le kell tiltani a WiFi Protected Setup (WPS) használatát.
f) A WiFi eszköz web-es adminisztrálási felületének eléréséhez tikosított (HTTPS) kapcsolatot kell alkalmazni.

2.113. Mobil eszközök hozzáférés-ellenőrzése

A Hivatal informatikai rendszereihez mobil eszközről történő hozzáférésnél a telephelyen belüli vezeték nélküli hozzáférés esetén az 2.108. Vezeték nélküli hozzáférés, az Interneten keresztüli távoli hozzáférés esetén az 2.100. Távoli hozzáférés pont rendelkezései szerint kell eljárni.

A vendégek számára biztosított vezeték nélküli Internet hozzáférés kivételével a hozzáférés csak a Hivatal tulajdonában lévő mobil eszközökről engedélyezett.

A mobil eszközök esetén nagyobb valószínűséggel fordulhat elő az eszköz elvesztése vagy eltulajdonítása. A kockázatok csökkentése érdekében az alábbiakról kell gondoskodni:

a) A hordozható számítógépeket felhasználói azonosítás nélkül használni tilos.
b) A hordozható számítógépek háttértárolóját titkosítani kell (pl. Windows operációs rendszer esetén a beépített BitLocker funkció használatával). A számítógép üzembe helyezési folyamatának részét kell képeznie a titkosítás beállításának.
c) A mobiltelefonokhoz, PDA-khoz, táblagépekhez való hozzáférést képernyő mintával, PIN kóddal (amely nem azonos a SIM kártya feloldásához alkalmazott PIN kóddal), vagy ujjlenyomattal kell védeni. Ennek beállítása az eszköz használójának a feladata, de a rendszergazdától segítség kérhető.
d) A mobiltelefonok, PDA-k, táblagépek elvesztése vagy eltulajdonítása esetén gondoskodni kell az eszköz tartalmának távolról történő törléséről, amennyiben az technológiailag lehetséges. Mivel a mobiltelefonok esetén a regisztrált és magán fióknak minősített bejelentkezésre is szükség lehet, ezért a munkavállalónak együttműködési kötelezettsége van a folyamat zökkenőmentes elvégzéséhez.
e) A mobil eszközök elvesztését vagy eltulajdonítását a 9.27. A biztonsági események jelentése pont szerint kell jelenteni.

2.115. Külső elektronikus információs rendszerek használata

A Hivatal belső informatikai rendszereinek külső rendszerből, pl. a Hivatalon/önkormányzaton kívüli, idegen hálózatból történő hozzáférése a 2.100. Távoli hozzáférés pontban meghatározott információbiztonsági előírások betartása mellett engedélyezett a felhasználók számára.

Tilos a külső rendszerből hozzáfért belső használatú, bizalmas vagy titkos dokumentumokat, adatokat kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni. Ennek keretében tilos pl. a rendelkezésre bocsátott dokumentumokat, adatokat idegen (pl. magántulajdonú) eszközre menteni!

2.124. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Hivatal/önkormányzat publikus weboldalát, Facebook vagy más közösségi média oldalát.

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

a) Új közösségi média oldalakat jegyző utasítására a rendszergazdának vagy a kijelölt felelősnek kell létrehozni annak megakadályozására, hogy az oldal egyetlen munkavállalóhoz kötődjön, amely munkavállaló jogviszonyának megszűnésével a Hivatal elveszítse a hozzáférését a munkavállaló által létrehozott közösségi média oldalhoz. A kijelölt felelős feladata a közösségi média oldal adminisztrátori felületének kezelése (amennyiben a közösségi média oldal rendelkezik ilyennel.
b) Ki kell jelölni azokat a felhasználókat, akik jogosultak a Hivatal/önkormányzat honlapján vagy közösségi média oldalán a szervezettel kapcsolatos bármely információ közzétételére (ezen kijelölt felhasználók – valamint a honlap rendszergazdája - rendelkezhetnek a honlapon, illetve a közösségi média oldalon közzétételt biztosító hozzáférési jogosultsággal, vagy ha egy adott közösségi média oldal csak egyetlen fiókkal kezelhető, ismerhetik a közösségi média fiók jelszavát).
c) A jegyzőnek és/vagy a polgármesternek kell egyedileg kialakítani a honlapra, hivatalos közösségi oldalra, profilra kerülő tartalmak engedélyezési és ellenőrzési folyamatát és az engedélyezésekről készült feljegyzések megőrzését (ki, mit, mikor engedélyezett feltöltésre, a feljegyzés hol kerül tárolásra), valamint az érintettek tájékoztatását.
d) A weboldal, közösségi médiaoldal kulcsfelhasználójának a közzététel előtt minden esetben át kell vizsgálnia a publikálandó tartalmakat a nem nyilvános információk tekintetében. Amennyiben a publikálandó tartalom informatikai rendszerek használatával, működésével, felépítésével kapcsolatos információkat tartalmaz, akkor a kulcsfelhasználónak a biztonságért Felelőst is be kell vonnia a vizsgálatba, az olyan, nem kívánt információk kiadásának elkerülése érdekében, amely egy rosszindulatú támadó részére segítséget nyújthat egy informatikai rendszer elleni támadáshoz.
e) A kulcsfelhasználónak legalább havi gyakorisággal át kell vizsgálnia a szervezet honlapját és közösségi média oldalát a nem nyilvános információk tekintetében és gondoskodnia kell azok eltávolításáról. Amennyiben bármely felhasználó nem nyilvános információkat fedez fel a honlapon vagy a közösségi média oldalon, akkor erről értesítenie kell a kulcsfelhasználót, aki intézkedik az eltávolításról.

f) Amennyiben a Hivatallal szerződéses jogviszonyban álló külső szolgáltató rendelkezik technikai hozzáféréssel, számára a kijelölt megbízott adhat át dokumentált módon írásban – nyilvános közzétételre szánt, ellenőrzött – információt.
g) A biztonságtudatossági képzés keretében minden felhasználót – a rendszergazdát is beleértve - fel kell készíteni a nem nyilvános információk (pl.: személyes adatok, jogszabállyal védett adatok, üzleti titkok) felismerésére, annak biztosítása érdekében, hogy a publikálandó nyilvános tartalmak ne tartalmazzanak nem nyilvános információkat (Ld. 3.2. Biztonságtudatossági képzés).
h) Tilos a hatályos törvénybe, jogszabályba, belső szabályzatba ütköző, vagy a szervezet érdekeit, a jó ízlést és közerkölcsöt sértő tartalmat közzétenni (Ld. 13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások).

A biztonsági eseményekkel kapcsolatos nyilvános tájékoztatások során a BCP terv külső kommunikációra vonatkozó pontja szerint kell eljárni, és ekkor is biztosítani kell, hogy a tájékoztatás ne tartalmazzon nem nyilvános- vagy az informatikai rendszerek elleni rosszindulatú támadáshoz felhasználható információkat.

A közérdekű adatok közzétételre vonatkozóan a hatályos Közzétételi Szabályzat szerint kell eljárni.

3. TUDATOSSÁG ÉS KÉPZÉS

3.1. Képzési eljárásrend

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

A biztonság tudatosítása a felhasználók esetében oktató anyagok terjesztésével és képzések útján történik, melyről a jegyző gondoskodik. A szerepkör szerinti oktatási tematikákat és anyagokat a biztonságért Felelős személy készíti, a jegyző véleményezi, szükség szerint a rendszergazda bevonásával. A képzés része az Üzletmenet-folytonossági tervvel kapcsolatos tudnivalók oktatása.

A biztonságáért Felelős a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megszerzése érdekében kapcsolatot alakít ki és tart fenn az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és ágazati szervezetekkel, partnerekkel, szakmai szervezetekkel. Figyelemmel kíséri a kiadott tájékoztatókat, riasztásokat, amelyeket beépít az oktatási anyagba.

3.2. Biztonságtudatossági képzés

A Hivatal biztonságtudatossági képzést nyújt az elektronikus információs rendszer felhasználói vagy ahhoz hozzáféréssel rendelkezők számára annak érdekében, hogy az informatikai rendszerek felhasználói tudatában legyenek a rendszerekre ható fenyegetéseknek - képesek legyenek ezek felismerésére, biztonságosan tudják használni a rendszereket, minimalizálni tudja a felhasználókra ható veszélyforrások bekövetkezéséből fakadó károk hatásait, a felhasználók megismerjék az érvényes lévő biztonsági követelményeket, a rájuk vonatkozó szabályokat és felkészültek legyenek a védelmi intézkedésekre vonatkozó szabályozások betartására, valamint tisztában legyenek a feladataikkal, felelősségükkel.

A képzés szükséges:

a) az elektronikus információs rendszer újonnan belépő felhasználói számára, a kezdeti képzés részeként (az informatikai rendszerekkel újonnan kapcsolatba kerülő felhasználók jogosultság-igényléséhez kapcsolódóan),
b) eltérő munkakörbe kerülés esetén, ha indokolt,
c) amikor az elektronikus információs rendszerben bekövetkezett változás szükségessé teszi,
d) ismétlődően 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 Információbiztonsági 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.

A biztonságáért Felelős feladata az érintettek, felhasználók számára az Információbiztonsági tudatosság megszerzéséhez, szinten tartásához szükséges oktatási anyag összeállítása, naprakészen tartása.

A képzésen a következő témaköröket kell minimálisan érinteni:

a) Információbiztonsági alapfogalmak;
b) Támadási formák: számítógépes kártevők fajtái, ember által elkövetett támadások fajtái;
c) Vonatkozó jogszabályok, szabályzatok;
d) Felhasználók feladatai, felelősségei;
e) Biztonsági események, belső fenyegetések felismerése és jelentése;
f) Az Internet és az elektronikus levelezés biztonsága;
g) Vírusok és egyéb kártevők elleni védelmi intézkedések;
h) Nem nyilvános információk (pl.: személyes adatok, jogszabállyal védett adatok, üzleti titkok) felismerése;

i) Jogosultsági rendszer, jogosultság igénylés folyamata;
j) Üzletmenet-folytonossági tervben meghatározott intézkedések tudatosítása (minden felhasználó ismerje, milyen esetben, és kit kell értesíteni katasztrófa esetén – ezek az információk mindenki számára elérhetőek a belső hálózaton;

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).

A biztonság tudatosság képzések megtartása a biztonságért Felelős vagy a jegyző által kijelölt felelős feladata. A képzés elvégezhető e-learning képzési formában is. A jegyző vagy az általa kijelölt képzési felelős 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 a biztonságáért Felelős felé. A belső oktatásokon, illetve a jogszabály vagy hatóság által elrendelt éves továbbképzéseken kötelező a részvétel, amelyről részvételi nyilvántartást kell vezetni.

A képzést a 3.13. A biztonsági képzésre vonatkozó dokumentációk pontban leírtak szerint kell dokumentálni.

3.4. Biztonságtudatossági képzés – Belső fenyegetés

A biztonságtudatossági képzés keretében a felhasználókat a belső fenyegetések felismerésére is fel kell készíteni, és tudatosítani kell jelentési kötelezettségüket.

3.9. Szerepkör alapú biztonsági képzés

A Hivatal szerepkör 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) éves rendszerességgel.

A Hivatal a Szerepkörök, tevékenységek felelősségek fejezetben határozta meg az 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 az illetékes szervezeti egység vezető/adatgazda által kijelölt személy közreműködésével sajátítják el a szükséges ismereteket. Akkor lehet önálló munkával megbízni, ha megfelelő gyakorlatot szerzett és a felelős meggyőződött a felkészültségéről.

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 az illetékes szervezeti egység vezető/adatgazda feladata. Az új bevezetésű szakrendszerek felhasználóinak - ha szervezett - részt kell venni az előírt oktatásokon, amely alapján a rendszert az elvárásoknak megfelelően, önállóan is használni tudják. A felhasználók képzése megtörténhet a szakrendszer által biztosított képzések elvégzésével vagy pl. az Önkormányzati alkalmazásközpont dokumentációinak felhasználásával.

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 az illetékes szervezeti egység vezető/adatgazda.

A biztonságért Felelős személy, a biztonságért Felelős helyettesítésére jogosult személy (helyettes Felelős), illetve a szervezet vezetőjeként a jegyző teljesíti a Kiberbiztonsági törvény által előírt, Magyarország kiberbiztonságáról szóló törvény szerinti végzettségekre, szakképzettségekre, valamint képzésekre és továbbképzésekre vonatkozó rendeletben előírt képzési és továbbképzési kötelezettségeket.

A szervezet vezetőjének képzésére és továbbképzésére vonatkozó rendelkezések alapján a jegyző a szervezet vezetőjévé válását követő egy éven belül szervezett képzésen vesz részt, melynek tárgykörei: kiberbiztonsági trendek, -kockázatok és szervezeti stratégiák, uniós és hazai kiberbiztonsági jogszabályi kötelezettségek és feladatok, kiberbiztonsági incidenskezeléshez kapcsolódó feladatok, -jógyakorlatok és tapasztalatok megosztása. Az ismétlődően évente szervezett továbbképzés tárgykörei: kiberbiztonsági trendek, -kockázatok és szervezeti stratégiák, uniós és hazai kiberbiztonsági jogszabályi kötelezettségek és feladatok változásai, kiberbiztonsági jógyakorlatok és tapasztalatok megosztása.

3.13. A biztonsági képzésre vonatkozó dokumentációk

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

4. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

4.1. Naplózási eljárásrend

A naplózás során az informatikai rendszerek automatikusan rögzítik az eseménynaplóban a rendszerben bekövetkező eseményeket, hibákat, felhasználói tevékenységeket és ezek időpontját. A naplózás lehetővé teszi a változások észlelését, a felhasználók számonkérhetőségét, és elengedhetetlen a biztonsági események kezeléséhez. A naplózási beállítások elvégzése a rendszergazda feladata és felelőssége. A naplózási beállításokat legalább évente egyszer a rendszergazdának kell felülvizsgálni és szükség esetén módosítani, illetve akkor, ha az elektronikus információs rendszerben változás történik.

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

4.2. Naplózható események

A naplózásnak az informatikai rendszerek kapcsolódó környezetére is ki kell terjednie, vagyis az alkalmazói szoftverek mellett a szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök esetén is engedélyezni kell a naplózást. Az informatikai rendszerek naplózásának kialakításakor a rendszer kulcsfelhasználóját is be kell vonni azért, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek. A naplózás során az informatikai rendszerek automatikusan eseménynaplóban rögzítik a rendszerben bekövetkező eseményeket, hibákat, felhasználói tevékenységeket és ezek időpontját. A naplózható események meghatározásakor a rendszergazda figyelembe veszi az érintett munkatársak információigényét is.

A Hivatal rendelkezésében lévő informatikai rendszerekre vonatkozóan biztosítani kell, hogy az informatikai rendszerek és kapcsolódó környezetük naplózni tudja legalább a következő eseményeket:

a) a felhasználók be- és kijelentkezését a rendszerbe (beleértve a sikeres és a sikertelen kísérleteket);
b) a rendszergazdai jogosultsággal végzett tevékenységeket;
c) a felhasználói fiókok és jogosultságok létrehozását, módosítását, engedélyezését, letiltását, törlését;
d) a konfigurációs beállítások módosítását;
e) az alap infrastruktúra rendszereire vonatkozóan az alkalmazói szoftverekben az adatállományok (adatbázisok) módosítását;
f) a rendszer eseményeket (pl. a rendszer leállását és újraindulását);
g) a vírusvédelmi rendszer működésével és beállításaival kapcsolatos eseményeket;
h) a rendszerben fellépő hibákat, eseményeket, pl. nem szabályos leállásokat,
i) a határvédelem logolását.

A naplózási beállításokat a biztonságért Felelős a rendszergazda közreműködésével a rendszerek bevezetésekor és az éves felülvizsgálatok során ellenőrzi annak érdekében, hogy elengedőek-e esetleges biztonsági események kivizsgálásához. Az adminisztrátori tevékenységeket a rendszerek meglévő naplózási szolgáltatásai rögzítik, ezekről külön gondoskodni jelenleg nem szükséges.

4.3. Naplóbejegyzések tartalma

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

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

Az informatikai rendszerek naplóbejegyzéseinek (ha releváns) a következőket kell tartalmazniuk:

a) az esemény forrását (rendszerelem, szoftver),
b) az esemény kódját és/vagy leírását,
c) a felhasználó azonosítóját,
d) az esemény időpontját,
e) az esemény típusától függően az esemény vizsgálatához szükséges egyéb információkat (pl.: a kapcsolódó adatok azonosítóját, a megváltozott adattartalmakat, a funkció végrehajtási státuszát stb.).

4.5. Naplózás tárkapacitása

Biztosítani kell, hogy elegendő tárhely álljon rendelkezésre a naplóbejegyzések mentéséhez, a naplózást és a naplók tárkapacitását úgy kell beállítani, hogy a naplóbejegyzések gyakrabban kerüljenek mentésre, mint ahogyan a napló betelése miatt a bejegyzések felülírásra kerülnének, ezzel biztosítva, hogy a napló-bejegyzések ne veszhessenek el. A mentéshez elegendő tárhely megállapításánál figyelemmel kell lenni a keletkező naplók számosságára, illetve azok megőrzési idejére. A megőrzési időt úgy kell megválasztani, hogy biztosítható legyen egy adott tevékenység bizonyíthatósága a naplók felhasználásával, illetve legyen szinkronban jogszabályban vagy egyéb szabályozó dokumentumban meghatározott értékkel.

A naplók tárkapacitásának figyelését az informatikai rendszerek felügyeleti tevékenységébe kell beépíteni (ld. 18.13. Az EIR monitorozása).

4.7. Naplózási hiba kezelése

Az informatikai rendszerek naplóinak a figyelését oly módon kell kialakítani, hogy naplózási hiba esetén a rendszer automatikusan küldjön riasztást az üzemeltetésért felelős rendszergazdának.

A Hivatal központi naplógyűjtő- és naplóelemző rendszereket alkalmazhat. A naplógyűjtő rendszer felépítését tekintve egy hardened virtuális szerver, VLAN és tűzfal védelemmel elkülönítve. A naplógyűjtő szerveren a privilegizált felhasználók többtényezős hitelesítése, audit naplózás és integritás védelem biztosítja a megfelelő biztonsági szintet. A naplógyűjtő szerverre kerül becsatornázásra minden naplózásra képes rendszer, és itt képződnek az archív hiteles naplók is. Oldalágon (forward) valós időben innen kerülnek továbbításra a naplók a naplóelemző rendszer (SIEM rendszer) felé, ahol elemzésre és vizualizálásra kerülnek, és itt találhatóak azok a dashboard-ok is, ahonnan a kritikus események bekövetkezése esetén a szükséges e-mail riasztások kiküldésre kerülnek a rendszergazdáknak. Naplógyűjtő szerver esetében szigorú monitoring szabályokat kell beállítani annak érdekében, hogy a naplófolyam (különösen a hitelesítési és audit napló típusok) folytonossága biztosítható legyen. Az olyan napló eseményeket, amelyek a naplógyűjtő szerver egy esetleges kiesése alatt keletkeztek, a logger parancs segítségével hiteles módon újra szükséges küldeni.

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

Az informatikai rendszerek és kapcsolódó környezetük (alkalmazói szoftverek, szerverek, hálózati eszközök, határvédelmi eszközök és egyéb biztonsági eszközök) eseménynaplóit az üzemeltetési feladatok részeként a rendszergazdának legalább havonta át kell vizsgálniuk, hogy kiszűrhetőek legyenek a szokatlan tevékenységek.

Az eseménynaplók vizsgálatának támogatására, automatizálására erőforrások rendelkezésre állása esetén vagy ha kockázatértékelés alapján indokolt, automatizált központi naplógyűjtő és elemző szoftver használata szolgál, amely egységesen, egy helyre gyűjti a rendszerek napló fájljait. Ezek a szoftverek általában képesek az elemzések alapján riasztás küldésére is, ezzel csökkentve a rendellenes tevékenység felfedezésének idejét.

A hibabejegyzéseket és a szokatlan működésre utaló jeleket a 18.2. Hibajavítás pontban leírtak alapján kell kezelni. A biztonsági eseményre utaló jeleket a 9.27. A biztonsági események jelentése pont szerint kell jelenteni. Naplózási inkonzisztencia vagy nagyobb kiesés esetén a rendszergazdáknak jelentési kötelezettségük van a biztonságért Felelős felé, aki vizsgálatot végez az audit naplók alapján a megfelelő integritás megtartása érdekében. Vizsgált, szokatlan tevékenységek különösen a sorozatos belépési kísérletek, hivatali vagy szokásos időn túli felhasználói, ezen belül kiemelten a rendszergazdai jogosultsággal végzett tevékenységek, a felhasználói fiókokkal kapcsolatos szokatlan tevékenységek, a konfigurációban bekövetkezett nem várt változtatások, szokatlan adatbázis műveletek, rendszer események, a központi menedzser funkciót nem biztosító vírusvédelmi rendszer gyanús eseményei, külföldi és/vagy ismeretlen IP címről érkező kapcsolatok.

4.24. Időbélyegek

Az informatikai rendszereknek valamennyi naplóbejegyzését időbélyeggel (időbejegyzéssel) kell ellátnia, melyhez a rendszerórát kell alapul venniük. A szerverek, a munkaállomások és a tűzfalak belső óráját a naplóbejegyzések követhetősége érdekében úgy kell beállítani, hogy azok az internetről automatikusan szinkronizálódjanak a szokásos internetes időszolgáltatások (Network Time Protocol, NTP) egyikéről, az óraszinkronizáláshoz szükséges protokoll átengedését a tűzfalakon biztosítani kell.

A naplótevékenységek egységes naplózásához a Hivatal a time.windows.com időszinkront használja, a rendszergazda feladata, hogy minden eszközön ezt állítsa be (UTC +01:00 Budapesti időzóna szerint).

4.25. Naplóinformációk védelme

Az elektronikus információs rendszert, szervereket és munkaállomásokat úgy kell konfigurálni, hogy csak a rendszergazdai jogosultsággal rendelkezők tudjanak a naplóinformációkhoz hozzáférni.

Gondoskodni kell arról, hogy az informatikai rendszerek naplóinformációi védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben. A naplóinformációk védelmét a Hivatal a hozzáférési jogosultságok megfelelő beállításával, illetve központi naplógyűjtő- és naplóelemző rendszerek alkalmazásával éri/érheti el.

4.38. A naplóbejegyzések megőrzése

A naplóinformációk mentését be kell vonni a Hivatal mentési rendszerébe. A mentéseket a napló tárkapacitással összhangban úgy kell kialakítani, hogy a naplóbejegyzések nem veszhetnek el (4.5.Naplózás tárkapacitása). A naplózási szolgáltatásokat úgy kell beállítani, hogy azok lehetőség szerint (amennyiben a rendelkezésre álló tárhely lehetővé tesz) legalább 6 hónapra visszamenőleg rendelkezésre álljanak. Amennyiben nem áll rendelkezésre megfelelő méretű tárhely az eseménynaplók 6 hónapra visszamenő megőrzéséhez, úgy az eseménynaplót a biztonságos működést nem veszélyeztető maximumban kell beállítani.

A naplóinformációkat a biztonsági események utólagos kivizsgálása érdekében:

a) az alkalmazói szoftverek naplóira vonatkozóan minimálisan 1 évig;
b) az egyéb környezeti naplók (pl.: operációs rendszerek, hálózati eszközök, határvédelmi eszközök naplói) esetén 6 hónapig kell megőrizni.

A megőrzési idők biztosítása érdekében az alkalmazói szoftverek naplóinak mentését az éves, illetve az archív mentésekkel, az egyéb környezeti naplók mentését a havi mentésekkel együtt kell végezni.

4.40. Naplóbejegyzések létrehozása

Az elektronikus információs rendszernek biztosítania kell a naplóbejegyzések előállítását a 4.2. Naplózható események fejezetben meghatározottak szerinti eseményekre, a 4.3. Naplóbejegyzések tartalma pontban meghatározott tartalommal.

5. ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS

5.1. Biztonságértékelési eljárásrend

A Hivatal biztonsági elemzés segítségével értékeli az informatikai rendszerei és annak működési környezete védelmi intézkedéseit. Az elemzés célja az, hogy a Hivatal meggyőződhessen arról, hogy a szükséges védelmi intézkedések megvalósítása megfelelően megtörtént, működésük a tervezettnek megfelelő, eredményei alapján megállapíthatók az eltérések a szabályzatban rögzített információbiztonsági előírások és a gyakorlatban megvalósított megoldások között. A célok érdekében a jelen fejezetben meghatározott Biztonságértékelési eljárásrendet kell alkalmazni.

5.2. Biztonsági értékelések

A biztonsági értékelések a jelen Információbiztonsági szabályzatban előírt védelmi intézkedések vizsgálatára terjednek ki. Az informatikai rendszerek és működési környezetük védelmi intézkedéseinek értékelésére, és a bevezetett intézkedések működőképességének, valamint a tervezettnek megfelelő működésének kontrolljára a Hivatal tervezett módon, legalább kétévente rendszeres biztonságértékeléseket (továbbiakban: tervezett biztonságértékelések), valamint szükség szerint, eseti jelleggel rendkívüli biztonságértékeléseket (továbbiakban: eseti biztonságértékelések) végez. Az eseti biztonságértékelések szükségességéről és a biztonságért Felelős és a jegyző közösen dönt. A Biztonságértékelés tervezését, koordinálását és ja elentés elkészítését a biztonságért Felelős végzi.

A tervezett és az eseti biztonságértékelések résztvevői: a biztonságért Felelős, rendszergazda, a személyes interjúk lefolytatása és a védelmi intézkedések működéséhez kapcsolódó bizonyítékok bekérése érdekében közreműködőként bevonásra kerülhetnek az adatgazdák, felhasználók is.

A tervezett biztonságértékelésekhez Biztonságértékelési tervet kell készíteni, és a tervben foglaltakat végre kell hajtani. A tervnek tartalmaznia kell:

a) az értékelés célját;
b) az értékelési környezetet;
c) a biztonsági ellenőrzések eredményességét meghatározó eljárást (a feltárt biztonsági hibák kockázati besorolását);
d) a terv végrehajtásához kapcsolódó szerepköröket és ezek feladatait;
e) a kiválasztott, értékelendő védelmi intézkedéseket;
f) a terv végrehajtásának ütemezését.

A Biztonságértékelési terv elkészítéséért a biztonságért Felelős felel, a tervet a jegyző hagyja jóvá. Ezeket a feladatokat legalább az éves felülvizsgálatok alkalmával el kell végezni. A biztonságért Felelős a rendszergazdától, jegyzőtől, felhasználóktól szerzett információk alapján végzi az értékelést, kiegészítve a helyszíni ellenőrzések alkalmával tapasztaltakkal és szúrópróbaszerű vizsgálatokkal. A biztonságértékelések keretében az éves gyakoriságú kockázatértékelés eredményeit is fel kell használni, azon belül a magas és kritikus besorolású kockázatokat, valamint az információbiztonságot érintő szabályzatokat és a hozzájuk kapcsolódó dokumentációkat is vizsgálni kell, hogy aktuálisak vagy módosításra szorulnak-e.

A belső biztonságértékelések eredményét a biztonságért Felelősnek a Biztonságértékelési jelentésben (szükség szerint és/vagy Intézkedési tervben) kell összefoglalnia, amelynek tartalmaznia kell:

a) az elvégzett tevékenységeket;
b) a feltárt biztonsági hibákat (beleértve a módosításra szoruló szabályzatokat és kapcsolódó dokumentációkat);
c) a javasolt intézkedéseket;
d) tervezett biztonságértékelések esetén a korábbi vizsgálatok eredményével történő összehasonlítást.

A Biztonságértékelési terv és jelentés(ek) bizalmas jellegű dokumentumok, amelyet a feltárt biztonsági hibák kezelésében érintett személyekkel (a jegyzővel, a rendszergazdával, szükség szerint az érintett informatikai rendszerek adatgazdáival, illetve az érintett szervezeti egységek vezetőivel) oszthatók meg.

5.4. Biztonsági értékelések – Kiberbiztonsági audit

A Hivatal nem kötelezett független auditor által elvégzett kiberbiztonsági auditra.

5.7. Információcsere

A Hivatal informatikai rendszereinek más informatikai rendszerekkel történő összekapcsolása (a rendszerek közötti interfészes kapcsolat létrehozása) az érintett rendszerek adatgazdái, a rendszergazda és a biztonságért Felelős jóváhagyásával történhet. Információcsere-megállapodás vagy egyéb dokumentum keretében dokumentálni kell az interfészes kapcsolatok leírását, jellemzőit, biztonsági követelményeit, a kapcsolaton keresztül átvitt adatok típusát, védelmi intézkedéseit, felelősségi köröket. Az információcsere-megállapodás részleteit hivatalos szerződésekben kell rögzíteni, különösen állami és nem állami szervezetek, szolgáltatók, rendszerfejlesztők és rendszerintegrátorok esetében.

Rendszeres időközönként felül kell vizsgálni és szükség esetén frissíteni kell az információcsere-megállapodásokat és dokumentumokat, hogy azok megfeleljenek az aktuális kockázati és működési követelményeknek. Az új vagy növekvő fenyegetések hatásának figyelembevételével a Hivatalnak kockázatelemzést kell végeznie az információcserében érintett rendszerek között, különös tekintettel a biztonsági követelmények és védelmi intézkedések különbségeire. A szervezetnek a kockázatok mérlegelése során figyelembe kell vennie azokat a rendszereket is, amelyek ugyanabban a hálózati környezetben működnek, az esetleges belső biztonsági fenyegetések elkerülése érdekében.

A Hivatal informatikai rendszereink külső informatikai rendszerekhez való az érintett rendszerek adatgazdáinak, a rendszergazdának és a biztonságért Felelősnek a jóváhagyásával és a következő biztonsági követelmények teljesülése esetén engedélyezett:

a) A határvédelem üzemeltetése során alapértelmezés szerint minden kapcsolatot tiltani kell, csak a működéshez szükséges, dokumentált portokat, protokollokat és szolgáltatásokat szabad engedélyezni.
b) Amennyiben értelmezhető, az interfészes kapcsolatnál IP alapú korlátozást kell bevezetni.
c) Gondoskodni kell az interfészes kapcsolatok megfelelő azonosításról és hitelesítésről. Minden interfész dedikált technikai felhasználóval és jelszó kiválasztási követelményeknek megfelelő generált jelszóval kell azonosítani magát a 8.22.6. Beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelése vonatkozó eljárása szerint.
d) Szabványos, sérülékenységektől mentes kriptográfiai eszközökkel biztosítani kell az átvitt adatok bizalmasságát és sértetlenségét.

5.10. Az intézkedési terv és mérföldkövei

A biztonságértékelések után a biztonsági hibák javítása érdekében Információbiztonsági intézkedési tervet kell készíteni, a tervet rendszeresen felül kell vizsgálni és karban kell tartani az 1.4. Intézkedési terv és mérföldkövei fejezetben leírtak szerint, illetve a biztonságértékelések és az auditok eredményét fel kell használni a kockázatelemzési folyamatban.

5.12. Engedélyezés

Az informatikai rendszerekkel kapcsolatos engedélyezésekért a rendszer adatgazdája felel, amely magában foglalja a következő feladatokat:

a) engedélyezi a külső és belső felhasználók különböző szintű hozzáférését az informatikai rendszerhez,
b) engedélyezi a rendszerben végzett változtatásokat,
c) az informatikai rendszer bevezetése vagy módosítása során a jegyzővel közösen engedélyezi a rendszer használatba vételét.

Az informatikai rendszerek közös biztonsági követelményeit (beleértve a külső informatikai rendszerekkel szembeni követelményeket is), jelen Információbiztonsági szabályzat tartalmazza.

5.15. Folyamatos felügyelet

Adott informatikai rendszerekre vonatkozóan a védelmi intézkedések megvalósulásának és hatékonyságának értékelését, ennek eredményéről az érintettek tájékoztatását, és a javasolt válaszintézkedések kidolgozását a biztonságért Felelős az 1.23 Folyamatos felügyeleti stratégia pontban leírtak szerint végzi.

5.18. Folyamatos felügyelet – Kockázatmonitorozás

A kockázatok monitorozását a biztonságért Felelős végzi. A kockázatmonitorozás részeként ellenőrzi, hogy mely biztonsági követelmények teljesülnek és azt, hogy a bevezetett kockázatcsökkentő intézkedések milyen hatékonysággal működnek. Az Információbiztonsági kockázatelemzést felül kell vizsgálni, ha változás következik be az informatikai rendszerekben vagy azok környezetében, továbbá olyan körülmények esetén, amelyek befolyásolják az informatikai rendszerek biztonsági állapotát.

5.25. Belső rendszerkapcsolatok

A Hivatal belső engedélyhez köti az elektronikus információs rendszereinek összekapcsolását. A Hivatal informatikai rendszereinek szervezeten belüli összekapcsolása az érintett rendszerek adatgazdáinak, a jegyzőnek és a biztonságért Felelősnek a jóváhagyásával történhet.

Az informatikai rendszerek részét képező alrendszerek közötti belső interfészes kapcsolatok engedélyezésére, dokumentálására, felülvizsgálatára vonatkozóan is az 5.7. Információcsere pontban leírtakat kell alkalmazni. Az egyes rendszerelem kategóriákra (pl. szerver, munkaállomás, tűzfal, router, switch stb.) vonatkozóan akkor engedélyezett az informatikai rendszerhez való kapcsolódás, ha megfelelnek az Alapkonfigurációban meghatározott hardver/szoftver követelményeknek és konfigurációs beállításoknak (ld. 6.2 Alapkonfiguráció).

A rendszergazda feladata, hogy a felügyelt rendszerek interfészeit legalább kétévente felülvizsgálják (beleértve a kapcsolat szükségességét), és a szükségtelen kapcsolatokat megszüntessék.

6. KONFIGURÁCIÓKEZELÉS

6.1. Konfigurációkezelési eljárásrend

A konfigurációkezelés célja, hogy az informatikai rendszerek elvárt védelmi követelményének megfelelően biztosítsa azok megbízható működését a rendszerösszetevők telepítésének, konfigurálásának, megváltoztatásának, tesztelésének és nyilvántartásának szabályozott körülmények közötti végrehajtásával.

A munkaállomások és kapcsolódó perifériák üzembe helyezését, javítását és karbantartását a rendszergazda és a jegyző által ezzel megbízott külső partnerek végezhetik. Az üzembe helyezés helyét és az eszközért felelős felhasználó személyét a közvetlen (vagy felettes) munkahelyi vezető jelöli ki.

Az üzembe helyezés során:

a) jól látható helyen (lehetőleg az eszköz előlapján) el kell helyezni az eszköz egyedi azonosítására szolgáló informatikai azonosítót;
b) a számítógépeken be kell állítani az Alapkonfiguráció szerinti egységes szoftver környezetet (ld. 6.2. Alapkonfiguráció pont);
c) telepíteni kell a Hivatal által biztosított egyéb szoftvereket.

Az üzembe helyezést végzőnek az üzembe helyezett eszköz hardver/szoftver konfigurációját üzembe helyezési jegyzőkönyvön, Munkalapon vagy egyéb dokumentumban kell rögzítenie és az eszközért felelős felhasználóval vagy munkahelyi vezetőjével aláíratni. Ez alapján kell a hardver konfiguráció adatait, a telepített licencköteles szoftvereket, valamint az eszköz tárolóhelyét és az eszközért felelős felhasználó személyét felvezetni a hardver- és szoftver nyilvántartásokba (ld. 6.36. Rendszerelem leltár). Az üzembe helyezési dokumentum másolatával kell átadni a számviteli területnek a befektetett eszközök nyilvántartásba felveendő, tárgyi eszköznek számító informatikai eszközök, illetve szoftverek pontos megnevezését és az eszközök informatikai azonosítóját. A befektetett eszközök nyilvántartásban az informatikai eszközök megnevezése mellett az informatikai azonosítót is rögzíteni kell, amely megkönnyíti a számviteli és az informatikai nyilvántartások egyeztetését és az eszközök leltározását.

A külső szervizből visszaérkezett javított eszközök konfiguráció változását ellenőrizni kell, mivel a javítás, karbantartás során változhat az eszközök hardver konfigurációja, cserélődhetnek a tartozékai. A változásokat ilyen esetben a nyilvántartásokban, leltárakban is szerepeltetni kell.

6.2. Alapkonfiguráció

Az informatikai rendszerekhez dokumentált formában Alapkonfigurációt kell készíteni és ezt biztonságos helyen kell tárolni.

Az Alapkonfiguráció dokumentációjának célja, hogy új rendszerelemek esetén rögzítse, hogyan kell az elemet telepíteni és konfigurálni, illetve meghibásodás esetén a rendszerelemeket hogyan kell újratelepíteni. A dokumentáció az egyes eszköztípusokra (pl.: szerver, munkaállomás, tűzfal, router, switch stb.) vonatkozóan meghatározza az adott feladat ellátásához szükséges hardver és szoftver környezetet.

Az Alapkonfigurációnak minimálisan a következőket kell magában foglalnia (amennyiben az adott eszköztípusra értelmezhető):

a) a feladat ellátásához szükséges minimális és ajánlott hardver elemek listáját;
b) a szükséges szoftverek listáját aktuális verzió számmal, biztonsági frissítési információkkal;
c) a szoftverek konfigurációs beállításait, paramétereit;
d) a szoftver telepítőkészletek listáját és elérhetőségi helyét;
e) az engedélyezett szolgáltatások, portok és protokollok listáját a „szükséges minimum" elv alapján (ld. 6.26. Legszűkebb funkcionalitás)

Az informatikai rendszerek Alapkonfigurációját a rendszergazda készíti el, legalább kétévente felülvizsgálja és a módosításokat átvezeti. A dokumentációt a biztonságért Felelős javaslata alapján a jegyző hagyja jóvá. Az Alapkonfigurációhoz kapcsolódóan az informatikai rendszerek lényeges elemeiről nyilvántartást kell vezetni a 6.36. Rendszerelem leltár pontban leírtak szerint.

6.15. Biztonsági hatásvizsgálatok

A kisebb változásokat, azonos vagy hasonló konfigurációval ellátott rendszerelem (eszköz) cseréket, illetve azokat a programverzió frissítéseket, amelyek nem tartalmaznak jelentős működésbeli változtatásokat minimális tesztelést követően a rendszergazda elvégezheti. A kisebb verzióváltások, a gyártó által kiadott frissítések telepítése kivételével a változtatás megkezdése előtt a biztonságért Felelősnek információbiztonsági szempontból értékelnie kell a változtatás informatikai rendszer biztonságára gyakorolt hatását, és szükség szerint előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható kockázatának minimalizálását.

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

Az informatikai rendszerekben változtatásokat csak a változtatás elvégzésére jogosult, fizikai belépési engedéllyel, illetve rendszergazdai hozzáférési jogosultságokkal rendelkező személyek végezhetnek.

A hozzáférésekre vonatkozó biztonsági követelményeket a 2.2 Fiókkezelés és a 12.2. A fizikai belépési engedélyek pontok tartalmazzák.

6.23. Konfigurációs beállítások

Az informatikai rendszerek működtetése során csak az Alapkonfigurációban szereplő, jóváhagyott hardver és szoftver elemek, konfigurációs beállítások használhatók. Ettől eltérő eszközöket és beállításokat csak engedélyeztetést követően lehet elvégezni. A kötelező konfigurációs beállítások érvényesítését a biztonságért Felelős a Biztonságértékelési tervben foglaltak szerint az Alapkonfiguráció alapján ellenőrzi (ld. 5.2. Biztonsági értékelések).

6.26. Legszűkebb funkcionalitás

Az informatikai rendszereket a „szükséges minimum" elv alapján úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszerek biztonságos működéséhez szükségesek. Az engedélyezett szolgáltatások, portok és protokollok listáját a rendszerek alapkonfigurációjában kell rögzíteni.

Az engedélyezett szolgáltatások, portok és protokollok kizárólagos használatát a biztonságért Felelős a Biztonságértékelési tervben foglaltak szerint ellenőrzi (ld. 5.2. Biztonsági értékelések).

6.36. Rendszerelem leltár

A rendszergazdának vagy a jegyző által kijelölt felelősnek leltárt kell vezetni az informatikai rendszerek valamennyi hardver/szoftver eleméről, gondoskodni kell a leltár teljességéről és naprakészségéről. A nyilvántartást rendszeres időközönként, bármely fejlesztés, bővítés, változás esetén, de legalább évente felül kell vizsgálnia és frissítenie kell. A leltár célja, hogy információval szolgáljon a Hivatalnál használt eszközökről, ahol lehetséges ezek alapkonfigurációiról, a bekövetkezett változásokról, valamint szükségessé válhatnak a Hivatal számára a hatékony személyes anyagi felelősségre vonhatósághoz. Ennek érdekében úgy kell elkészíteni, hogy pontosan tükrözze az elektronikus információs rendszer aktuális állapotát, valamint a rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza az elektronikus információs rendszerekhez vagy felhasználókhoz rendelve.

A leltár alapja a hardver eszközök egyértelmű és egyszerűen kezelhető azonosítása. Ennek érdekében az informatikai eszközökhöz az alkalmazott egységes névkonvenció szerint (pl. a szervezet nevének, az eszközök csoportjának és egy sorszámnak a felhasználásával) egyedi azonosítót (továbbiakban: informatikai azonosítót) kell rendelni. Az informatikai eszközök üzembe helyezésekor az informatikai azonosítót a hivatali gyakorlat szerint az eszközön jól látható módon fel kell tüntetni és – ahol értelmezhető – az eszköz szoftverében elektronikusan be kell állítani.

Változások (pl.: új informatikai eszközök/szoftverek üzembe helyezése vagy selejtezése; informatikai eszközök áthelyezése; szoftverek telepítése/eltávolítása; stb.) esetén folyamatosan karban kell tartani a nyilvántartásokat. A változások átvezetése a rendszergazda felelőssége, aki a változással kapcsolatos műveletet végrehajtotta. A hardver- és szoftver nyilvántartások adott rendszerhez kapcsolódó rendszerelemeit a rendszergazdának a legalább kétévente felül kell vizsgálniuk és az esetlegesen át nem vezetett változásokat át kell vezetniük.

6.36.1. Hardver nyilvántartás

A hardver nyilvántartásnak az alábbi adatokat kell az informatikai eszközökre vonatkozóan tartalmaznia:

a) az eszköz azonosítóját;
b) az eszköz leltári számát (opcionálisan);
c) ha az eszköz nincs használatban, akkor az eszköz állapotát (pl. tartalék, felesleges, selejt);
d) az eszköz gyártóját és típusát;
e) a fő jellemzőket (számítógépek esetén a processzor típusát, a memória és háttértár méretét, hálózati eszközök esetén a portok számát stb.);
f) számítógépek esetén az operációs rendszer típusát;
g) az eszköz fizikai helyét, tárolóhelyét (virtuális szerverek esetén a gazda szerver vagy klaszter azonosítóját);
h) felhasználói oldali eszközök esetén az eszközért felelős személy nevét;
i) szerver oldali eszközök esetén az informatikai rendszer megnevezését (amelyből az Informatikai rendszerek nyilvántartása alapján meghatározhatók a kijelölt rendszergazdák);
j) a beszerzés dátumát (opcionálisan);
k) a garancia lejáratának dátumát (opcionálisan);
l) az eszköz szállítóját (opcionálisan);
m) ha releváns, akkor a feleslegessé válás, illetve selejtezés dátumát.

A nyilvántartáshoz kapcsolódóan – az informatikai eszközök üzemeltetésének támogatására – visszakereshető formában meg kell őrizni az eszköz számlájának szkennelt másolatát, a garancia jegyet, telepítő adathordozót és az egyéb gyártói dokumentációt (pl.: kezelési- és karbantartási útmutató, műszaki leírás, stb.). A megőrzési idő az eszköz selejtezéséig tart.

6.36.2. Szoftver nyilvántartás

A szoftver nyilvántartásban az alábbi adatokat kell minimálisan vezetni:

a) a szoftver leltári számát (opcionálisan);
b) a szoftver nevét és verziószámát;
c) a szoftver funkciójának rövid megnevezését;
d) a szoftverlicenc típusát (pl.: OEM, dobozos, mennyiségi, belső/külső fejlesztés);
e) a beszerzett licencek darabszámát;
f) a felhasználható licencek darabszámát (mennyiségi licencek esetén);
g) a számítógép(ek) azonosítóját, amelyen a licenc felhasználásra került (OEM licenc esetén ez mindig a szoftverrel együtt vásárolt számítógép azonosítója);
h) a beszerzés dátumát (opcionálisan);
i) a szoftver szállítóját (opcionálisan).

A nyilvántartáshoz kapcsolódóan – a szoftverlicencek igazolása céljából – visszakereshető formában meg kell őrizni a szoftverek számlájának szkennelt másolatát és a szoftverlicencet igazoló egyéb dokumentumokat (pl.: licencszerződés, licencengedély, licenckulcs, stb.).

Alkalmazói szoftvereket kizárólag a rendszergazda, illetve a jegyző által ezzel megbízott külső partnerek telepíthetnek a felhasználói munkaállomásokra. A szoftverek munkaállomásokra történő telepítését vagy eltávolítását a rendszergazdától kell a felhasználóknak igényelni. A licencköteles (vásárolt, bérelt vagy fejlesztett) szoftverek licenceit a Szoftver nyilvántartásban kell nyilvántartani. Az ilyen szoftverek telepítése előtt a telepítést végző munkatársnak a nyilvántartás alapján ellenőriznie kell, hogy az adott szoftverre vonatkozóan a Hivatal rendelkezik-e felhasználható szoftverlicenccel. Tilos a szoftvereket a licenc által megengedett darabszámot meghaladó számban használni. A szabad szoftverek telepítése előtt ellenőrizni kell, hogy a szoftver szerepel-e a szoftverek nyilvántartásában, és milyen korlátozásokkal használható. A szoftver telepítését nem lehet elvégezni, ha a szoftver nem szerepel a nyilvántartásban.

A leltárnak tartalmazni kell a rendszerekben használt hardver és szoftverek elemek listáját, az azonosításukhoz szükséges adatokat és a hardver/szoftver elemek összerendelését, a szoftver elemekhez rendelt szoftverlicenceket és az egyes elemek használóját, felelősét.

Javasolt leltár elemek:

a) azonosító (gépnév),
b) gyártó (brand), típus (desktop, laptop)
c) tárolási hely / eszköz kijelölt felelőse (más nyilvántartásban is kezelhető)
d) CPU (gyártó, típus, órajel - GHz),
e) RAM (gyártó, típus, méret - GB),
f) HDD (gyártó, típus, méret - GB),
g) operációs rendszer
h) irodai szoftver
i) antivírus
j) javasolt ebben a nyilvántartásban is szerepelni: rendszergazdai ellenőrzés gyakorisága (előírt, nap)

A szoftvereket a Szoftver licencek nyilvántartásában kell nyilvántartani és a következőkre kell kiterjednie:

a) szoftver tulajdonosa (gyártó/fejlesztő)
b) szoftver megnevezése, típusa
c) szoftver verzió
d) nyelv
e) licenc típusa,
f) licenc száma,
g) licenc érvényessége, lejárata,
h) eredeti licenc konstrukció,
i) számítógépek vagy felhasználók azonosítója
j) megjegyzés

Az eszközök hálózatba történő illesztéséről dokumentációt kell készíteni, pl. Munkalapon. A nyilvántartás alapját képező, az elektronikus információs rendszerekhez kapcsolódó hardver és szoftver elemekről részletes nyilvántartások megőrzése az azt készítő vagy tárolásért kijelölt felelős feladata.

6.47. A szoftverhasználat korlátozásai

A Hivatal minden felhasználó számára biztosítja a munkavégzéshez szükséges szoftvereket, ezért a számítógépeken csak legális, a Hivatal által rendelkezésre bocsátott szoftverek használhatók a licencszerződésben foglaltak szerint. A rendszergazda és a jegyző felelőssége, hogy csak a Hivatal által vásárolt/bérelt, illetve számára belső vagy külső fejlesztéssel készült legális szoftverek, valamint az engedélyezési eljáráson átesett szabad szoftverek kerüljenek üzembe helyezésre.

A legális szoftverhasználat biztosítása és az informatikai rendszerek biztonsága érdekében az alábbi előírásokat kell betartani:

a) A felhasználók nem telepíthetnek vagy távolíthatnak el szoftvereket (ld. 6.49. Felhasználó által telepített szoftver), csak a rendszergazda, illetve a jegyző által ezzel megbízott külső partnerek.
b) A szoftverek felhasználói munkaállomásokra történő telepítésének igénylése és a telepítés végrehajtása során a jogosultságigénylésre és szoftverekkel, licencekkel kapcsolatos megkötésekre vonatkozó pontok szerint kell eljárni.
c) A licencköteles szoftverek telepítő adathordozóit és licenckulcsait a másolatok ellenőrzése érdekében a kijelölt rendszergazdáknak elzárva kell tárolnia és ellenőriznie kell a hozzáféréseket.
d) A kijelölt rendszergazdáknak ellenőrzés alatt kell tartania a hálózati megosztások jogosultság beállítását és tartalmát, és gondoskodnia kell arról, hogy a megosztások ne tegyék lehetővé a szerzői jogokkal védett szoftverek illegális használatát, illetve a szoftverek telepítőkészletének vagy licenckulcsának illetéktelen másolását, terjesztését.
e) Szoftverek telepítőkészleteit kizárólag a rendszergazda helyezhet el hálózaton megosztott mappákban az általa végzett szoftvertelepítések végrehajtása céljából. A licencköteles szoftverek telepítőkészletéhez csak rendszergazda rendelkezhet hozzáférési jogosultsággal. A felhasználók csak az engedélyezett szabad szoftverek telepítőkészletéhez férhetnek hozzá az automatizált telepítési folyamatok működése érdekében.

f) A szoftvereket kizárólag a licencszerződés előírásainak megfelelően lehet használni. A hálózati megosztásra, vagy több felhasználó által használt szerverekre (terminál szerverekre) történő szoftvertelepítést megelőzően ellenőrizni kell, hogy a licencszerződés milyen feltételekkel teszi lehetővé az ilyen használatot.

6.49. Felhasználó által telepített szoftver

A felhasználók nem telepíthetnek vagy távolíthatnak el szoftvereket, csak a rendszergazda vagy a jegyző által ezzel megbízott külső partnerek. A korlátozást az operációs rendszer segítségével kell kikényszeríteni, azaz a felhasználók csak korlátozott felhasználói fiókot használnak, amelynek nincs jogosultsága a telepítésre.

A szabályok betartását a biztonságért Felelős a Biztonságértékelési tervben foglaltak szerint (az 5.2. Biztonsági értékelések pont szerint) és szúrópróba-szerűén ellenőrzi.

Rendszerprogramokat, illetve felhasználói alkalmazásokat kiszolgálókra és munkaállomásokra, infokommunikációs eszközökre csak a rendszergazda telepíthet, másolhat, távolíthat el. A felhasználók semmilyen szoftvert, alkalmazást nem telepíthetnek a munkaállomásaikra, az infokommunikációs eszköz használata során kizárólag, az eszközre telepített szoftvereket, alkalmazásokat használhatják. Új szoftver, alkalmazás telepítését vagy a meglévő alkalmazás jogosultságváltozását igényelni kell. A rendszergazda és az adatgazda javaslata alapján a jegyző jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági vagy gazdasági okból annak elutasítására.

6.49.1. Telepítés nélkül futtatható szoftverek

A telepítés korlátozása a telepítés nélkül futtatható (ún. portable) szoftverek segítségével megkerülhető. Léteznek olyan telepítés nélkül használható szoftverek, melyeket szerzői jogok védelme alatt álló szoftverek feltörésével, illegális módon hoztak létre. Az ilyen szerzői jogot sértő szoftverek birtoklása és használata illegális szoftverhasználatnak minősül. A telepítés nélkül futtatható szoftverek nehezen felügyelhetők, használatuk biztonsági és licenc problémákat vet fel, ezért általános esetben a Hivatal számítógépein a telepítés nélkül futtatható szoftverek elindítása vagy a számítógépen történő tárolása tilos.

A tiltást lehetőség szerint technikai eszközökkel is érvényre kell juttatni (pl. tartományi szintű csoportházirend alkalmazásával a munkaállomásokon a futtatható programok helyének korlátozásával).

A telepítés nélkül futtatható szoftverek használatát a rendszergazda eseti alapon engedélyezheti. Az ilyen szoftverek engedélyezése során ugyanúgy kell eljárni, mintha a szoftver telepítésre kerülne az adott számítógépre (a licencköteles szoftverekhez érvényes licenccel kell rendelkezni, a szabad szoftvereknek át kellett esniük az engedélyezési eljáráson).

6.49.2. Automatizáltan települő szoftverek

Az engedélyezett szabad szoftverek és az összes munkaállomáshoz licenccel rendelkező szoftverek telepítése vagy a szoftverek verziófrissítése céljából rendszergazda alkalmazhat automatizált telepítési módszereket, amelyek pl. a hálózati bejelentkezés folyamán, egy szoftver indításának részeként, vagy a felhasználó opcionális döntése alapján indulnak el. Ezeket az automatizált telepítéseket a Hivatal által végzett telepítésnek kell tekinteni, akkor is, ha egy felhasználói művelet hatására aktivizálódnak.

Az automatizált telepítésekkel szembeni követelmény, hogy a telepítéseket naplózni kell és a munkaállomás felügyeleti rendszer kijelölt rendszergazdáinak a naplók vizsgálatával felügyeletet kell gyakorolnia a telepítési folyamat felett (ld. 4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel).

7. KÉSZENLÉTI TERVEZÉS

7.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

Az üzletmenet-folytonosság tervezés célja, hogy

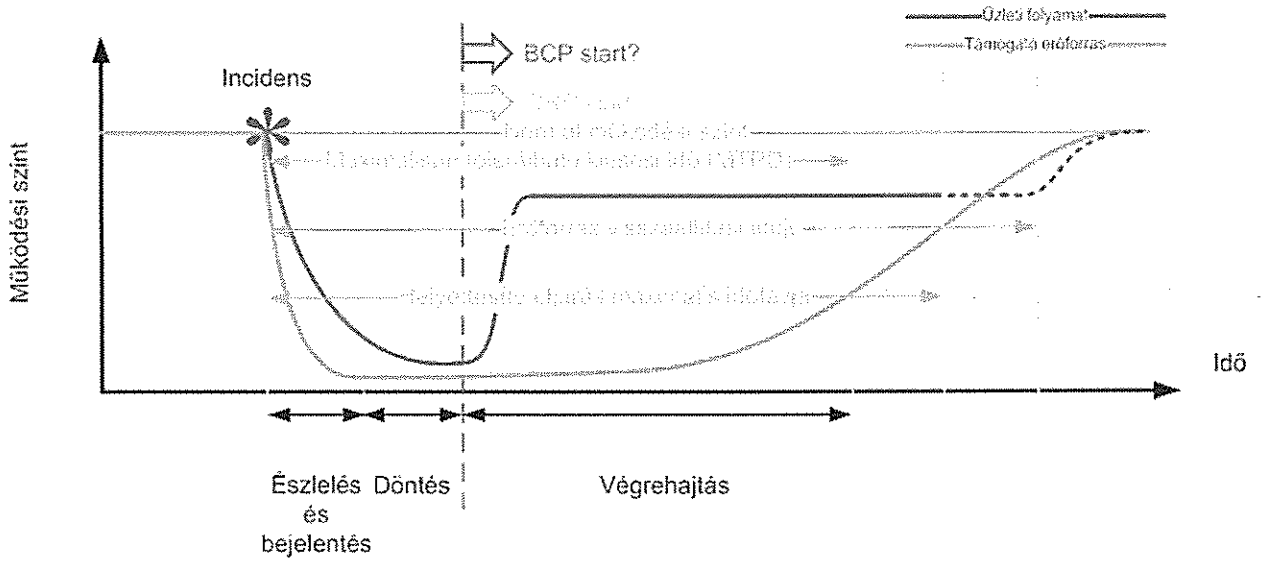
a) biztosítsa az informatikai rendszerek elvárt szintű folyamatos működését;
b) minimalizálja a nem várt események bekövetkezési valószínűségét;
c) csökkentse a nem várt esemény bekövetkeztekor keletkező károk hatásait, megvédje a kritikus folyamatokat a meghibásodások és katasztrófák negatív hatásaitól;
d) elősegítse az informatikai rendszerek üzemszerű működésének minél hamarabbi visszaállítását.

A célok érdekében a jelen fejezetben meghatározott Üzletmenet-folytonosságra vonatkozó eljárásrendet kell alkalmazni.

7.2. Üzletmenet-folytonossági terv

Informatikai üzletmenet-folytonossági tervet (továbbiakban: BCP terv) és ezzel összefüggésben Informatikai katasztrófa-elhárítási tervet (továbbiakban: DRP terv) kell készíteni az informatikai erőforrások kiesésére vonatkozóan az informatikai rendszerek folyamatos működésének biztosításához.

Egy katasztrófa esemény, vészhelyzet bekövetkezésekor két folyamatot kell elindítani (ld. az ábrán „DRP start" és „BCP start"):



a) Vissza kell állítani a katasztrófa következményeként kiesett informatikai erőforrásokat (DPR terv). A DRP tervet minden esetben életbe kell léptetni, ha valamely üzleti folyamatot támogató informatikai erőforrás kiesik.
b) Biztosítani kell a rendszer teljes visszaállításáig a kiesett erőforrások nélküli minimális funkcionalitást nyújtó üzleti működést, vészhelyzeti működést (BCP terv).

   A BCP tervet csak akkor szükséges aktiválni, ha az erőforrás várható visszaállítási ideje meghaladja a meghatározott maximálisan tolerálható kiesési időt. Ha ezen belül vissza lehet állítani az erőforrást, akkor nincs szükség a BCP terv életbe léptetésére.

7.2.1. Informatikai üzletmenet-folytonossági terv (BCP terv)

Az Informatikai üzletmenet-folytonossági tervben meg kell határozni:

a) a katasztrófa események definícióját;
b) a terv életbe léptetésének a feltételeit (hogyan kell a helyzetet értékelni, kiket kell bevonni, ki dönti el a katasztrófa tényét, ki felelős a folyamat inicializálásáért);
c) a vészhelyzeti szerepköröket, ezek felelősségét, feladatait;
d) a szerepköröket betöltő személyek nevét és elérhetőségét;
e) külső támogatást nyújtó partnerek esetén a kapcsolattartó személyek nevét és elérhetőségét;

f) vészhelyzet esetén a szereplők értesítésének módját, a riadóláncot;
g) mely informatikai rendszerek élveznek prioritást korlátozott vészhelyzeti működés esetén;
h) az informatikai rendszerek alapfeladatait és alapfunkcióit (a biztosítandó szolgáltatásokat), a minimális funkcionalitást, amelyeket a rendszer összeomlása, kompromittálódása vagy hibája ellenére is fenn kell tartani, valamint az alapfunkciókhoz kapcsolódó vészhelyzeti követelményeket;
i) a vészhelyzet esetén követendő eljárásokat, azaz a működést és/vagy az emberi életet veszélyeztető esemény bekövetkezte után végzendő teendők leírását, beleértve a nyilvánosság kezelésére, a hatóságokkal (pl.: rendőrséggel, tűzoltósággal, önkormányzattal) történő hatékony kapcsolatfelvételre vonatkozó rendelkezéseket;
j) az alapvető tevékenységek vészhelyzeti működésben történő folytatásának lehetőségeit, ezek megvalósításának lépéseit:
   - az automatizált folyamatok kézi póteljárásait;
   - az informatikai erőforrások dinamikus átcsoportosításának, tartalék eszközök beiktatásának a lehetőségét;
   - idegen szervezet eszközeinek igénybevételére épülő tartalék megoldást;
k) a felkészülési feladatokat a terv végrehajtásához, a biztosítandó erőforrásokat (pl.: a kézi póteljáráshoz szükséges törzsadatokat, szerződéseket stb.);

7.2.2. Informatikai katasztrófa-elhárítási terv (DRP terv)

Az Informatikai katasztrófa-elhárítási tervben meg kell határozni:

a) a vészhelyzeti szerepköröket, ezek felelősségét, feladatait;
b) a szerepköröket betöltő személyek nevét és elérhetőségét;
c) támogatást nyújtó külső partnerek esetén a kapcsolattartó személyek nevét és elérhetőségét;
d) a katasztrófa megelőzése érdekében végzett tevékenységeket;
e) a katasztrófa elhárítás előfeltételeként elvégzendő mentések rendszerét (ld. 7.35.6. A mentési rendszer dokumentálása);
f) a felkészülési feladatokat a terv végrehajtásához, a biztosítandó erőforrásokat (pl.: tartalék- és segédeszközöket, telepítő adathordozókat, üzemeltetési dokumentációkat stb.);
g) a végleges, teljes informatikai rendszer helyreállításának lépéseit úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket;

Az Informatikai üzletmenet-folytonossági terv (BCP terv) és az Informatikai katasztrófa-elhárítási terv (DRP terv) elkészítéséért és karbantartásáért – a rendszergazdával és az adatgazdákkal együttműködve – a biztonságért Felelős felel. Mindkét tervet a jegyző fogadja el.

A tervek bizalmas minősítésű dokumentumok, amelyeket a tervekben rögzített, a végrehajtásban érintett személyek, szervezeti egységek (vészhelyzeti szereplők) számára kell kihirdetni, akik illetéktelenek azt nem adhatják tovább.

A terveket legalább kétévente felül kell vizsgálni és minden olyan esetben aktualizálni kell, ha változás következik be az informatikai rendszerekben vagy környezetükben, illetve a tervekben szereplő adatokban, így például:

a) új informatikai rendszer bevezetése;
b) új nagyteljesítményű hardver eszközök beszerzése;
c) a vészhelyzeti szereplők személyének változása;
d) támogatást nyújtó külső partnerek változása;
e) elérhetőségi adatok (e-mail címek, telefonszámok) változása.

A tervek éles helyzetben történő végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálni, javítani kell a tervek tartalmát. A tervek változásairól tájékoztatni kell a tervekben rögzített vészhelyzeti szereplőket.

7.10. A folyamatos működésre felkészítő képzés

Az üzletmenet-folytonosság megfelelő szinten tartása, valamint a nem várt események esetén alkalmazandó Informatikai üzletmenet-folytonossági terv és Informatikai katasztrófa-elhárítási terv megfelelő hatékonysággal történő végrehajtása érdekében a tervek végrehajtásában érintett szereplők részére a szerepkörbe kerülésüket vagy a tervek változását követően felkészítő és évente ismétlő képzéseket kell tartani.

A képzés tartalmának összeállítása és a képzések lebonyolítása a biztonságért Felelős feladata. A képzést a 3.13. A biztonsági képzésre vonatkozó dokumentációk pontban leírtak szerint kell dokumentálni.

7.35. Az elektronikus információs rendszer mentései

Az informatikai rendszerek által kezelt adatokról, a működését biztosító szoftverekről, a rendszer eseménynaplóiról és a rendszerhez kapcsolódó dokumentációkról rendszeresen biztonsági mentést kell készíteni.

A rendszergazda felelős a mentések elkészítéséért, ellenőrzéséért, tárolásáért és a kapcsolódó nyilvántartások vezetéséért. Ha az informatikai rendszer mentéseit nem közvetlenül maga a rendszergazda kezeli, hanem a központi mentőrendszer segítségével került megvalósításra, akkor a központi mentőrendszer rendszergazdájával egyeztetve az adatgazdák és a rendszergazda felelőssége a mentendő adatok körének, a mentések gyakoriságának meghatározása, és a központi mentőrendszer rendszergazdája gondoskodik a mentések kezelésének többi feladatáról.

A mentések során olyan eljárást kell alkalmazni, amely egyértelműen biztosítja, hogy a mentés adathordozókra az adatok sértetlenül és visszaolvashatóan felírásra kerüljenek.

A mentések visszaállításához biztosítani kell a háttérkörnyezetet, annak érdekében, hogy a mentett adatok és szoftverek esetleges adattároló hiba, az informatikai rendszerek összeomlása vagy megsemmisülése esetén visszaállíthatóak legyenek.

7.35.1. Adatok mentése

Az informatikai rendszerben kezelt adatokról alapesetben naponta kell mentést készíteni. A napi mentéseken kívül hosszabb megőrzési idővel heti, havi (és amennyiben költséghatékonyan megvalósítható éves) mentéseket is kell végezni.

Az egyes informatikai rendszerekre, rendszerelemekre vonatkozóan a rendszergazda az Informatikai üzletmenet-folytonossági tervben rögzített, elvárt helyreállítási pontokat, az adatok éles/teszt jellegét, változási ütemét, valamint a mentés elkészítéséhez szükséges időt figyelembe véve előírhat a napi rendszerességtől eltérő (pl. napi többszöri, heti vagy havi) gyakoriságú mentéseket is.

7.35.2. Szoftverek, eseménynaplók, kapcsolódó dokumentációk mentése

Az informatikai rendszer telepítésekor a rendszergazdának mentést kell végeznie a rendszerről, amit minden konfigurációváltoztatáskor és a változáskezelés hatálya alá eső, a rendszer működését befolyásoló beavatkozáskor ismételten el kell végeznie. Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

Az alkalmazói szoftverek környezetének, az alap informatikai szolgáltatásokat megvalósító rendszereknek (alaprendszereknek) a biztonsági mentéséről a kijelölt rendszergazdáknak kell gondoskodniuk.

A mentésnek ki kell terjednie az alábbi aktív hálózati eszközökre és szerver funkciókra is:

a) aktív hálózati eszközök (switch-ek, router-ek, és vezeték nélküli hozzáférési pontok) konfigurációs beállításai;
b) tűzfalak szabálylistája;
c) központi címtár adatbázisa;
d) DNS szerverek adatbázisa;
e) központi levelezés;
f) központi weboldalak.

A biztonsági események utólagos kivizsgálása érdekében gondoskodni kell az informatikai rendszer eseménynaplóinak mentéséről. Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

Az informatikai rendszerhez kapcsolódó dokumentációk, szabályzatok, eljárásrendek mentéséről is gondoskodni kell. A kapcsolódó dokumentációk mentését minden egyes változtatás esetén el kell végezni. Technikailag ezeket a mentéseket az adatok mentésével együtt kell végezni.

7.35.3. Archiválás

Az adattárolók helytakarékos használatához szükség lehet a ritkán használt vagy használaton kívüli, meghaladottá vált, de nem selejtezhető adatok, szoftverek archiválására, azaz hosszú távú megőrzés céljából adathordozóra írására és törlésére az elsődleges adattárolóról.

Az informatikai rendszerek rendszergazdái archiválást végezhetnek a következő adatokra vonatkozóan:

a) informatikai rendszerek bevezetése, migrációja kapcsán keletkezett adatok;
b) szoftverfrissítések vagy egyéb változásokkal kapcsolatos telepítő állományok, funkcionális mentések;
c) kilépett munkatársak mentett adatai;
d) folyamatosan keletkező naplófájlok, felhasználói lekérdezések;
e) egyéb felhasználói igények alapján meghatározott adatok.

Az alkalmazói rendszerek kivezetésével kapcsolatos archiválást a rendszer adatgazdájával egyeztetve lehet elvégezni. Az informatikai rendszerrel kapcsolatos archiválási igényeket a rendszer adatgazdájának vagy kulcsfelhasználójának a rendszergaztától kell igényelni.

7.35.4. Adatok hosszú távú megőrzése

Az Iratkezelési Szabályzatban és a vonatkozó jogszabályokban előírtak alapján a megőrzési idők teljesülése érdekében a következő előírásokat kell alkalmazni:

a) a napi mentések megőrzési ideje minimum 1 hét;
b) a heti mentések megőrzési ideje minimum 1 hónap;
c) a havi mentések megőrzési ideje minimum 6 hónap;
d) az éves és az archív mentéseket 8 évig kell megőrizni;
e) a számlázási adatok az éles számlázási rendszerekből 8 évig nem törölhetőek;
f) bizonyos munkaügyi adatokra vonatkozó megőrzési idő került megállapításra, ezért munkaügyi, bér- és társadalombiztosítási adatok nem törölhetőek az éles munkaügyi rendszerekből.

Az adatgazda feladata arról gondoskodni, hogy a jogszabályok által előírt adatok, informatikai rendszerektől független, hosszú távon olvasható formátumban (pl. PDF) exportálásra kerüljenek a munkaügyi rendszerekből, hogy az adatok a rendszerek kivezetése után is hozzáférhetők maradjanak. Az egyes informatikai rendszerekben tárolt adatok (különösen a személyes adatok) megőrzési ideje rövidebb lehet a rendszerről készült mentések fenti hosszú távú megőrzési idejénél. A rendszerek központi mentőrendszerrel történő csoportos mentése és az adattárolási mód technikailag nem teszi lehetővé a lejárt megőrzési idejű adatok mentésből történő eltávolítását, ezért a visszaállítást követően kell a kulcsfelhasználóknak gondoskodni arról, hogy a visszaállított adatok közül törlésre kerüljenek a már nem tárolható adatok. A kulcsfelhasználónak dokumentáltan és visszakereshető módon meg kell őriznie azokat az adattörléseket, amikor lejárt megőrzési idejű adatok, vagy az adatkezelés jogalapjának megszűnésével (pl. egy érintett visszavonta hozzájárulását a személyes adatai kezeléséhez) már nem tárolható adatok törlésre kerültek a rendszerből, és a mentés visszaállítása után a dokumentumok alapján újra el kell végezni az adattörlést a visszaállított adatokon.

7.35.5. Mentés adathordozók tárolása, kezelése

A mentések adathordozóit biztonságos környezetben, elzárva kell őrizni. A napi mentések kivételével a többi mentés adathordozóit az eredeti adatokat tartalmazó szerverteremtől eltérő helyszínen (lehetőség szerint eltérő telephelyen, de legalább eltérő épületben) kell tárolni.

Az adathordozókat egyedi azonosítóval kell ellátni, nyilván kell tartani és visszakereshető formában kell tárolni.

A központi mentőrendszerre vonatkozóan az elvégzett mentési feladatok és a mentés adathordozók tartalmának tételes nyilvántartása elektronikus formában, a mentést végző szoftver által történik. A szoftver belső adatbázisa tartalmazza továbbá a mentési feladatok időzítését, beállításait is. Mindezek miatt a mentőszoftver adatbázisát is rendszeresen menteni kell a többi informatikai rendszer mentésével együtt.

7.35.6. A mentési rendszer dokumentálása

A mentések rendszerét az Informatikai katasztrófa-elhárítási terv mellékleteként kell dokumentálni (ld. 7.2.2. Informatikai katasztrófa-elhárítási terv (DRP terv).

A mentési rendszer dokumentációjának célja, hogy a mentések visszaállításához információval szolgáljon a rendelkezésre álló mentésekre vonatkozóan; biztosítsa a mentőrendszer személyektől független üzemeltetését; valamint a mentőrendszer összeomlása esetén újra lehessen telepíteni a rendszert.

A dokumentációnak tartalmaznia kell:

a) a mentéseket megvalósító mentési feladatokat (mentés job-okat);
b) a mentés módját (milyen eszközzel, milyen adathordozóra történik a mentés);
c) a mentés típusát (teljes mentés vagy csak az utolsó teljes mentés óta történt változásokat tartalmazó különbségi mentés);
d) a mentés tartalmát (a mentendő adatok helyét);
e) a mentések gyakoriságát (napi, heti, havi), indulási idejét;
f) a mentések megőrzési idejét;
g) a mentési feladat által mentett adatmennyiséget és a mentés időtartamát (a szükséges adathordozók mennyiségének meghatározásához és a különböző mentési feladatok időzítésének összehangolásához);
h) a mentési feladatokat megelőző feladatokat (pl. az adatbáziskezelő szoftver által a szerver háttértárjára végzett mentéseket, amelyet a mentési feladat ír ki a mentés adathordozókra) és ezek időzítését;
i) a mentőszoftver használatát (a mentés elkészítésének és a mentett adatok visszaállításának rövid, szabatos leírását).

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

Az informatikai erőforrásokat érintő katasztrófa esetén az Informatikai üzletmenet-folytonossági tervben és az Informatikai katasztrófa-elhárítási tervben szereplő lépések végrehajtásával kell visszaállítani a normál (vagy a rendszer teljes visszaállításig a csökkentett funkcionalitású) működést (ld. 7.2. Üzletmenet-folytonossági terv). A kiemelten fontos hardver eszközökre vonatkozóan külső partnerekkel is köthető támogatási szerződés, hogy az eszközöket megadott időn belül kijavítsák, vagy helyettesítésükről gondoskodjanak.

Egyes kiemelten fontos hardver eszközökre, rendszerekre külső partnerrel köthető támogatási szerződés, ilyen esetben a szerződésben kell rögzíteni a helyreállításra vonatkozó elvárásokat.

A rendszergazdának gondoskodnia kell az informatikai rendszerek helyreállításához szükséges mentések meglétéről, elérhetőségéről (ld. 7.35. Az elektronikus információs rendszer mentései). A mentési és visszaállítási eljárások úgy kerültek kialakításra, 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. Biztosítania kell, hogy az üzemidő-kiesés, adatsérülés és adatvesztés oly mértékű legyen, amely a Hivatal által meghatározott elfogadható kockázati értéken belül marad.

8. AZONOSÍTÁS ÉS HITELESÍTÉS

8.1. Azonosítási és hitelesítési eljárásrend

A hitelesítés az informatikai rendszerekbe bejelentkező felhasználók személyazonosságának ellenőrzésére szolgál, és alapját képezi a rendszerekhez történő hozzáférések ellenőrzésének. A Hivatal jelen fejezet szerint gondoskodik arról, hogy a felhasználók mindegyike egyedileg legyen azonosítva és hitelesítve, valamint egyedileg legyenek azonosítva és hitelesítve a felhasználók által végzett tevékenységek

8.2. Azonosítás és hitelesítés

Az informatikai rendszerekben egyedileg kell azonosítani és hitelesíteni a Hivatal valamennyi belső felhasználóját, ami lehetővé teszi, hogy egyénileg nyomon lehessen követni a felhasználók által végzett tevékenységeket, ezáltal elkerülhetővé válhatnak a jogosulatlan hozzáférések, csökkenthetőek a jogosulatlan hozzáférésekből származó információbiztonsági incidensek. Ennek érdekében az alkalmazott névkonvenció alapján a felhasználóknak egyedi, névre szóló felhasználói azonosítókat kell képezni. A csoportos vagy szerepkör alapú azonosítók használata nem engedélyezett. Ez fokozottan vonatkozik a kiemelt jogosultságokkal rendelkező, rendszergazda felhasználók fiókjaira.

Azon hardver eszközök esetén, amelyek nem képesek egyedileg azonosítani a felhasználót, a beépített rendszergazdai fiókok használata a 2.2. Fiókkezelés és a 8.22.6. Beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelése pont szerint engedélyezett

8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése

A kiemelt jogosultságokkal rendelkező, ún. privilegizált felhasználók (rendszergazdák) hálózati és távoli bejelentkezésére többtényezős hitelesítést kell alkalmazni. Azon rendszerek esetén, amelyek nem támogatják a többtényezős hitelesítést, ott egyéb intézkedésekkel, technikai megvalósítással kell garantálni a biztonságot.

A többtényezős hitelesítés két különböző módszerrel kell, hogy történjen. A hagyományos jelszavas hitelesítés mellett a második tényező lehet pl. egy titkosító kulcs birtoklása (tárolhatja szoftver vagy hardver token); egy biometrikus azonosító (pl.: ujjlenyomat, írisz, érminta); vagy egy mobiltelefonra SMS-ben küldött egyszer használatos jelszó.

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

Az informatikai rendszerekben olyan hitelesítési mechanizmusokat lehet alkalmazni mind a privilegizált, mind a nem-privilegizált fiókok esetében, amelyek biztosítják a visszajátszás elleni védelmet. A visszajátszás elleni védelem biztosítása érdekében naplózást és monitorozást kell alkalmazni, hogy észlelni lehessen a visszajátszásos támadásokat és reagálni lehessen rájuk.

8.14. Azonosító kezelés

A felhasználói azonosítókat a rendszergazda kezeli. Az azonosítókat úgy kell létrehozni, hogy azok egyértelműen hozzárendelhetőek legyenek a kívánt személyhez (vagy szoftverek/hardver eszközök által használt technikai felhasználói fiókok esetén a kívánt rendszerelemhez).

Az azonosítók ismételt felhasználása 6 hónapig tilos (ennek biztosítására a megszűnt jogviszonyú felhasználók fiókjai 6 hónap után törölhetők). Azonos nevű felhasználók esetén a felhasználói azonosítókat sorszám kiegészítéssel kell megkülönböztetni, abban az esetben is, ha az egyik felhasználói fiók már inaktív.

Azokban az informatikai rendszerekben, amelyekben lehetőség van az inaktív felhasználói fiókok letiltására, be kell állítani, hogy a rendszer 1 év inaktivitás után – illetve, ha egy újonnan létrehozott felhasználói fiókba 6 hónapig nem jelentkeztek be - automatikusan tiltsa le a fiókot. Valamint hasonló módon le kell tiltani az 1 éve a hálózatra nem csatlakozó munkaállomásokat is.

Az inaktivitás következtében vagy más okból letiltott felhasználói fiókokat és a letiltott munkaállomásokat csak a közvetlen vagy felettes munkahelyi vezetőtől érkező írásbeli kérelem alapján lehet feloldani (ld. 2.1.Hozzáférés-felügyeleti eljárásrend).

A kiosztott felhasználói azonosítókat a rendszergazda a hozzáférési jogosultságok nyilvántartásában vezeti, amely minimálisan az alábbiakat tartalmazza:

a) a felhasználó nevét és a Hivatal munkavállalói esetén a dolgozói törzsszámát;
b) külső felhasználók esetén a szervezet nevét;
c) a felhasználói azonosítót;
d) az informatikai rendszert / rendszerelemet, amelyre a hozzáférési jogosultság vonatkozik;
e) a felhasználói fiók állapotát (aktív vagy letiltott).

A nyilvántartás a különböző informatikai rendszerekhez / rendszerelemekhez felvett hozzáférési jogosultságok nyilvántartására bevezetett informatikai rendszer (továbbiakban: jogosultság nyilvántartó rendszer) segítségével, elektronikus módon is megvalósítható.

8.21. A hitelesítésre szolgáló eszközök kezelése

A hitelesítésre szolgáló eszközök (pl.: jelszavak, hardver tokenek, biometrikus azonosítók) a felhasználók informatikai rendszerekhez, szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A Hivatal az informatikai rendszereihez való illetéktelen hozzáférés megakadályozására alapvetően jelszavas védelmet alkalmaz. A rendszergazdák többtényezős hitelesítésére második tényezőként szolgáló eszköz a rendszergazdához tartozó mobiltelefon és SIM kártya, vagy hitelesítésre szolgáló tanúsítvány (ld. 8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése pont.

Az informatikai rendszerekben használt jelszavak kiválasztására, továbbítására, tárolására és megváltoztatására vonatkozó követelményeket a 8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés pont tartalmazza.

Az ASP rendszer kétfaktoros azonosítást alkalmaz:

a) jelszó (tudás) alapú hitelesítést,
b) birtoklás alapú (token) hitelesítés

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

Az elektronikus ügyintézéshez szükséges a Központi Azonosítási Ügynökön keresztüli azonosítás:

a) Ügyfélkapu+: olyan kétfaktoros azonosítási szolgáltatás, amely lehetővé teszi, hogy a felhasználó biztonságosan léphessen kapcsolatba az elektronikus közigazgatási ügyintézést nyújtó szervezetekkel
b) Digitális Állampolgárság Program, DÁP

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

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

8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítania a megfelelő színvonalú jelszavak használatát. Az informatikai rendszerekben használt jelszavak kiválasztására, továbbítására, tárolására és megváltoztatására vonatkozó követelményeket jelen eljárás tartalmazza.

A gyakran használt, könnyen kitalálható, vagy korábban kompromittált jelszavakról és ezek használatának tilalmáról a biztonságtudatossági képzés keretében kell a felhasználókat tájékoztatni. Ha az informatikai rendszerek technikailag támogatják a tiltott jelszavak figyelését, akkor a rendszergazdáknak be kell állítaniuk a rendszerekben ezek kiválasztásának tiltását.

8.22.1. Informatikai rendszerek jelszókezelésének követelményei

A Hivatalnál csak olyan informatikai rendszer használható, amely:

a) lehetővé teszi a felhasználók számára jelszavuk kiválasztását és megváltoztatását;
b) megköveteli a felhasználók bejelentkezését a jelszó megváltoztatásához;
c) interaktív módon kikényszeríti a megfelelő minőségű jelszavak használatát;
d) beíráskor nem jeleníti meg a jelszavakat a képernyőn;
e) a jelszavakat a kilens és a szolgáltatást nyújtó szerver között titkosítva továbbítja;
f) a jelszavakat titkosítva tárolja (vagy nem tárolja, mert a hitelesítést egy másik rendszer/alrendszer pl. az operációs rendszer végzi biztonságos módon).

8.22.2. Kezdeti jelszavak kezelése

A felhasználók első belépését lehetővé tévő kezdeti jelszavak létrehozása és felhasználóknak történő átadása az alábbi módon történik:

a) A felhasználói azonosítókat az informatikai rendszer kijelölt rendszergazdája hozza létre oly módon, hogy kezdeti jelszót állít be a felhasználó részére.
b) A felhasználók kezdeti jelszavát a jelszó kiválasztására vonatkozó szabályok betartásával véletlenszerűen kell generálni (ez történhet manuális módon vagy az informatikai vezető által engedélyezett szoftverrel/szolgáltatással). A kezdeti jelszavaknak nem kell megjegyezhetőnek lenniük (ezzel is ösztönözve a felhasználót a jelszó lecserélésére), viszont a könnyebb szóbeli közölhetőség érdekében a manuálisan generált jelszavaknál annyi engedményt tehető, hogy az azonos típusú karakterek (kisbetű, nagybetű, szám) lehetnek egymás után csoportosítva (pl. „voptSKHB4283").
c) Minden felhasználónak egyedi kezdeti jelszót kell generálni, azaz nem lehet ugyanazt a jelszót adni több felhasználónak.
d) Az alábbi módszerek valamelyikével biztosítani kell, hogy a kezdeti jelszavak biztonságos körülmények között kerüljenek a felhasználóknak átadásra:
   - személyesen átadva;
   - személyes használatú mobiltelefonra SMS-ben elküldve (pl. ha még nincs e-mail címe);
   - a rendszergazda által engedélyezett, a jelszó egyszeri megtekintését, adott ideig (pl. 7 nap) lehetővé tévő rendszer (pl. https://onetimesecret.com) által generált link (továbbiakban: egyszer használatos jelszó link) használatával személyes használatú e-mail címre elküldve (pl. ha egy külső felhasználónak csak az e-mail címe ismert). A rendszer nem tartalmazhat információt arról, hogy a jelszó mire vonatkozik.
   - személyes használatú, a rendszergazda által üzemeltetett „belső" e-mail címre, a belső hálózaton elküldve. Belső e-mail címre elküldhető egy levélben a felhasználói név és a kódolatlanul a jelszó, külső e-mail címre viszont csak a felhasználói név küldhető, a jelszót más csatornán pl. SMS-ben vagy egyszer használatos jelszó link használatával kell elküldeni;
   - lezárt jelszó értesítő borítékban átadva (pl. új rendszer bevezetése esetén jelszavak tömeges generálásakor). A boríték átadható a felhasználói fiókot igénylőnek vagy a HR szervezetnek is.
e) A felhasználónak a kezdeti jelszavukat az első belépés során meg kell változtatniuk.

8.22.3. Jelszavak kiválasztásának követelményei

A jelszó minél komplexebb, annál kisebb a valószínűsége, hogy a felhasználó nevében visszaélést követnek el. Ennek érdekében az alábbi szabályokat kell a jelszó kiválasztásakor betartani:

a) a jelszó legyen legalább 10 karakter hosszú és tartalmazzon kisbetűt, nagybetűt és számot;
b) legyen könnyen megjegyezhető és nehezen kitalálható;
c) ne legyen a felhasználói névre vagy a Hivatal nevére, adataira (pl. irányítószám) utaló;
d) semmi olyasmi felhasználóhoz kötődő adaton ne alapuljon, amely alapján valaki kitalálhatja (ilyenek a nevek, telefonszámok, születési dátumok, lakcímek, stb.);
e) ne tartalmazzon bármilyen nyelvű szót szótári alakban;
f) ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl.: 123456, qwerty, asdfgh, stb.).

A felhasználói fiókok jelszókezelését a 2.1.9. A jelszókezelés követelményei pont tartalmazza.

8.22.4. Jelszavak rendszeres megváltoztatása

A jelszavakat meghatározott időnként meg kell változtatni. Erre vonatkozóan az alábbi szabályokat kell alkalmazni:

a) a jelszavakat maximum 180 naponta meg kell változtatni (a felhasználó saját elhatározásból ennél gyakrabban is megváltoztathatja a jelszavát);
b) az előző 3 jelszó nem használható újra;
c) a jelszavakat egy napon belül nem lehet többször megváltoztatni (az utóbbi két szabály célja, hogy megnehezítse a jelszóváltoztatás kényszerének megkerülését és a korábbi jelszó beállítását).

A jelszavak helyes kiválasztására és rendszeres megváltoztatására vonatkozó szabályok az informatikai rendszerek által technikailag kikényszeríthető részét a rendszergazdának be kell állítaniuk a rendszerekben.

8.22.5. Felhasználók felelőssége a jelszóhasználat során

Minden felhasználó felelőssége, hogy a jelszavak használata során betartsa a következő jelszavak védelmére vonatkozó szabályokat:

a) A felhasználói azonosító létrehozásakor (vagy a jelszó elfelejtése miatt) beállított kezdeti jelszót az első bejelentkezéskor meg kell változtatni.
b) A jelszó kiválasztásakor be kell tartani a jelszavak képzésére vonatkozó szabályokat, és a jelszavakat meghatározott időnként meg kell változtatni (ld. Jelszavak rendszeres megváltoztatása).
c) A felhasználó a jelszavát köteles titokban tartani, a jelszót tilos leírni, tilos nyilvános helyen kiírva (pl. monitorra ragasztva) tartani vagy másnak továbbadni.
d) A jelszót a rendszergazdának sem szabad elárulni. Ha a munkaállomások vagy egyéb eszközök karbantartásához szükség van a felhasználó jelszavára, a karbantartást végző csak a jelszó felhasználó általi beírását kérheti. Ha a munkaállomások telepítésével/beállításával kapcsolatban elkerülhetetlen a felhasználói jelszó ismerete, viszont a felhasználó nincs jelen, hogy beírja a jelszót, akkor sem lehet a felhasználótól bekérni a jelszavát, hanem a felhasználóval egyeztetve új kezdeti jelszót kell számára beállítani, amelyet a következő belépéskor meg kell változtatnia.
e) Ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott vagy feltételezhető a megismerése, azonnal meg kell változtatni a jelszót, és az esetet jelenteni kell a 9.27. A biztonsági események jelentése pontban leírtak szerint;
f) A jelszó nem tehető egy automatikus bejelentkezési folyamat részévé (pl. makróra, vagy funkcióbillentyűre).
g) A Hivatalnál használt jelszavak szervezeten kívüli rendszerekben nem használhatóak.

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerekben.

8.22.6. Beépített rendszergazdai- és a technikai felhasználói fiókok jelszavának kezelése

A beépített adminisztrátori- és a technikai felhasználói fiókok jelszavának kezelésére vonatkozó előírások:

a) A szoftverek és hardver eszközök telepítése után a beépített rendszergazdai fiókok gyárilag vagy szállító által beállított alapértelmezett jelszavát meg kell változtatni.
b) A technikai felhasználói fiókok jelszavának lejáratára vonatkozóan nem szabad érvényességi időt beállítani, mert ez a fiókot használó szoftver/szolgáltatás leállásához vezethet. Ezen jelszavak cseréjéről a kijelölt rendszergazdáknak kell gondoskodniuk (pl. a jelszó kompromittálódása esetén).
c) A beépített rendszergazdai- és a technikai fiókok jelszavára a normál felhasználói fiókoktól szigorúbb követelmények érvényesek, az eszközök beállítási lehetőségeit is figyelembe véve a jelszó minimális hossza 12 karakter és tartalmaznia kell kisbetűt, nagybetűt, számot és speciális karaktert.
d) A beépített rendszergazdai- és technikai fiókok jelszavát véletlenszerűen kell generálni, azaz a jelszavaknak nem kell megjegyezhetőnek lenniük (ugyanis a beépített rendszergazdai fiókok helyett a névre szóló rendszergazdai fiókok használatára kell törekedni, és a technikai fiókok esetén a szolgáltatásoknak, eszközöknek mindegy, hogy milyen jelszóval működnek).
e) Minden beépített rendszergazdai- és technikai fióknak egyedi jelszót kell generálni, azaz tilos a jelszavakat több helyen is újra felhasználni!
f) A jelszavakat az erre a célra bevezetett központi jelszókezelő rendszerben kell rögzíteni, illetve egy katasztrófahelyzetben kulcsfontosságú jelszavakat papíralapú formában, lezárt borítékban, felbontást gátló módon, aláírva is el kell helyezni, és a borítékokat a jegyző által meghatározott helyen elzárva kell tárolnia. A jelszó borítékokról nyilvántartást kell vezetni. A jelszó borítékok elhelyezése, felülvizsgálata vagy megsemmisítése során az informatikai rendszerek kijelölt rendszergazdáinak a feladata a rendszerükhöz tartozó jelszó borítékokra vonatkozóan a nyilvántartás aktualizálása.
g) A központi jelszókezelő rendszerhez történő hozzáféréshez a benne tárolt kritikus adatok miatt többtényezős hitelesítést kell alkalmazni. A rendszernek alapvetően a belső hálózatból szabad elérhetőnek lennie, külső helyszínről csak szervezeti tulajdonú hordozható számítógéppel, VPN-en keresztül (szintén többtényezős hitelesítéssel) csatlakozva megengedett az elérése.
h) A központi jelszókezelő rendszerben lévő jelszavakról havonta titkosítással védett exportot kell készíteni, amelyet az Informatikai katasztrófa-elhárítási tervet tartalmazó merevlemezeken, a DRP terv mellékleteként kell tárolni.
i) A központi jelszókezelőn, a leborítékolt jelszavakon és a jelszó exporton kívül a jelszavakat tilos máshol tárolni (pl. notesz, titkosítatlan dokumentumok, felhő tárhely, stb.). A jelszavak titkos minősítésű adatok, amelyeket tilos a Hivatalból bármilyen módon (pl. e-mail, magáncélú felhő tárhely, magántulajdonú adattároló) kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.
j) A jelszavak megtekintését minden esetben naplózni kell, a központi jelszókezelő rendszer és az Active Directory esetén a rendszer által elektronikus módon, a lezárt borítékok, illetve a jelszó export esetén manuális módon. A borítékok felbontását, illetve a jelszó export megtekintését az informatikai vezető vagy akadályoztatása esetén az informatikai területi vezetők engedélyezik.
k) A jelszavakhoz csak a rendszergazda férhet hozzá a feladatellátása szerint. A jelszavakat (pl. a munkaállomások helyi rendszergazdájának jelszavát) a felhasználóknak kiadni tilos! A jelszót azonnal meg kell változtatni, ha a felhasználó tudomására jutott.
l) A rendszergazda jogviszonyának megszűnésével vagy munkaköre változása esetén meg kell változtatni a rendszergazda által hozzáférhető beépített rendszergazdai fiókok jelszavát (különös tekintettel a távolról hozzáférhető rendszerekre).

8.22.7. A többtényezős hitelesítésre szolgáló eszközök, tanúsítványok kezelése

A rendszergazdák többtényezős hitelesítésére második tényezőként szolgáló mobiltelefon és SIM kártya (továbbiakban: eszközök) kezelésére az alábbi előírások vonatkoznak:

a) Többtényezős hitelesítésre elsősorban - amennyiben a felhasználó számára biztosított - csak a Hivatal tulajdonában lévő eszközök használhatók.
b) A munkatársak használatába adott eszközökről nyilvántartást kell vezetni (ld. 6.36. Rendszerelem leltár). Az eszközök kiadását, visszavonását, elvesztését, eltulajdonítását dokumentálni kell.

c) Az eszközök többtényezős hitelesítésre történő beállítását, illetve ennek visszavonását a többtényezős hitelesítést kezelő rendszer kijelölt rendszergazdája végzi.
d) A munkatársaknak védeniük kell az eszközöket az illetéktelen hozzáféréstől (képernyő mintával, PIN kóddal vagy ujjlenyomattal), illetve az eltulajdonítástól. Az eszköz többtényezős hitelesítésre történő használatának visszavonása érdekében azonnal jelenteniük kell az eszközök elvesztését vagy eltulajdonítását (ld. 2.113. Mobil eszközök hozzáférés-ellenőrzése).
e) A munkatársak jogosultságának változásakor (pl. áthelyezés, kilépés) vagy az eszközök változásakor (pl. csere, elvesztés, eltulajdonítás) gondoskodni kell a többtényezős hitelesítés módosításáról, illetve visszavonásáról.

A többtényezős hitelesítésre szolgáló tanúsítványok kezelésére vonatkozóan a 17.49. Kriptográfiai kulcs előállítása és kezelése pontban leírtak szerint kell eljárni.

8.36. Hitelesítési információk visszajelzésének elrejtése

Csak olyan informatikai rendszer használható, amely a hitelesítési folyamat során hibás azonosító vagy jelszó megadása esetén csak olyan hibaüzenetet ad vissza, amelyből nem szerezhető további információ sem az azonosítóra, sem a jelszóra vonatkozóan (pl.: nem derülhet ki az üzenetből, hogy a próbált azonosító érvényes, csak a jelszó hibás; vagy nem tartalmazhatja az üzenet a jelszó hosszára vagy bonyolultságára vonatkozó előírásokat).

8.37. Hitelesítés kriptográfiai modul esetén

Amennyiben a hitelesítés egy kriptográfiai modul (titkosítást végző hardver eszköz) felhasználásával történik, a modul használata során be kell tartani a hitelesítés szolgáltató által rendelkezésre bocsátott hitelesítési útmutatóban foglaltakat, jogszabályi, utasítási és szabványi előírásokat.

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

A Hivatal informatikai rendszereiben munkát csak olyan külső partner végezhet, aki érvényes szerződéssel rendelkezik, és a szerződés titoktartási kötelezettségvállalást és a Hivatal információbiztonsági előírásainak megismerésére és betartására vonatkozó kötelezettségvállalást tartalmaz (ld. 13.3. Viselkedési szabályok).

Külső személy az adatgazda engedélyével és irányításával, valamint a jegyző tudtával végezhet tevékenységet az informatikai rendszerben. Amennyiben a külső személynek az informatikai rendszeren rövid ideig tartó, nem tervezett beavatkozást kell végeznie, a munkát csak folyamatos felügyelet biztosításával végezheti. A folyamatos felügyelet biztosítása az informatikai rendszer adatgazdájának felelőssége.

Az informatikai rendszeren folyamatos vagy hosszabb feladat elvégzésére irányuló tevékenységet csak regisztrált, névre szóló felhasználói azonosítóval rendelkező külső felhasználó végezhet (ld. 8.36. Azonosítás és hitelesítés (szervezeten kívüli felhasználók). Ebben az esetben az informatikai rendszer adatgazdájának a rendszergazdától kell igényelnie a szükséges hozzáférést.

Az informatikai rendszeren történő munkavégzéshez külső felhasználó számára csak a szerződésben rögzített tevékenységhez szükséges, a legszükségesebb – és elégséges – jogosultságokat kell biztosítani és kifejezetten csak a munkavégzés idejére (a munka végén, vagy az előre meghatározott időtartam lejárta után a hozzáférést azonnal vissza kell vonni).

Külső felhasználóknak távoli hozzáférés csak indokolt esetben, az adatgazda tudtával biztosítható.

A külső felhasználóknak kiosztott felhasználói azonosítókat a rendszergazda a hozzáférési jogosultságok nyilvántartásában vezeti. A külső felhasználók tevékenységének a naplózására a 4.1. Naplózási eljárásrend alapján kiemelt figyelmet kell fordítani.

8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata

Amennyiben a szervezeten kívüli felhasználók hitelesítése nyilvános kulcsú titkosítási eljárással történik, a nyilvános kulcsot tartalmazó tanúsítványok csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott vagy a Hivatal által kiállított tanúsítványok lehetnek.

8.43. Újrahitelesítés

A munkaállomásokon a rendszergazdának tartományi szintű csoportházirend segítségével vagy helyi fiók-beállításokkal be kell állítania, hogy max. 15 perc tétlenségi idő után, jelszavas képernyővédő alkalmazásával automatikusan zárolódjon az eszköz. A munkaállomások felhasználó általi zárolását (eszközöktől történő fizikai távozás esetén) vagy automatikus időalapú zárolását követően a felhasználóknak újra hitelesíteniük kell magukat. Az automatikus zárolás beállítása alól kivétel képeznek azok a munkaállomások, amelyek rendeltetésük szerint információk (pl. kameraképek állapotának) állandó megjelenítésére szolgálnak.

9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

9.1. Biztonsági eseménykezelési eljárásrend

Az informatikai rendszerekben előforduló biztonsági események hatékony, gyors kezelése érdekében, illetve biztonsági események gyanúja esetén a jelen fejezetben meghatározott Biztonsági eseménykezelési eljárásrendet kell alkalmazni.

Az eljárásrendben szereplő főbb fogalmak:

a) Kiberfenyegetés: bármely olyan potenciális körülmény, esemény vagy cselekmény, amely károsíthatja vagy megzavarhatja a hálózati és információs rendszereket, az ilyen rendszerek felhasználóit és más személyeket, vagy azokra egyéb kedvezőtlen hatást gyakorolhat;
b) Kiberbiztonsági incidensközeli helyzet: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;
c) Kiberbiztonsági incidens: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;
d) Üzemeltetési kiberbiztonsági incidens: olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;
e) 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.

9.2. Képzés a biztonsági események kezelésére

A biztonsági események felismeréséhez és jelentéséhez szükséges általános felhasználói ismeretek átadásáról a biztonságtudatossági képzés keretében kell gondoskodni (ld. 3.2. Biztonságtudatossági képzés). Ezen túl az eseménykezelést végző szereplőket a biztonsági események kezelésével kapcsolatban külön képezni kell. A képzéseket a biztonságért Felelős tartja.

9.9. Biztonsági események kezelése

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 állasa, 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.

A jellemző biztonsági események a következők:

a) emberi mulasztás (dokumentált eljárások megszegése),
b) az informatikai rendszerekhez történő illetéktelen hozzáférés;
c) a rendszerekben kezelt adatok rendellenes megváltozása;
d) bizalmas adatok kiszivárgása, engedély nélküli nyilvánosságra hozatala;
e) kártékony programok általi fertőzés;
f) weboldalak megrongálása;
g) túlterheléses támadások (DoS, DDoS támadások);
h) informatikai eszközök elvesztése vagy eltulajdonítása;
i) a fizikai beléptetés kijátszása, illetéktelen személy bejutása az épületbe/védett területre.

Az eseménykezelés során elsődleges cél a normál működés lehető leggyorsabb helyreállítása és az üzleti folyamatokra gyakorolt káros hatás minimalizálása, ezért a lehető leghamarabb mérséklő intézkedésnek kell születnie. Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett eszközt le kell választani a hálózatról, illetve szükség esetén ki kell kapcsolni.

A bejelentés alapján a biztonságért Felelős feladata az esemény kivizsgálása és dokumentálása. A felelősnek javaslatot kell tennie a jegyző részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

9.25. A biztonsági események nyomonkövetése

Az informatikai rendszerek és kapcsolódó környezetük eseménynaplóinak vizsgálatával, valamint a kialakított hibakezelési eljárások hatékony működtetésével folyamatosan figyelemmel kell kísérni az informatikai rendszerekben bekövetkező biztonsági eseményeket. 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 a biztonságért Felelős részére.

A biztonsági események folyamatos figyelése és észlelés esetén azok jelentése, valamennyi munkatárs, szerződött fél felelőssége. A kiberbiztonsági incidenskezelő központtal való kapcsolattartás a biztonságért felelős feladata.

9.27. A biztonsági események jelentése

Az informatikai rendszerekkel kapcsolatba került minden személy köteles jelenteni, ha biztonsági problémát okozó jelenséget, biztonsági eseményt vagy erre utaló jelet észlel. Adatvédelmi és/vagy információbiztonsági incidens esetén az adatvédelmi tisztviselőnek, a biztonságáért Felelősnek, a jegyzőnek és a rendszergazdának egyeztetési, együttműködési feladata van az incidens kezelésében.

A felhasználók események bejelentésével kapcsolatosan elvárt eljárása:

1) Kártékony programok általi fertőzésre utaló jelek esetén a felhasználónak az adott számítógép hálózati csatlakozását azonnal meg kell szüntetnie (gyanús gépet szeparálnia szükséges) a hálózaton lévő többi eszköz védelme érdekében.
2) Informatikai jellegű probléma, biztonsági esemény vagy erre utaló jel észlelése esetén (pl. kártékony programok általi fertőzésre utaló szokatlan jelek, működés, a rendszerekben kezelt adatok rendellenes megváltozása, az informatikai rendszerekhez történő illetéktelen hozzáférés, weboldalak megrongálása, túlterheléses támadások) esetén késedelem nélkül értesítenie kell lehetőség szerint telefonon a rendszergazdát, megadva az észlelő nevét, a kapcsolódó informatikai rendszer megnevezését és a biztonsági esemény részletes leírását, majd követni kell a szóbeli utasításait.
3) A rendszergazda számára lehetőség szerint bizonyítékokat kell gyűjteni majd e-mailben elküldeni az észlelt eseményről, rögzíteni az eseményre utaló képernyőképet vagy hibaüzenetet és a tapasztalás helyét, idejét. A bizonyítékok megőrzése érdekében a felhasználók semmiféle kísérletet nem tehetnek az esemény kezelésére, a működést érintő hiba megszüntetésére vonatkozóan, amíg a pontos hibaüzenet, képernyőkép lementésre és elküldésre nem került vagy a rendszergazda a hibát nem látta.
4) A rendszergazdának szóban, majd az azonnali szükséges teendők elvégzése után haladéktalanul, legkésőbb a következő munkanap első órájában írásban is jelentenie kell az eseményt az illetékes adatgazdának, a jegyzőnek és a biztonságért Felelősnek.
5) Nem informatikai jellegű probléma, biztonsági esemény vagy erre utaló jel észlelése esetén (pl. emberi mulasztás, az informatikai rendszerekhez emberi mulasztásból eredő illetéktelen hozzáférés, bizalmas adatok kiszivárgása, engedély nélküli nyilvánosságra hozatala, informatikai eszközök elvesztése, eltulajdonítása vagy a fizikai beléptetés kijátszása, illetéktelen személy bejutása az épületbe/védett területre) az észlelőnek az illetékes adatgazdát kell elsőként értesíteni.
6) A jegyzőt és a biztonságért Felelőst az eseményről először tudomást szerző adatgazda értesíti a tudomására jutást követően késedelem nélkül, azt biztosítva, hogy a biztonságért Felelős a jegyző elérhetetlensége esetén is késedelem nélkül tudomást szerezzen a biztonsági eseményről.

7) Az adatgazda/jegyző akadályoztatása esetén az eseményt észlelőnek haladéktalanul közvetlenül a biztonságért Felelőst kell értesítenie a helyben szokásos leggyorsabb kommunikációs csatornán, elsődlegesen telefonon a gyors intézkedés érdekében, majd az esemény kivizsgálása érdekében rögzített dokumentumokat e-mailben is el kell küldeni.

A biztonságért Felelős feladata, hogy az elektronikus információs rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodjon a gyors és hatékony reagálásról, szükség esetén az illetékes kiberbiztonsági incidenskezelő központnak – adatvédelmi incidens gyanújának felmerülése esetén az adatvédelmi tisztviselőnek – való bejelentésről, a kiberbiztonsági incidensek kezeléséről, valamint a helyreállításról. Az önkormányzati ASP-t ért incidensek észlelését jelenteni kell az ASP Központ felé is a hibabejelentő rendszerben. A jelentés nem tartalmazhat olyan szenzitív adatot, elemeket, amelyet harmadik fél nem ismerhet meg.

9.27.1. A biztonsági esemény jelentése a Hivatal vezetője és az incidenskezelő központ felé

A biztonságért Felelős feladata, hogy a közvetlenül hozzá eljutott, az elektronikus információs rendszereikben bekövetkezett, illetve a tudomásukra jutott fenyegetéseket, kiberbiztonsági incidensközeli helyzeteket és kiberbiztonsági incidenseket – beleértve az üzemeltetési kiberbiztonsági incidenst is – haladéktalanul jelentse a jegyzőnek vagy a szükséges mértékig tájékoztassa arról, illetve jelentse a nemzeti kiberbiztonsági incidenskezelő központ részére az MK rendeletben meghatározottak szerint, a központ által meghatározott módon, elektronikus úton vagy elektronikus felületen. A nemzeti kiberbiztonsági incidenskezelő központ felé nem kell bejelenteni azt a nem ismétlődő kiberbiztonsági incidensközeli helyzeteket és üzemeltetési kiberbiztonsági incidenst, amely az incidenskezelési folyamatba kerülés során, automatizmus által kezelésre, elhárításra került és nem járt a szolgáltatás degradációjával, romlásával.

A biztonságért Felelősnek a kiberbiztonsági incidenskezelő központ felé a bejelentés keretében indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül első bejelentést kell tenni, amelyben – amennyiben az információk rendelkezésre állnak – fel kell tüntetni:

a) az érintett elektronikus információs rendszer megjelölését,
b) a kiberbiztonsági incidens rövid leírását, ennek keretében annak jelzését, hogy az incidens üzemeltetési kiberbiztonsági incidensnek minősül-e,
c) a kiberbiztonsági incidens státuszát,
d) a kiberbiztonsági incidens időtartamát,
e) ha becsülhető, a szolgáltatás helyreállításának várható időpontját,
f) a kiberbiztonsági incidens által érintett adatok fajtáját, jellegét,
g) a kiberbiztonsági incidens által érintett felhasználók számát,
h) a szolgáltatás működésében támadt zavar mértékét,
i) a kiberbiztonsági incidens kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,
j) közvetítő szolgáltató vagy központi szolgáltató igénybevétele esetén a közvetítő szolgáltató vagy központi szolgáltató megnevezését, elérhetőségét,
k) a kiberbiztonsági incidens szándékolt incidensnek minősül-e,
l) a kiberbiztonsági incidens által érintett terület földrajzi kiterjedését,
m) lehet-e a kiberbiztonsági incidensnek határokon átnyúló hatása,
n) minden olyan információt, amely lehetővé teszi a Központ számára, hogy meghatározza az esemény határokon átnyúló hatásait;

Amint rendelkezésre állnak, a fertőzöttségi mutatókat, majd indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja a már bejelentett információkat, és tartalmazza az incidens első értékelését, beleértve annak súlyosságát és hatását.

A Központ kérésére közbenső helyzetjelentést, majd zárójelentést, kell benyújtani legkésőbb az eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:

a) a kiberbiztonsági incidens részletes leírása, beleértve annak súlyosságát és hatását,
b) a kiberbiztonsági incidenst valószínűleg kiváltó fenyegetést vagy kiváltó ok típusát,
c) alkalmazott és folyamatban lévő mérséklési intézkedéseket,
d) adott esetben a kiberbiztonsági incidens határokon átnyúló hatását;

Ha a zárójelentés benyújtásának időpontjában még folyamatban van a kiberbiztonsági incidens, az addig elért eredményekről szóló jelentést, majd a kiberbiztonsági incidens kezelését követő egy hónapon belül egy zárójelentést kell benyújtani.

9.27.2. Természetes személyek adatait érintő adatvédelmi incidens jelentése

Amennyiben a biztonsági esemény személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását is érinti, a biztonságért Felelősnek haladéktalanul tájékoztatni kell erről a jegyzőt, akadályoztatása esetén közvetlenül az adatvédelmi tisztviselőt 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).

9.31. Segítségnyújtás a biztonsági események kezeléséhez

A felhasználók felé az információbiztonsági események kezeléséhez kapcsolódó információk és irányelvek megadása, tanácsadás és támogatás a rendszergazda közreműködésével biztonságért Felelős feladata. A támogatást a felhasználók szükség szerint igényelhetik. Szükség esetén a kiberbiztonsági incidenskezelő központ szakmai támogatást nyújt bejelentett incidenssel kapcsolatban, ill. a hasonló incidensek megelőzésében vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekben.

9.34. Biztonsági eseménykezelési terv

A biztonsági események kezelésére felkészülve Biztonsági eseménykezelési tervet kell kidolgozni, amely iránymutatást ad az események kezelési módjaira.

A tervnek tartalmaznia kell:

a) a bejelentésköteles biztonsági események meghatározását (példákkal az egyes esemény fajtákra);
b) a biztonsági események súlyosság szerint kategorizálásának módját;
c) az egyes a biztonsági események Hivatal szervezetéhez illeszkedő kezelésének módját (ahol előre meghatározható, ott konkrét eseménykezelési lépéseket megadva, egyébként átfogó megközelítést nyújtva);
d) a biztonsági eseményeket kezelő szerepköröket, ezek felelősségét, feladatait;
e) a biztonsági események belső mérésének, kiértékelésének módját (amely mérési eredményeket, tapasztalatokat fel kell használni a kockázatelemzésnél, az eseménykezelési terv felülvizsgálatánál és be kell építeni az információbiztonsági képzésekbe);
f) azon erőforrásoknak és vezetői támogatásnak a meghatározását, amelyek szükségesek a biztonsági eseménykezelési lehetőségek fenntartásához, illetve bővítéséhez, hatékonyabbá tételéhez.

A terv elkészítéséért és karbantartásáért – a rendszergazdával egyeztetve – a biztonságért Felelős felel, jóváhagyása a jegyző feladata.

A Biztonsági eseménykezelési terv bizalmas minősítésű dokumentum, amelyeket az eseménykezelésben érintett személyek, szervezeti egységek számára kell kihirdetni, akik illetékteleneknek nem adhatják tovább. A terv megismerésére és tárolására jogosult szereplők feladata gondoskodni arról, hogy a terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A tervet frissíteni kell, és legalább kétévente felül kell vizsgálni, figyelembe véve az informatikai rendszerek és a Hivatal változásait vagy a terv megvalósítása, végrehajtása során felmerülő problémákat. A terv változásairól tájékoztatni kell a tervekben érintett szereplőket.

10. KARBANTARTÁS

10.1. Karbantartási eljárásrend

A rendszeres karbantartás célja, hogy a Hivatal biztosítani tudja az ügymenethez szükséges eszközök és szolgáltatások zavartalan működését, hiba esetén időben történő javítását, melyre vonatkozóan jelen eljárásrendet kell alkalmazni.

10.2. Szabályozott karbantartás

A folyamatos működés biztosítása érdekében az informatikai rendszerek elemeit megadott rendszeres időközönként karban kell tartani. A hardver eszközök karbantartásának célja, hogy megelőzze az eszközök véletlenszerűen bekövetkező meghibásodását. Ilyen karbantartás lehet például:

a) az eszközök belső portalanítása;
b) az elhasználódó alkatrészek cseréje;
c) a nyomtatók mozgó és szennyeződő alkatrészeinek tisztítása;
d) a szünetmentes tápegységek akkumulátorának öntesztel történő ellenőrzése.

A szoftver elemek karbantartása során kell elvégezni azokat a szerver oldali rendszeres szoftverfrissítéseket, amelyek informatikai rendszerek vagy alapszolgáltatások leállításával járnak.

A karbantartásokat a gyártói ajánlások és a szoftverfrissítésekre vonatkozó előírások figyelembevételével kell végezni. A hálózati rendszer bővítését vagy átalakítását kizárólag a rendszergazda vagy a jegyző által ezzel megbízott külső partnerek végezhetik. Illetéktelen személy a kialakított hálózati rendszeren nem változtathat, hálózati végpontot nem helyezhet át, aktív hálózati eszközt vagy szerverfeladatokat ellátó eszközt a hálózatra nem kapcsolhat rá, a hálózat elemeit (pl.: fali aljzatokat, csatlakozókat, hálózati kábeleket stb.) nem bonthatja meg.

A hálózat működési biztonsága szempontjából alapvető jelentőségű a hálózat kábelezése, amelyre vonatkozóan a következőket kell figyelembe venni:

a) A hálózat tervezésénél, kiépítésénél strukturált felépítést kell alkalmazni.
b) A hálózat kiépítése során külön kábelcsatornában vagy tálcában kell haladniuk az áramellátást, illetve az adatkommunikációt biztosító vezetékeknek.
c) A kábeleket csatornán kívül vezetni – még ideiglenes megoldásként – sem szabad.

A karbantartandó eszközök körét és a karbantartás rendszerességét a biztonságért Felelős határozza meg az eszközök alkalmazási körülményeit és nagyságrendjét is figyelembe véve. Ha a karbantartandó eszközök nagyságrendje nem igényli, akkor döntése alapján mellőzhető az éves karbantartási terv készítése. Külső személy/szolgáltató esetén a karbantartások ütemezését és azok feltételeit a szerződésben kell rögzíteni.

A tervezett karbantartásokat a rendszergazda által készített, a jegyző által jóváhagyott éves karbantartási terv vagy a lenti szabályok alapján kell elvégezni.

A tervezett karbantartások mértékének és gyakoriságának meg kell felelni a gyártói előírásoknak és ajánlásoknak, de minimum évente egyszer szükséges elvégezni. A Hivatal az eszközparkot az alábbi gyakorisággal tartja, tartatja karban, ha más karbantartási tervben nem rögzített, akkor az alábbi szabályokat határozta meg:

1) számítógépek és szerverek: évenkénti karbantartás. Felelős: rendszergazda
2) számítástechnikai hálózat: évenkénti karbantartás és tesztelés. Felelős: rendszergazda
3) nyomtatók és egyéb eszközök: igény szerinti, de legalább évente. A nyomtatók, fénymásolók karbantartását eseti megbízás alapján vagy átalánydíjas szerződés alapján külső megbízott végzi.

A tervezett karbantartás keretein belül legalább éves gyakorisággal legalább alábbi feladatokat el kell végezni:

1) a hardver eszközök fizikai/mechanikai tisztítása portól és egyéb szennyeződéstől; amennyiben szükséges, egyéb karbantartási feladatok elvégzése, (pl. processzor hűtőpaszta csere),
2) logikai/szoftveres karbantartás (merevlemez töredezettség-mentesítés, felesleges/nem használt fájlok, szoftverek, esetleges kártevőket tartalmazó állományok törlése, hibaellenőrzés stb.);
3) szünetmentes tápegységek akkumulátorának öntesztel történő ellenőrzése;
4) szerveren/felhasználók munkaállomásain telepített alkalmazások megfelelőségének ellenőrzése, szoftverfrissítések ellenőrzése, szükség esetén elvégzése;

5) az informatikai hálózat, a számítógépek, informatikai eszközök biztonsági beállításainak ellenőrzése, (pl. tűzfal/router beállítások);
6) a felhasználóval és szükség esetén az adatgazdával az elmúlt év üzemeltetési tapasztalatainak elemzése, a nyilvántartások alapján az eszköz élettartama alatt elvégzett mechanikai és logikai intézkedések, javítások értékelése azért, hogy az eszközök élettartama és megbízhatósága megfelelő szinten maradjon, az esetleges csere és bővítés szükségességének megállapítása céljából;
7) a teljesítményjavítás, élettartam-növelés, a felhasználók munkáját vagy az informatikai biztonságot támogató fejlesztési lehetőségek feltárása, melyet Munkalapon vagy egyéb feljegyzésen is rögzíteni kell, azokról be kell számolni a jegyző és a biztonságáért Felelős felé.

Ha a karbantartás valamely informatikai rendszernek vagy szolgáltatásának a leállításával jár, akkor az érintett felhasználókat a karbantartás megkezdése előtt legalább 1 munkanappal korábban értesíteni kell. A szerverek karbantartását ütemezetten, lehetőség szerint munkaidőn kívül kell végrehajtani. A tervezett karbantartások alkalmával, vagy rendkívüli események, rendszerhibák kapcsán a jegyző korlátozhatja a hálózathoz, egyes hálózati szolgáltatásokhoz (alaprendszerekhez) vagy alkalmazói rendszerekhez történő hozzáféréseket.

A karbantartásokat és javítási munkákat csak arra felhatalmazott személy, külön engedély nélkül a rendszergazda végezhet, beleértve a hardver hibák felderítését és a speciális szakismeretet, szerszámokat és anyagokat nem igénylő hardver karbantartásokat, javításokat, valamint a speciális szakismeretet, szerszámokat vagy anyagokat igénylő karbantartásokat és javításokat is, melyekkel indokolt esetben a jegyző előzetes hozzájárulásával külső partnerek is megbízhatóak.

A rendszergazda által végzett karbantartások elvégzését Munkalapon vagy egyéb feljegyzésben kell dokumentálni, amely egyben az elvégzett karbantartások nyilvántartására is szolgál.

Külső karbantartó partnerek igénybevétele esetén a 10.18. Karbantartó személyek pontban leírtakat kell alkalmazni. A külső karbantartók által végzett karbantartások dokumentálására a külső partner által használt munkalap szolgál.

A munkalapok, feljegyzések megőrzése a jegyző által kijelölt helyen, ennek hiányában az irattárban történik.

Amennyiben a karbantartáshoz kapcsolódóan adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a 11.8. Adathordozók törlése pontban leírtak szerint kell eljárni. Ez az eljárás vonatkozik a nem javítható eszközöket selejtezése során is, melyek esetleges adattartalmát – szükség esetén véglegesen és helyreállíthatatlanul – törölni kell, a törlésről jegyzőkönyvet/munkalapot kell készíteni.

Az eszközök ki- és beszállításánál be kell tartani a vonatkozó szabályzatok rendelkezéseit. A kiszállítást a rendszergazda vagy az adott eszköz adatgazdája/jegyző engedélyezi.

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és szükség szerinti biztonsági tesztet kell végezni, sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe. Az eseményt jelenteni kell a jegyzőnek, aki a rendszergazdával és biztonságért Felelőssel közösen dönt a további intézkedésekről.

10.11. Távoli karbantartás

Távoli karbantartásnak nevezzük azt, amikor egy személy hálózat segítségével végez karbantartási munkát, függetlenül attól, hogy az külső vagy belső hálózaton történik (pl. VPN, távoli asztal, SSH hálózati kapcsolat segítségével).

A távoli karbantartásra a következő előírások vonatkoznak:

a) Távoli karbantartást csak névre szóló felhasználói fiókkal rendelkező, erre felhatalmazott, a karbantartáshoz szükséges hozzáférési jogosultságot kapott) személy végezhet.
b) A karbantartó személy bejelentkezéshez többtényezős hitelesítést kell alkalmazni (ld. 8.1. Azonosítási és hitelesítési eljárásrend).
c) A távoli karbantartás során naplózni kell a karbantartó személy által végzett műveleteket;
d) A távoli karbantartás végén szabályos módon ki kell jelentkezni a hálózati kapcsolatból.

Információbiztonsági szempontból elvárás a multifunkciós nyomtató üzemeltető részéről - pl. nyomatszám számláló, diagnosztikai állapotlekérés céljából - történő távoli elérés tiltása. Csak a helyszínen történő lekérdezés/ online bejelentő űrlap használata támogatott, erre kell törekedni, mert a fénymásoló hálózati sérülékenysége miatt a belső hálózat támadási felülete jöhet létre, ill. a szkennelt dokumentumokhoz való hozzáférésre kerülhet sor.

10.18. Karbantartó személyek

Abban az esetben, ha az informatikai rendszerek karbantartását a rendszergazda saját erőből nem tudja elvégezni, akkor a jegyzőnél kezdeményezi külső partner megbízását. Karbantartási tevékenységet csak olyan külső partner végezhet, aki érvényes szerződéssel rendelkezik, és a szerződés titoktartási kötelezettségvállalást, illetve a Hivatal Információbiztonsági előírásainak megismerésére és betartására vonatkozó kötelezettségvállalást tartalmaz. A külső partnerrel kötött szerződésben rögzíteni kell, hogy a karbantartást felügyelő munkatárs jogosult ellenőrizni a karbantartást végző személy jogosultságát.

A karbantartást végző külső partnerekről a Hivatalnak a biztonságért Felelős felügyeletével nyilvántartás kell vezetni (Külső karbantartók nyilvántartása), melynek minimálisan a következőket kell tartalmaznia:

a) a karbantartó szervezet megnevezését;
b) a szerződés tárgyát, hatályát (mely rendszerelemekre terjed ki);
c) a szerződés időtartamát;
d) a szerződés szkennelt változatát;

A külsős rendszergazdán kívüli külső partner munkavégzése esetén a rendszergazda vagy a jegyző által kijelölt felelősnek szükséges folyamatos felügyeletet biztosítania a karbantartás során. Külső karbantartók esetében - akár épület, akár eszköz karbantartási, vagy ellenőrzési célból érkeznek-, a Hivatalba történő belépéshez, a karbantartási, ellenőrzési feladatok ellátásához a személyazonosságot igazolni szükséges.

A kritikus biztonsági követelményű helyiségekbe érkező, állandó belépési engedéllyel nem rendelkezőket a jegyzőnek vagy az általa kijelölt személynek (informatikai jellegű esetekben a rendszergazdának) kísérnie kell és figyelemmel kell követnie a tevékenységüket. Az eszközök, rendszerek karbantartási munkálatait külső karbantartók esetében a rendszergazdának felügyelni szükséges, hogy kizárásra kerüljenek a jogosulatlan hozzáférések, illetve hibás karbantartási tevékenységek.

11. ADATHORDOZÓK VÉDELME

11.1. Adathordozók védelmére vonatkozó eljárásrend

A Hivatal jelen eljárásában rögzíti az adathordozók védelmére vonatkozó előírásait.

Az adathordozó használatára való igényt az adatgazdához/jegyzőhöz kell benyújtani. A rendeltetésszerű eszközhasználatot a Hivatal elektronikus információs rendszereihez történő csatlakoztatás után, a rendszergazda szúrópróbaszerűen ellenőrizheti. A munkavégzéshez a Hivatal tulajdonában lévő, nyilvántartott adathordozót lehet használni. Az adathordozókat a hardver nyilvántartás részeként (ld. 6.36.1. Hardver nyilvántartás) vagy adathordozók, hordozható informatikai eszközök nyilvántartásában kell nyilvántartani.

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

Az adathordozók információbiztonsági kezelésének általános irányelvei:

a) informatikai eszközöket, adathordozókat tilos nyilvános helyen vagy harmadik félnél történő munkavégzés során őrizetlenül hagyni;
b) munkavégzés közben nem lehet a használatban lévő mobil eszközöket felügyelet nélkül hagyni, a használaton kívüli eszközöket védett helyen kell tárolni („tiszta asztal" szabálya);
c) az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani nem lehet;
d) tilos az olyan hordozható adathordozó használata az elektronikus információs rendszerben, melynek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni;
e) az adathordozókat a felhasználók nem csatlakoztathatják egymás eszközeihez úgy, hogy az eszköz tulajdonosa nem tud róla;
f) amennyiben kívülről érkezik adat valamilyen adathordozón, annak a megtekintése a 11.14. Adathordozók használata pontban szereplő vírusellenőrzési folyamat után használható.

Az adathordozók védelme érdekében figyelemmel kell lenni valamennyi, az eszközökben lévő adathordozókra is. A merevlemezes tárolóval rendelkező multifunkciós nyomtató/fénymásoló eszközökön lévő, vagy azokra kerülő bizalmas adatok védelmére az eszköz a hivatal felügyelete alóli kikerülés, pl. szervizbe történő szállítás, visszaadása esetén az adathordozókra vonatkozó szabályoknak megfelelően kell eljárni.

Bármely adathordozó eltűnését azonnal jelenteni kell a 9.27. A biztonsági események jelentése pont alapján azzal az információval együtt, hogy milyen minősítésű dokumentum kompromittálódott. Az adathordozók védelme során figyelembe kell venni a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács (EU) 2016/679 rendeletét (GDPR). Ha személyes adatot tartalmazó, kriptográfiai védelemmel el nem látott adathordozó eltűnése, jogosulatlanokhoz jutása feltételezhető, akkor azonnal jelentést kell tenni az adatvédelmi tisztviselő felé is.

Az adathordozókat a hatályos Beszerzési Szabályzat szerint kell beszerezni.

A szoftverek telepítő állományainak fizikai védelme érdekében gondoskodni kell arról, hogy a telepítő adathordozók ne károsodjanak, ezért az eredeti példányukról másolatot kell készíteni (fizikai adathordozóra és/vagy hálózati megosztásra). Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni és a másolatokat kell a napi tevékenység során használni.

Az informatikai rendszerek részét képező informatikai eszközöket, adathordozókat, dokumentációkat olyan technikákkal és módszerekkel kell selejtezni, amely megakadályozza, hogy az informatikai rendszerből származó adatok illetéktelen személyek tudomására jussanak. Ennek érdekében a selejtezés során a 19.27. Rendszerelem selejtezése, megsemmisítése pontban leírtak szerint kell eljárni.

11.2. Hozzáférés az adathordozókhoz

Az informatikai rendszerekben csak a Hivatal tulajdonában lévő, regisztrált adathordozók használhatók. Nem a Hivatal tulajdonában lévő adathordozókat a Hivatal informatikai rendszereihez kizárólag a rendszergazda vagy az adatgazda tudtával és engedélyével lehet csatlakoztatni.

A Hivatalhoz újonnan belépő munkavállalók a munkahelyi vezető/adatgazda által előzetesen igényelt informatikai eszközöket az első munkanapjukon a munkavégzés helyszínén vagy a rendszergazdánál vehetik át. A munkaállomások és kapcsolódó perifériák esetében Üzembe helyezési / Átadás-átvételi jegyzőkönyv kerül kitöltésre, míg a mobiltelefonok, SIM kártyák, valamint a belépőkártyák esetén Átadás-átvételi bizonylaton/egyéb feljegyzésen kerül rögzítésre az átvétel.

Az engedélyezett adathordozó típusokat, az adathordozókhoz hozzáférő szerepköröket, a hozzáférés módját és célját az alábbi táblázat tartalmazza:

Adathordozó típus	Szerepkör	Hozzáférés / jogosítvány
Informatikai rendszerek szerver oldali háttértárai (merevlemez)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Szerver oldali, központi mentések adathordozói (szalagos adatkazetta, CD, DVD)	Rendszergazda	Fizikai, logikai / tárolás, mentés, visszaállítás
Munkaállomások háttértárai (merevlemez)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
	Felhasználó	Logikai / szerepkörének megfelelően
Munkaállomás mentések adathordozói (CD, DVD, pendrive, külső merevlemez)	Rendszergazda	Fizikai, logikai / karbantartás, mentés, visszaállítás
Adatszolgáltatások adathordozói (CD, DVD, pendrive, külső merevlemez)	Felhasználó, Külső partner	Fizikai, logikai / tárolás, adatszolgáltatás létrehozása, olvasása
Dokumentumok hálózattól független (offline) hozzáféréséhez használt adathordozók (pendrive, külső merevlemez)	Felhasználó	Fizikai, logikai / tárolás, dokumentumok létrehozása, olvasása
Rendszerelemek telepítő adathordozói (CD, DVD)	Rendszergazda	Fizikai, logikai / tárolás, telepítés
Vészhelyzeti terveket (Informatikai üzletmenet-folytonossági terv, Informatikai katasztrófa-elhárítási terv) és vészhelyzeti adatokat tároló adathordozók (CD, DVD, pendrive, külső merevlemez)	A vészhelyzeti tervekben megadott szereplők	Fizikai, logikai / a vészhelyzeti tervekben leírt műveletek elvégzése és a tervek karbantartása

11.8. Adathordozók törlése

Az adathordozók vagy adathordozót tartalmazó informatikai eszközök újrahasznosítása, mások rendelkezésre bocsátása vagy selejtezése előtt minden esetben gondoskodni kell arról, hogy az adathordozón tárolt adatok visszaállíthatatlanul eltávolításra kerüljenek.

Ennek érdekében helyreállíthatatlanságot biztosító törlési technikákkal törölni kell az adatokat (pl. mágneses elvű adathordozók esetén olyan szoftvert alkalmazásával, amely többszörösen felülírva törli az adatokat), vagy az adathordozót roncsolással fizikailag kell használhatatlanná tenni, megsemmisíteni.

Az adatok eltávolítását az adathordozók kezeléséért felelős munkatársak kérése bejelentés alapján a rendszergazda végzi. Az adatok eltávolításának tényét és módszerét az eltávolítást végző munkatársnak Munkalapon vagy jegyzőkönyvben dokumentálnia kell.

Számítógépek esetében, ha a javítás külső helyszínen történik, mentést követően, az elszállítást megelőzően a védett, személyes adatokat, információkat tartalmazó adattartalmat helyreállíthatatlanságot biztosító eljárással törölni, az el- és visszaszállítást pedig dokumentálni kell. A törlést abban az esetben nem szükséges végrehajtani, ha az elszállítandó berendezést a felhasználója vagy a rendszergazda kíséri és felügyeli a javítást, vagy ha az adathordozót kiszerelik és azt megfelelően biztonságos helyen helyben tárolják.

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

11.14. Adathordozók használata

Tilos belső használatú, bizalmas vagy titkos dokumentumokat, adatokat CD-n, DVD-n, pendrive-on, külső merevlemezen, elektronikus levélben, Interneten vagy bármilyen más módon a Hivatalból kijuttatni, illetéktelen személy részére hozzáférhetővé tenni. Nem tartozik e tilalom alá a hatósági adatszolgáltatás és a titoktartási kötelezettséggel védett szerződéses kapcsolatban álló személyekkel való kapcsolattartás.

Az adathordozók használatát, az informatikai rendszerhez történő csatlakoztatása után a Hivatal figyelheti, monitorozhatja, az adathordozók használatát információbiztonsági megfontolásból hardver, illetve szoftver úton korlátozhatja.

A szakfeladatokat támogató szakrendszerek munkaállomásain az adathordozók használatát az engedélyezett jogosultságoknak megfelelően kell beállítani, csak az azonosított, a felügyeletéért felelőshöz rendelt adathordozó használata engedélyezett. A Hivatal megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható. Az adathordozókat sorszámmal és/vagy a felügyeletéért felelős nevével azonosítani kell, azokat a felhasználóhoz kell rendelni.

Az adathordozókat mindig a gyártói előírásoknak (a csomagoláson vagy a kísérő dokumentációban leírtaknak) megfelelően kell kezelni. Az adathordozókat óvni kell mindenféle mechanikai hatástól (pl.: ütés, hajlítás, karcolás), mágneses elvű adathordozók esetén mágneses hatástól, egyéb külső hatástól (pl.: hő, maró anyagok, nedvesség), szennyeződéstől (pl.: por, korom). A védelemről a kezelésért, tárolásért felelős munkatársnak kell gondoskodnia. Az adathordozók nem megfelelő kezelése az adathordozón lévő adatok elvesztéséhez, illetve az adathordozót használó eszköz károsodásához vezethet.

A Hivatalhoz küldeményként érkezett adathordozókon (pl. CD/DVD/pendrive) minden esetben vírusellenőrzést kell végezni az iratok átvételi folyamatának részeként. A vírusellenőrzés előtt meg kell győződni arról, hogy az ellenőrzésre használt számítógép vírusvédelmi szoftvere friss, aznapi dátumú vírusdefiníciós adatbázissal rendelkezik, ugyanis az ellenőrzés csak friss adatbázissal végezhető. Az ellenőrzés eredményét (az adathordozó kártevő mentességét, illetve a talált kártevőket) az adathordozóhoz tartozó kísérőlapon írásban kell dokumentálni.

A vírusellenőrzést a rendszergazdán kívül végezhetik a rendszergazda útmutatója alapán a Hivatal azon munkatársai, akik a küldemények átvételét végzik. Amennyiben a vírusellenőrzést a Hivatal munkatársai végzik és nem frissül a vírusvédelmi szoftver vírusvédelmi adatbázisa vagy az ellenőrzés fertőzést jelez, akkor a frissítési hiba elhárítását, illetve a fertőzött adathordozó vírusmentesítését a rendszergazdától kell igényelni. Fertőzött és a vírusvédelmi szoftver által nem vírusmentesíthető adathordozókat tilos használatba venni, ezeket vissza kell juttatni a küldemény feladójának.

Hivatal a szakmai munkát segítő, CD/DVD adathordozókon megjelent és rendszeresen frissített adattárakkal (pl. Jogtárral) rendelkezhet. Az adattárakat és frissítéseiket a jegyző által kijelölt kezeli.

Az adattárak használatára az alábbiak vonatkoznak:

a) Az adattárakhoz egy időben csak adott számú felhasználó férhet hozzá a megvásárolt licenceknek megfelelően. A felhasználóknak az adattárak használatának befejezése után ki kell lépniük az adattárból, hogy mások is hozzá tudjanak férni.
b) Az adattárakból kinyomtatott, lementett információk (különösen a jogszabályok) nem ellenőrzött állapotba kerülnek, ezért felhasználás, alkalmazás, hivatkozás előtt meg kell győződni arról, hogy továbbra is érvényben vannak-e.
c) A rendelkezésre álló adattárakhoz a 2.1.2. Új hozzáférés igénylése pontban leírtak szerint kell hozzáférési jogosultságot igényelni.

12. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

12.1. Fizikai és környezeti védelemre vonatkozó eljárásrend

A fizikai védelmi intézkedések célja, hogy biztosítsák az informatikai rendszereknek helyt adó épületek, helyiségek fizikai védelmét az illetéktelen személyek behatolásával és károkozásával szemben, valamint az informatikai eszközök védelmét a természeti és környezeti fenyegetésekkel (pl.: villámcsapás, áradás, tűz, magas hőmérséklet vagy páratartalom) szemben. Ezen célok érdekében a jelen Fizikai és környezeti védelemre vonatkozó eljárásrendet kell alkalmazni.

12.2. A fizikai belépési engedélyek

Az elvárt fizikai védelem érdekében a Hivatal a különböző funkcionális területeit besorolta. A nyilvános területeken kívül védett területként az elektronikus információs rendszereknek helyt adó helyiségeket, ezen kiemelten védett területként az informatikai infrastruktúra és más fokozottan védendő helyiségeit definiálta.

A különböző funkcionális területek között biztonsági határvonalak, ellenőrzött, lehetőség szerint zárt áthaladási pontok, ajtók helyezkednek el.

Az alábbi biztonsági területek kerültek meghatározásra:

Biztonsági követelmények	Helyszínek/belépésre jogosultak
Nyilvános terület - alacsony biztonsági követelmény,	A Hivatal épületein belül és kívül elhelyezkedő mindazon területek, amelyek bárki (pl. ügyfél, látogató) részére nyilvánosan elérhetőek (pl. váróterem, nyilvános folyosó, parkoló)
Védett terület - magas biztonsági követelmények	A Hivatal szakfeladatait támogató elektronikus információs rendszereinek (pl. ASP, anyakönyv, választási, egyéb szakrendszereknek) helyt adó helyiségek. A belépés csak az arra jogosultaknak lehetséges. Látogatók, ügyfelek, külső személyek belépése és ott tartózkodása csak kíséret és felügyelet mellett engedélyezett. Az ügyfélfogadási időn kívüli belépéseket nyilván kell tartani.
Kiemelten védett terület - kritikus biztonsági követelmények	IT- és ellátó infrastruktúra valamennyi helyisége, pl. elosztó- és szerverhelyiségek (ideértve a szerverfunkciójú számítógépeket, adatmentő szervereket, NTG hálózati eszközöket). A belépés kizárólag a rendszergazdának, üzemeltetésért felelősnek engedélyezett, egyéb személyek kizárólag indokolt esetben, felügyelettel léphetnek be és tartózkodhatnak ott. Minden belépést nyilván kell tartani.

12.2.1. Védett területekhez történő hozzáférés

A Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó, jellemzően irodai helyiségekbe belépésre jogosultakat a 12.2.3. Belépésre jogosultak listája pont szerint határozta meg.

A telephelyekre, épületekbe történő fizikai belépések, illetve a védett területekhez történő hozzáférés ellenőrzése megvalósítható elektronikus beléptetőrendszer segítségével és/vagy élőerős védelem formájában, a fizikai biztonsági munkatárs felügyeletével.

Elektronikus beléptetőrendszer szükségességét vagyonvédelmi, információbiztonsági és adatvédelmi szempontból a fizikailag védendő vagyonelemek, informatikai eszközök és tágabb értelemben az informatikai rendszerekben kezelt adatok értéke, a vagyonelemekre és informatikai rendszerekre ható fenyegetések és kockázatok mértéke (a kockázatelemzés eredménye), és az elektronikus- illetve élőerős védelem költségei alapján kell meghatározni. Elektronikus beléptetőrendszer alkalmazása esetén a belépő személy azonosítására és belépési jogosultságának igazolására elektronikus belépőkártya szolgál, mely a beléptető-rendszerben beállított jogosultság szerint engedélyezi a belépéseket, a kijelölt belépési pontokon a belépőkártya használatával nyitható az ajtó. A beléptetőrendszert a rendszergazda vagy jegyző által kijelölt felelős üzemelteti, felügyeli.

Ha az adott telephelyen nincs elektronikus beléptetőrendszer, a belépő személyek azonosítására és belépési engedélyének igazolására papíralapú beléptetőkártya, más telephelyen alkalmazott elektronikus belépőkártya vagy a naprakészen vezetett belépésre jogosultak nyilvántartása szolgál. Ebben az esetben a fizikai biztonsági munkatárs feladata a kijelölt belépési pontokon a belépés felügyelete és a belépési engedélyek (belépőkártyák) ellenőrzése vagy a belépő belépésre jogosultak nyilvántartásában történő azonosítása.

A védett területre történő belépés/hozzáférés ellenőrzése és naplózása megvalósulhat az elektronikus beléptetőrendszer segítségével (az elektronikus belépőkártya használatával) vagy élőerős védelem formájában, a fizikai biztonsági munkatárs felügyeletével (a védett terület kulcsának felvételével és leadásával).
A védett területek kulcsát védett területen biztonságos kulcsszekrényben vagy a fizikai biztonsági munkatársnál kell elhelyezni, aki a belépési engedély ellenőrzését követően adja ki a kulcsot és a jegyző utasításának megfelelően – dokumentálástól eltekintve, Belépési napló vezetésével vagy egyéb dokumentumon – dokumentálja a kulcs felvételét és leadását.

12.2.2. Kiemelten védett területekhez történő hozzáférés

Kiemelten védett területnek kell tekinteni a központi IT- és ellátó infrastruktúra helyiségeit: a szerver-, hálózati rendező helyiséget, nem védett területnek számító helyiségben elhelyezett egyedi rack szekrényeket.

Ezek fizikai védelméről biztonsági szempontból az alábbiak szerint kiemelt figyelmet kell fordítani:

a) A szerver-, hálózati rendező helyiséget, ill. a védett területen elhelyezett rack szekrényeknek zárhatónak kell lenniük és zárva kell ezeket tartani;
b) a védett területen elhelyezett rack szekrényekhez hozzáférhetnek, ill. a kiemelten védett területnek minősülő helyiségekbe beléphetnek az erre a helyiségre belépési engedéllyel rendelkező személyek;
c) a belépési engedéllyel nem rendelkezők (pl. karbantartással vagy javítással megbízott külső partnerek munkavállalói (ld. 10.18. Karbantartó személyek) a kiemelten védett területen csak az engedéllyel rendelkezők állandó felügyelete mellett tartózkodhatnak vagy dolgozhatnak.
d) a belépéseket/hozzáféréseket naplózni kell, amely ellenőrizhetővé teszi a kiemelten védett területen tevékenységet végzőket.

A kiemelten védett területre történő belépés/hozzáférés ellenőrzése részben megvalósulhat az elektronikus beléptetőrendszer segítségével, az elektronikus belépőkártya használatával, a rendszergazda vagy az általa/jegyző által kijelölt személy felügyeletével, a helyiség kulcsának naplózott felvételével és leadásával. A szerverhelyiség és rackszekrények kulcsát egyedileg dokumentáltan kell kiosztani használatra kiadott kulcsok nyilvántartásában vagy egyéb dokumentumban, vagy a fizikai biztonsági munkatársnál kell elhelyezni, aki a belépési engedély ellenőrzését követően adja ki a kulcsot a kulcs felvételének és leadásának dokumentálásával.

A kiemelten védett területekre, a szerverhelyiségekbe állandó belépési engedéllyel nem rendelkezőket elsősorban a rendszergazdának kísérnie kell és figyelemmel kell követnie a tevékenységüket. Az eszközök, rendszerek karbantartási munkálatait külső karbantartók esetében a rendszergazdának felügyelni szükséges, hogy kizárásra kerüljenek a jogosulatlan hozzáférések, illetve hibás karbantartási tevékenységek.

A szerverhelyiségbe, IT- és ellátó infrastruktúra külön helyiségeibe történő valamennyi belépést rögzíteni kell Szerverhelyiség belépési naplóban az alábbi adattartalommal:

a) bejegyző neve,
b) bejegyzővel érkező egyéb érintettek neve(i),
c) be- és kilépés időpontja (év, hónap, nap, óra, perc),
d) belépés célja, esemény, művelet leírása.

A Szerverterem belépési napló vezetése a belépési engedéllyel rendelkezők feladata, a belépési napló vezetését nem váltja ki az elektronikus beléptetőrendszer naplózása.

A kiemelten védett területek helyiségeiben tilos állandó jelleggel munkát végezni, tilos a helyiségben a dohányzás és az étel-, ital fogyasztás, valamint a helyiségben tűz- vagy robbanásveszélyes anyagot vagy a helyiség funkciójától eltérő eszközöket, anyagokat tárolni.

12.2.2.1. Egyedi hálózati rack szekrények védelme

Nem számítanak védett területnek azok a helyiségek, amelyek elsődleges funkciójuk szerint nem hálózati eszközök elhelyezésére szolgálnak, de található a helyiségben egy kulccsal biztosított, zárt hálózati rack szekrény, amely hálózati eszközöket tartalmaz.

Magát a rack szekrényt viszont védett területként kell kezelni az alábbi kiegészítésekkel:

a) A rack szekrényben lévő aktív és passzív hálózati elemek karbantartását, javítását, módosítását, bővítését csak a rendszergazda vagy a jegyző által ezzel megbízott külső partnerek végezhetnek.

b) Az informatikai hálózat mellett egyéb rendszerek (pl.: telefon-, kamera-, riasztó-, fűtési rendszer, stb.) kábelezését is integráltan tartalmazó kábelezésű hálózatok esetén az adott rendszer elemeire vonatkozóan a rendszer üzemeltetői hozzáférést kaphatnak a rack szekrényekhez. A hozzáférés igénylése a védett területekre vonatkozó belépési engedélyek igénylésének eljárása szerint történik (ld. 12.2.4. Belépési engedélyek kiadása).
c) A rack szekrényeket kulccsal zárva kell tartani. A kulcs egy példányát a fizikai biztonsági munkatársnál, egy példányát pedig rendszergazdánál kell elhelyezni. A rack szekrények kulcsának kezelését a fizikai biztonsági munkatárs és a rendszergazda a 12.2.2. Kiemelten védett területekhez történő hozzáférés pont szerint végzi.
d) A rack szekrényhez hozzáféréssel rendelkezők számára folyamatos felügyelet mellett biztosítani kell a rack szekrényt tartalmazó helyiségbe történő bejutást, akár munkaidőn túl is. Munkaidőben a helyiséghez tartozó szervezeti egység, munkaidőn kívül a recepció/portaszolgálat/rendészet feladata a bejutás, illetve a felügyelet biztosítása.
e) Ha a rendelkezésre állási követelmények indokolják szünetmentes áramforrás alkalmazásával kell védeni a rack szekrényben elhelyezett eszközöket az áramellátás zavaraitól, megszakadásától.
f) A rack szekrényben lévő eszközök folyamatos működést igényelnek, tilos a rack szekrényben lévő eszközöket a szekrényhez hozzáféréssel nem rendelkező, illetéktelen személyeknek külsőleg áramtalanítani (kivéve rendkívüli események pl. beázás, tűz esetén).

12.2.3. Belépésre jogosultak listája

A Hivatal telephelyeire/épületeibe és a védett területekre belépésre jogosultak listáját a Fizikai belépési engedélyek nyilvántartása dokumentumban kell vezetni, a nyilvántartást folyamatosan karban kell tartani és három havonta felül kell vizsgálni.

A felhasználók, a szabályzat személyi hatálya alá tartozó, foglalkoztatásra irányuló jogviszony alapján foglalkoztatottak (munkavállalók) belépési engedélye alapértelmezés szerint a Hivatal minden telephelyére /épületére vonatkozik, szükség szerint meghatározhatók kivételt jelentő telephelyek/épületek, amelyekre nem vonatkozik az alapértelmezett belépési engedély, és az engedélyt a védett területekhez hasonlóan, egyedileg kell kérvényezni. Belépési engedély adható a Hivatallal szerződéses kapcsolatban lévő más szervezetek, külső partnerek munkavállaló is, akik rendszeresen munkát végeznek a Hivatalnál. Ilyen esetben a belépési engedélyt egyedileg kell kérvényezni és az engedély megadását a fizikai biztonsági felelős hagyja jóvá.

Élőerős védelem alkalmazása esetén a Hivatal munkavállalóira és alapértelmezés szerinti belépési engedélyére vonatkozóan a Fizikai belépési engedélyek nyilvántartása megfeleltethető a munkaügyi nyilvántartásnak, amelynek folyamatos karbantartása a HR szervezet feladata.

Elektronikus beléptetőrendszer alkalmazása esetén a Fizikai belépési engedélyek nyilvántartása megfeleltethető a beléptetőrendszer belső adatbázisának. Ebben az esetben a beléptetőrendszer rendszergazdájának vagy a jegyző által kijelölt személynek a feladata az adatbázis folyamatos karbantartása, és három havonta történő felülvizsgálata.

Élőerős védelem esetén a Hivatal munkaügyi nyilvántartása nem tartalmazza a külső partnerek belépési engedélyt kapott munkavállalóit, valamint elektronikus beléptetőrendszer esetén is lehetnek olyan védett területek, amelyekhez való hozzáférés a kulcs naplózott felvételével és leadásával valósul meg (pl. rack szekrények). Ezekben az esetekben munkaügyi nyilvántartás, illetve a beléptetőrendszer adatbázisának kiegészítéseként továbbra is vezetni kell a Fizikai belépési engedélyek nyilvántartását olyan szűkített tartalommal, amely a külső partnerek munkavállalóit és az adott védett területekre belépési engedéllyel rendelkező személyeket tartalmazza. A kiegészítő nyilvántartás folyamatos karbantartása és három havonta történő felülvizsgálata a rendszergazda feladata.

A Fizikai belépési engedélyek nyilvántartásának naprakész karbantartása érdekében a HR szervezetnek értesítenie kell a rendszergazdát vagy a beléptetőrendszert üzemeltető, felügyelő felelőst a Hivatalhoz újonnan belépő, illetve onnan kilépő munkavállalókról, engedélyezett személyekről. A kilépőkről történő értesítés a kilépők jogviszonya végének munkaügyi rendszerben történő rögzítéséhez kapcsolódóan automatizált módon (program által küldött e-mail segítségével) is megvalósítható.

A Fizikai belépési engedélyek nyilvántartásának felülvizsgálata céljából a HR szervezetnek a rendszergazda vagy beléptetőrendszert üzemeltető, felügyelő rendelkezésére kell bocsátani, vagy elektronikusan hozzáférhetővé kell tenni a Hivatalnál aktuálisan dolgozó és utolsó 3 hónapban kilépett munkavállalók, megszűnt belépési jogosultak listáját. A nyilvántartás felülvizsgálata során a rendszergazda a belépési engedéllyel rendelkező személyek azonosíthatóságát és a jogviszony érvényességét vizsgálja. A fizikai biztonsági felelős feladata a belépési engedélyek indokoltságát vizsgálni, különösen a külső partnerek munkavállalóira vonatkozóan.

A Hivatal és külső partereinek munkavállalóira vonatkozóan a belépési engedélyek igazolására a HR szervezet a Hivatal kialakított folyamata szerint élőerős védelem esetén papíralapú belépőkártyákat, elektronikus beléptetőrendszer esetén elektronikus belépőkártyákat oszt ki. A belépési engedélyek megszűnésével a kártyák visszavonása is a HR szervezet és a beléptetőrendszert üzemeltető, felügyelő közös folyamata szerint történik.

A belépőkártyán nyomtatott formában szerepelnie kell:

a) a Hivatal nevének;
b) a belépésre jogosult nevének és a Hivatal munkavállalói esetén a dolgozói törzsszámának;
c) a Hivatal munkavállalói esetén a belépésre jogosult fényképének;
d) a belépőkártya számának.

A belépőkártyán nyomtatott formában szereplő adatok változása esetén szükségessé válik a belépőkártya cseréje, amelyet a kártya birtokosának a rendszergazdától vagy a kijelölt felelőstől kell igényelnie. Csak személyre szóló belépőkártyák adhatók ki, csoportokra/szervezetre vonatkozó kártyák nem engedélyezettek. Ez alól kivétel képeznek a vendégkártyák és vésznyitó kártyák, viszont ezek használatát személyre szólóan kell naplózni.

A Fizikai belépési engedélyek nyilvántartásának tartalmaznia kell:

a) a belépésre jogosult nevét és ha elrendelt, akkor a Hivatal munkavállalói esetén a dolgozói törzsszámát, azonosítóját;
b) a külső partnerek esetén a szervezet nevét;
c) a védett vagy kiemelten védett területeket, amelyekhez a belépő hozzáférést kapott (ld. 12.2.1. Védett területekhez történő hozzáférés, 12.2.2. Kiemelten védett területekhez történő hozzáférés);
d) a kiosztott belépőkártya számát (ha van).

12.2.4. Belépési engedélyek kiadása

Új munkatársak felvételekor a munkatárs a HR szervezet felvételi folyamata részeként kap belépési engedélyt az alapértelmezés szerinti telephelyekre, épületekbe. Alapértelmezés szerint az informatikai rendszerek szempontjából kiemelten védett területekre nem vonatkozik ez a belépési engedély.

Az alapértelmezéstől való eltérés vagy változások esetén a Hivatal telephelyeire, épületeibe, védett területeire történő belépést/hozzáférést a Fizikai belépési kérelem vagy egyéb dokumentum kitöltésével kell kérelmezni. A kérelemben fel kel tüntetni a belépés kezdeti és – amennyiben ismert – záró dátumát, a belépés indokát. A kérelmet a közvetlen (vagy felettes) munkahelyi vezetőknek kell kitölteniük és engedélyezniük a beosztott munkatársaikra és a védett területre belépésre engedélyezett külső partnerekre vonatkozóan. A belépést korlátozni kell a munkavégzéshez szükséges telephelyekre, épületekre.

A védett területhez tartozó szervezeti egység vezetőjével jóváhagyatott belépési kérelmet írásban/e-mail-ben el kell juttatni a beléptetőrendszert üzemeltető, felügyelő rendszergazdának vagy jegyző által kijelölt felelősnek.

A kérelem alapján a rendszergazda/kijelölt felelős (pl. HR szervezet) a 12.2.3. Belépésre jogosultak listája pontnak megfelelően elkészíti a papíralapú belépőkártyát vagy megszemélyesíti az elektronikus belépőkártyát és beállítja a beléptetőrendszerben a kártyához rendelt belépési jogosultságot, aktualizálja a Fizikai belépési engedélyek nyilvántartását, Átadás-átvételi jegyzőkönyvön vagy más dokumentumon kiadja a belépőkártyát és tájékoztatja a munkatársat felelősségeiről (ld. 12.6.3. Kártyabirtoklással összefüggő feladatok, felelősségek).

Az átadás-átvételi jegyzőkönyvek megőrzéséről rendszergazdának vagy a kijelölt felelősnek kell gondoskodnia. A megőrzési idő a belépőkártyák visszavételéig tart.

Ha az egyes telephelyekre/épületekbe vagy védett területre történő belépés/hozzáférés nem elektronikus beléptetőrendszer segítségével, hanem a fizikai biztonsági munkatárs felügyeletével valósul meg, akkor a Fizikai belépési engedélyek nyilvántartását a fizikai biztonsági munkatárs rendelkezésére kell bocsátani, vagy elektronikusan hozzáférhetővé kell tenni. Az erről való gondoskodás a beléptetőrendszert üzemeltető, felügyelő rendszergazda vagy jegyző által kijelöl felelős feladata.

12.2.5. Belépési engedélyek visszavonása

A belépési engedély visszavonása az elektronikus vagy papíralapú belépőkártyák visszavételét, az elektronikus beléptetőrendszerben a kártyához rendelt belépési jogosultságok törlését, a papíralapú kártyák megsemmisítését és a Fizikai belépési engedélyek nyilvántartásának aktualizálását jelenti.

A kilépő munkatársak jogviszonyának megszűnésekor a kialakított kilépési folyamat részeként kerül visszavonásra a belépési engedély és visszavételre a belépőkártya.

A beléptetőrendszert üzemeltető, felügyelő rendszergazdának vagy jegyző által kijelöl felelősnek a belépési kérelmek teljesítéséhez, a belépési engedélyek felülvizsgálatához, illetve a biztonsági események kivizsgálásához kapcsolódóan gondoskodnia kell a belépésre jogosultak belépési engedélyének visszavonásáról, ha

a) megszűnik a munkatárs jogviszonya, külső személy megbízása;
b) a belépési kérelmen a belépés végeként megjelölt határozott idő letelt;
c) a Hivatal vezetője egyedileg erre utasítja;
d) a belépőkártya elveszett;
e) felmerült a gyanú, hogy a belépőkártya idegen kézbe került.

12.6. A fizikai belépés ellenőrzése

A Hivatal meghatározta és védi azokat a be- és kilépési pontokat, melyeken a belépés csak belépési jogosultsággal rendelkezők számára vagy csak felügyelet és kíséret mellett lehetséges. Ügyfélfogadási időn kívül zárva tartja az ügyfélforgalom számára biztosított bejáratait, melyen indokolt esetben ideiglenes belépési engedély vagy felügyelet és kíséret mellett lehetséges a belépés.

A Hivatal telephelyeire, épületeibe történő be- és kilépés kizárólag a kijelölt belépési pontokon, személyek esetén a főbejáraton, gépkocsik esetén a gépkocsibejáraton keresztül lehetséges. A Hivatal telephelyeinek, épületeinek egyéb bejáratain (pl. gazdasági bejáró) a be- és kilépés nem engedélyezett. A nem az ügyfélforgalom számára kijelölt bejáratokat kulccsal zárva kell tartani, a belépést csak a kiosztott kulccsal rendelkezők számára lehet biztosítani.

A nyilvános területeken vagy ügyfélfogadási időben az ügyfelek számára szabadon látogathatóként kijelölt területeken kívül minden belépő ügyfelet, látogatót felügyelet alatt kell tartani, a Hivatal szakfeladatait támogató elektronikus információs rendszereinek helyt adó helyiségekbe, irodákba kizárólag adott ügyintézéshez, azonosítva vagy kísérettel mehetnek be és tartózkodhatnak ott. A látogatót, ügyfelet kísérő és fogadó munkatárs felelős a látogatóért, annak minden, az információbiztonságot veszélyeztető tettéért.

Elvárás, hogy a szakrendszerek és központi infrastruktúra helyiségeibe történő látogatói, ügyfél belépésekről információkat kell gyűjteni és megőrizni, kivéve ügyfélfogadási időben az ügyfelek számára szabadon látogathatóként kijelölt területeket.

A karbantartó szervezetekről, személyekről folyamatosan aktualizált nyilvántartást kell vezetni (lásd 10.18. Karbantartó személyek), kizárólag az engedélyezett karbantartók rendelkezhetnek a munkavégzés idejére belépési jogosultsággal.

12.6.1. Munkavállalók belépésének naplózása

Elektronikus beléptetőrendszer alkalmazása esetén a Hivatal munkavállalóinak be- és kilépését, az erre vonatkozó kártyaeseményeket a beléptetőrendszernek kell naplóznia. A naplózásnak teljesítenie kell a 4.1. Naplózási eljárásrend követelményeit. Ha egy munkavállaló otthon felejtette a belépőkártyáját, akkor vendégként kell kezelni és belépését a vendégek naplózási folyamata szerint kell rögzíteni. A beléptetőrendszer által naplózott belépések és kilépések idő adatai nem képezik a bérszámfejtés alapját. Az eseménynaplót naponta menteni kell, valamint gondoskodni kell a mentések hosszú távú megőrzéséről. A megőrzési időt az adatvédelmi tisztviselő állapítja meg és a Hivatal adatkezelési tájékoztatója tartalmazza. A mentésről a beléptetőrendszer rendszergazdájának kell gondoskodnia.

Elektronikus beléptetőrendszer hiányában a munkavállalók esetén a Belépési naplónak a helyben szokásosan vezetett jelenléti ív felel meg.

12.6.2. Ügyfelek, külső partnerek, vendégek belépésének naplózása

Elektronikus beléptetőrendszer alkalmazása esetén a külső partnerek állandó belépési engedélyt (belépőkártyát) kapott munkavállalóit a Hivatal munkavállalóival azonos módon kell naplózni, azaz be- és kilépésüket a beléptetőrendszernek kell naplóznia. Az ügyfelek, egyéb látogatók részére vendégkártyák kerülnek kiosztásra, mely jogosultságának beállításakor biztosítani kell, hogy annak felhasználásával a látogatók ne juthassanak be a kiemelten védett helyiségekbe.

Az állandó belépési engedéllyel vagy belépőkártyával nem rendelkezők esetén az elektronikus beléptetőrendszeren kívül a védett területekre ügyfélfogadási időn kívüli belépésekre a belépési napló nyilvántartást Belépési napló űrlapon vagy a rendszeresített egyéb bizonylaton a fizikai biztonsági munkatárs vezeti, a nyilvántartásnak legalább az alábbiakat kell tartalmaznia:

a) látogató neve,
b) látogatót fogadó, kísérő neve,
c) be- és kilépés időpontja
d) belépés célja (ügyintézés, látogató vagy szerződött ügyfél).

Ha egy telephelyen nincs fizikai biztonsági munkatárs kijelölve, akkor a nyilvántartás vezetése azoknak a feladata, akikhez a látogató érkezik.

A látogatók kíséretét az épületben történő mozgásuk során folyamatosan biztosítani kell. A kíséret biztosítása a fizikai biztonsági munkatárs vagy annak a feladata, akihez a vendég érkezik.

A belépési napló visszakereshető formában történő tárolásáról a fizikai biztonsági munkatársnak (illetve azoknak, akikhez a vendég érkezik) kell gondoskodnia.

A Hivatalhoz érkező, vendégkártyával nem rendelkező ügyfelek csak az ügyfélszolgálati térben, belépésüktől kezdve folyamatos felügyelet mellett tartózkodhatnak.

12.6.3. Kártyabirtoklással összefüggő feladatok, felelősségek

A kártyabirtokosok névre szólóan kiosztott belépőkártyáinak megfelelő kezeléséről és biztonságos őrzéséről az adott kártyabirtokos gondoskodik. A kártya másra nem átruházható, más használatába nem adható. A kártya elvesztése vagy megrongálódása esetén a kártyabirtokos felelőssége, hogy azonnal jelentse azt a beléptetőrendszert üzemeltető, felügyelő rendszergazdának vagy felelősnek, aki gondoskodik a kártya visszavonásáról és pótlásáról.

Elektronikus beléptetőrendszer alkalmazása esetén minden kártyabirtokosnak használnia kell az elektronikus belépőkártyát minden elektronikus kártyaolvasóval ellátott be- és kilépési ponton, a csoportos belépés nem engedélyezett (a beléptetőrendszernek nemcsak a belépések engedélyezése, hanem a be- és kilépések naplózása is a célja).

A belépési pontok védelme érdekében tilos kitámasztani és felügyelet nélkül nyitva hagyni az elektronikus kártyaolvasóval ellátott ajtókat, ha az ajtón át folyamatos rakodás történik, akkor egy belépésre jogosult személynek kell felügyelnie az ajtón áthaladókat.

A belépési pontokon tilos idegeneket beengedni, a belépőkártyával nem rendelkező, Hivatalhoz érkező vendégeket a fizikai biztonsági munkatárshoz kell irányítani, ahol elvégzik a vendégek regisztrációját.

12.6.4. Rendellenességek kezelése

Az információbiztonsági oktatások keretében a Hivatal minden tagjának fel kell hívni a figyelmét a rendellenességek jelentésére, amelyet a 9.27. A biztonsági események jelentése pont szerint kell megtenniük, ha a következő rendellenességeket tapasztalja:

a) elvesztett eszköz;
b) jogosulatlan hozzáférés;
c) belépési jogosultság ellenére belépés megtagadása;
d) idegen kártyahasználat (nem a kártyabirtokos használja a kártyát);
e) nem megfelelő kártyahasználat (valaki olyan helyiségbe próbál belépni, melyhez nincs engedélye);
f) kíséret nélkül közlekedő vendégek.

A biztonságért Felelős feladata, hogy a rendellenességeket kivizsgálja és kezdeményezze a további intézkedéseket az eset kezelése érdekében.

12.6.5. Belépések ellenőrzése

A fizikai belépéseket a kijelölt belépési pontokon a fizikai biztonsági munkatárs, a beléptetést végző elektronikus beléptetőrendszer naplóinak a feldolgozásával a rendszergazda ellenőrzi.

A biztonságért Felelős a Biztonságértékelési terv keretein belül (5.2 Biztonsági értékelések), illetve szúrópróbaszerűen jogosult a fizikai belépésre vonatkozó előírások betartását ellenőrizni.

12.17. A fizikai hozzáférések felügyelete

A Hivatal a fizikai biztonsági munkatárs által ellenőrzi az informatikai rendszereknek helyt adó telephelyekre, épületekbe belépéseket, védett területekhez történő hozzáféréseket annak érdekében, hogy észlelje a fizikai biztonsági eseményeket és reagáljon azokra.

A biztonságért Felelősnek a Biztonságértékelési terv keretein belül (ld. 5.2 Biztonsági értékelések) át kell vizsgálnia a fizikai hozzáférésekről készült belépési naplókat, illetve azonnal át kell vizsgálnia a naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

Ha a naplók átvizsgálásának eredménye alapján jogosulatlan fizikai hozzáférés történt, a 9.9. Biztonsági események kezelése pontban leírtak szerint meg kell kezdeni a biztonsági esemény kivizsgálását.

12.17.1. A fizikai hozzáférések felügyelete - Behatolásjelző és megfigyelő berendezések

A Hivatal fizikai behatolásjelző és felügyeleti berendezéseket vagyonvédelmi, információbiztonsági és adatvédelmi szempontból a fizikailag védendő vagyonelemek, informatikai eszközök és tágabb értelemben az informatikai rendszerekben kezelt adatok értéke, a vagyonelemekre és informatikai rendszerekre ható fenyegetések és kockázatok mértéke (a kockázatelemzés eredménye), és az elektronikus- illetve élőerős védelem költségei alapján határozza meg.

Azoknál a telephelyeken, épületekben, ahol vagyonvédelmi okokból kockázatelemzés alapján indokolt (az 1.10. Kockázatmenedzsment stratégia és az 1.10.1.Kockázatelemzési és kockázatkezelési eljárásrend alapján elvégzett kockázatelemzés alapján) vagy jogszabály alapján szükséges, elektronikus riasztórendszert kell kialakítani:

a) a kritikus biztonsági követelményű kiemelten védett terület (a szerver-, hálózati rendező helyiség),
b) a magas biztonsági követelményű védett terület, a szakrendszerek munkaállomásainak helyiségei

védelmére kellő számú jelzést adó egységet kell felszerelni:

a) mozgás- és nyitásérzékelőt (lehetőleg az egyes szintek/zónák külön partícióként programozva, védve),
b) üvegtörés érzékelőt (ahol a kockázatfelmérés alapján indokolt, pl. egyes kritikus földszinti helyiségek esetén),
c) füstérzékelőt (ahol a kockázatfelmérés alapján indokolt vagy Országos Tűzvédelmi Szabályzat alapján szükséges, a 12.33. Tűzvédelem követelményének megfelelően)

A kockázatkezelésért felelős személy (jegyző vagy az általa kijelölt személy) döntésének megfelelően vagy jogszabályi kötelezés alapján , vagy ha beépített tűzjelző berendezés katasztrófavédelem által felügyelt helyre átjelzése az Országos Tűzvédelmi Szabályzat alapján szükséges, akkor tűzjelző rendszer katasztrófavédelem által felügyelt helyre átjelzése nem elvárás vagyonvédelmi- és egyéb jelzéseit (betörésjelzések, műszaki jelzések) távfelügyeleti szolgáltató felé továbbítani kell, aki a szerződés alapján gondoskodik a szükséges intézkedések megtételéről, a szerződésben megadottak és/vagy a Hatóságok értesítésével.

Azoknál a telephelyeken, épületeknél, ahol a kockázatkezelésért felelős személy (jegyző vagy az általa kijelölt személy) döntésének megfelelően kockázatcsökkentő válaszlépésként, vagy jogszabály alapján kötelező, ott szükséges a kiépített riasztórendszer távfelügyeletre csatlakoztatása, a nyitás-zárások, riasztási események naplózása, a naplók rendszeres felülvizsgálata. Ehhez szükséges a rendszer olyan beállítása, mely az eseményeket küldi a távfelügyeleti központba (kommunikáció engedélyezése), a távfelügyeleti szolgáltatóval az események fogadására, a naplók küldésére vonatkozó szerződés kötése vagy a meglévő szerződés kiegészítése. Ez egyedi kódok használata és kódnyilvántartás mellett a riasztórendszer eseménytárából történő felülírás esetén is lehetővé teszi biztonsági esemény után a nyitás-zárások vizsgálatát, személyhez rendelését.

12.22. Látogatói hozzáférési naplók

A Hivatalhoz érkező vendégek informatikai rendszereknek helyt adó telephelyekre, épületekbe történő belépését a 12.6.2. Ügyfelek, külső partnerek, vendégek belépésének naplózása pontban leírtak szerint naplózni kell.

A rendszergazdának vagy a jegyző által kijelölt személynek azonnal át kell vizsgálnia a vendégek belépéséről készült naplókat, valamint az Adatvédelmi és Adatbiztonsági Szabályzat előírásainak betartásával az esetlegesen rendelkezésre álló kamarafelvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

12.31. Vészvilágítás

Az informatikai eszközöket koncentráltan tartalmazó szerverteremben és hálózati rendező helyiségekben automatikus vészvilágítási rendszert vagy utánvilágító táblákat kell alkalmazni és ezeket az Éves karbantartási tervnek megfelelően rendszeresen karbantartani, amely áramszünet esetén aktiválódik, és a vészkijáratok és menekülési útvonalak jelzésével biztosítja a helyiségek biztonságos elhagyását.

12.33. Tűzvédelem

Az informatikai eszközöket koncentráltan tartalmazó szerverteremben és hálózati rendező helyiségekben független áramellátással ellátott tűzjelzőt, valamint elektromos tüzek oltására alkalmas kézi vagy automatikus tűzoltó berendezést kell alkalmazni, és ezeket a tűzvédelmi előírásoknak megfelelően rendszeresen karban kell tartani.

Ezekben a kritikus biztonsági követelményű kiemelten védett helyiségekben - és ahol az tűzvédelmi szempontból indokolt - minimális elvárás a tanúsított gázzal oltó (CO2) hordozható, kézi tűzoltó készülék biztosítása, az elektromos tüzek oltására nem megfelelő a porral oltó készülék.

A 12.17.1. A fizikai hozzáférések felügyelete - Behatolásjelző és megfigyelő berendezések pont szerint, a kockázatelemzés alapján, ha vagyonvédelmi okokból indokolt (vagy beépített tűzjelző berendezés tűz- és hiba-átjelzéseinek katasztrófavédelem által felügyelt helyre átjelzése az Országos Tűzvédelmi Szabályzat alapján szükséges), akkor a jegyzőnek gondoskodnia kell távfelügyeleti szolgáltató felé átjelzésről (OTSZ előírás alapján tűzvédelmi hatóság által meghatározott, a katasztrófavédelmi szerv által felügyelt helyre továbbításáról). A távfelügyeleti szolgáltatóval való szerződéskötés a jegyző hatásköre.

Az informatikai eszközöket koncentráltan tartalmazó helyiségekben nem tárolhatóak tűzveszélyes anyagok, illetve nagy mennyiségben éghető anyagok (pl. csomagolóanyag, papír).

12.37. Környezeti védelmi intézkedések

Az informatikai eszközöket koncentráltan tartalmazó szerverteremben és hálózati rendező helyiségekben az eszközök biztonságos működése érdekében klímaberendezések alkalmazásával 18-20°C között kell tartani a hőmérsékletet és 40-60% között a relatív páratartalom szintjét.

A klímaberendezések darabszámát és teljesítményét az eszközök hődisszipációs mutatóit figyelembe véve úgy kell tervezni, hogy a helyiségben nem csak a jelenleg elhelyezett eszközök, hanem a jövőbeli, tervezett kihasználtság esetén is, még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.

Technikai lehetőség rendelkezésre állása esetén biztosítani kell a klímaberendezések automatikus újraindítását az esetleges áramszüneteket követően, hiányában manuálisan ellenőrizni kell a klímaberendezések újraindítását az esetleges áramszüneteket követően.

A hőmérsékletet szintjét hőmérséklet érzékelő eszközzel folyamatosan mérni kell, technikai lehetőség rendelkezésre állása esetén az eszköznek riasztást kell küldenie (pl.: e-mail, SMS útján) a rendszergazdának, ha a hőmérséklet 10°C alá csökken vagy meghaladja a 28°C-ot. Technikai lehetőség hiányában a helyiség hőmérsékletét a külső hőmérséklettől függően, de legalább napi gyakorisággal manuálisan ellenőrizni kell, illetve rendszergazdai tevékenység ellátása alkalmával, túlmelegedés gyanúja (pl. rendszer lassulása, elérhetetlenné válása) esetén.

A gépek közelében nem tárolhatók olyan anyagok, amelyek közvetve (pl. korrózióval) vagy közvetlenül (pl. vízkárral) káros hatást fejtenek ki az informatikai eszközökre. Ezért tisztítószereket vagy egyéb kémiai oldószert, folyadékot, valamint poros tárgyakat tilos ezen eszközök közvetlen közelében tárolni.

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

Az informatikai eszközök csővezetékek megrongálódásból származó károkkal szembeni védelme érdekében biztosítani kell, hogy a főelzáró szelepek hozzáférhetőek legyenek, megfelelően működjenek, valamint az épületek karbantartásáért felelős kulcsszemélyek és a fizikai biztonsági munkatársak számára ismertek legyenek. Az informatikai eszközöket koncentráltan tartalmazó szerverterem és hálózati rendező helyiségek tervezésekor gondoskodni kell a víz és más csővezetékek kiváltásáról, áthelyezéséről, vagy vízbetörésérzékelő szonda felszereléséről.

12.42. Be- és kiszállítás

Az informatikai eszközöket koncentráltan tartalmazó szerverterembe az informatikai vezető tudtával, és belépési engedéllyel rendelkező személyek felügyelete mellett lehet eszközöket be- és kiszállítani, és a be- és kiszállított eszközöket a Szerverterem belépési naplóban kell rögzíteni.

A Hivatalhoz érkező új eszközöket szállítólevélen kell a szállítótól átvenni, majd az eszközöket azok jellemzőivel együtt fel kell venni a hardver- és szoftver nyilvántartásokba. Az eszközök üzembehelyezését, áthelyezését és selejtezését a nyilvántartásokban kell vezetni, oly módon, hogy az eszközök állapota és elérhetősége naprakész legyen (ld. 6.36. Rendszerelem leltár).

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

A felhasználók számára névre szólóan, hordozhatóságot megengedően átadott informatikai eszközök (pl. laptop, mobiltelefon, PDA, táblagép, pendrive, külső merevlemez) Hivatalból való kiszállítása – az eszközt átvevő jogosult által – automatikusan engedélyezett. Az eszköz visszaszolgáltatásakor a visszavevőnek meg kell győződni arról, hogy az megfelel a kiadáskori állapotának.

A felhasználók által a Hivatal telephelyén használt, hordozhatóságot nem megengedően átadott informatikai eszközök (pl. asztali számítógép, monitor, nyomtató) felhasználók általi, telephelyről való kiszállításához jóváhagyott kiszállítási engedély szükséges. Az eszközök kiszállítását az informatikai üzemeltetési vezetőtől szükséges írásban kérvényezni, aki az engedélyezést vagy megtagadást írásban közli az igénylővel.

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

Informatikai eszköz szervizbe történő szállítását dokumentálni és az adathordozókra vonatkozó szabályoknak megfelelően kell eljárnia a 11.1. Adathordozók védelmére vonatkozó eljárásrend szerint.

13. TERVEZÉS

13.1. Biztonságtervezési eljárásrend

Az információbiztonsági irányítási rendszer tervezése során jelen fejezetben meghatározott Biztonság-tervezési eljárásrendet kell alkalmazni.

13.2. Rendszerbiztonsági terv

Ha a Hivatal hatáskörébe tartozik az informatikai rendszer tervezése, akkor a biztonsági követelmények dokumentálására Rendszerbiztonsági tervet kell készíteni, amelynek összhangban kell állnia a szervezeti felépítéssel, szervezeti sajátosságokkal. A terv készítését a biztonságért Felelős koordinálja, a készítésbe bevonja a rendszer szerepeit és felelőseit betöltőket (minimálisan a rendszergazdát, adatgazdákat, jegyzőt).

A tervnek minimálisan tartalmaznia kell az informatikai rendszer:

a) nevét és rövid nevét;
b) célját, hatókörét, alapfeladatait biztosító moduljait;
c) státuszát (üzemel, tervezés alatt, archiv);
d) típusát (főalkalmazás vagy általános támogató rendszer);
e) az informatikai rendszer szerepeit és felelősségi köreit betöltő személyeket (engedélyezésért felelős vezető, rendszertulajdonos, adatgazda, rendszergazda, üzemeltetési felelősök);
f) az informatikai rendszerben feldolgozott, tárolt és továbbított információtípusokat;
g) az informatikai rendszer biztonsági osztályát és az azt alátámasztó indoklást;
h) az informatikai rendszert fenyegető veszélyeket;
i) az informatikai rendszer működési környezetét és a más rendszerektől vagy rendszerelemektől való függőségeket vagy kapcsolatokat;
j) a biztonsági osztálynak megfelelő aktuális vagy tervezett védelmi intézkedéseket, helyettesítő intézkedéseket vagy intézkedésbővítéseket és azok indoklását.

A terv bizalmas minősítésű dokumentum, amelyet a tervben rögzített, a végrehajtásban érintett személyek, szervezeti egységek számára kell kihirdetni (ideértve a terv változásait is), akik illetékteleneknek nem adhatják tovább. A terv megismerésére (és tárolására) jogosult személyek feladata gondoskodni arról, hogy a terv jogosulatlanok számára ne legyen megismerhető, módosítható.

A terveket legalább kétévente felül kell vizsgálni és minden olyan esetben aktualizálni kell, ha változás következik be az informatikai rendszerekben vagy környezetükben, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

A terv és kapcsolódó rendszerdokumentációk elkészítése és karbantartása a biztonságért Felelős feladata. Az elkészült tervet, illetve annak változásait egyeztetni szükséges az informatikai rendszerek adatgazdáival. A tervet a jegyző vagy az általa kijelölt 'Engedélyezésért felelős vezető és a biztonságért Felelős közösen hagyják jóvá (az engedélyezésért felelős vezető a szervezeti felsővezetés azon tagja, aki jogosult hivatalosan felelősséget vállalni az információs rendszer Hivatal számára elfogadható kockázati szinten történő működtetéséért a szervezeti működés, a vagyonelemek vagy a személyek tekintetében). További felelősségeket, feladatokat az elektronikus információs rendszer Rendszerbiztonsági terve tartalmaz.

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

13.3. Viselkedési szabályok

A munkavállalói titoktartási kötelezettségvállalás a munkaszerződés/munkaköri leírás, valamint titoktartási nyilatkozat dokumentumban kerül rögzítésre, ettől függetlenül minden munkavállalóra az Mt. és egyéb jogszabály titoktartási kötelezettségvállalásra vonatkozó rendelkezéseinek betartása kötelező érvényű.

Nem munkaviszonyban történő foglalkoztatás, valamint egyéb jogviszony esetében külön titoktartási nyilatkozat megléte kötelező.

Az informatikai rendszerekhez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, a rendszerekhez kapcsolódó kötelező, vagy tiltott tevékenységet a Nyilatkozat az információbiztonsági és adatvédelmi előírások elfogadásáról dokumentum tartalmazza.

Az informatikai rendszerhez való hozzáférés engedélyezése előtt a hozzáférési jogosultságot igénylő személynek nyilatkoznia kell arról, hogy a fenti nyilatkozatban foglalt biztonsági szabályokat és kötelezettségeket megismerte, megértette, és azokat saját felelősségére betartja. A nyilatkozat történhet írásban papír alapon vagy e-learning rendszerben elektronikus formában. A belépő munkavállalók nyilatkoztatásáról a felvételi folyamat részeként vagy az új belépő képzés keretében kell gondoskodni.

A nyilatkozatban foglalt előírásokat legalább kétévente felül kell vizsgálni, és szükség szerint aktualizálni kell, amely a biztonságért Felelős feladata. A változásokról a módosított szabályzat kihirdetésével kell a felhasználókat tájékoztatni és az érintett munkavállalóknál az előírások változása esetén a nyilatkozattételt meg kell ismételni.

A Hivatal informatikai rendszereivel kapcsolatba kerülő külső partnerekre vonatkozó, a biztonságért Felelős által megfogalmazott információbiztonsági előírásokat a Külső partnerekre vonatkozó információbiztonsági előírások dokumentum tartalmazza. A kapcsolat alapját képező szerződés megkötése során kell a titoktartási kötelezettségvállalást, valamint az előírások megismerésére és betartására irányuló kötelezettségvállalást a külső partnerek irányában érvényesíteni.

13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások

A közösségi média és külső webhelyek, alkalmazások használatára a következő előírások vonatkoznak:

a) A Hivatal informatikai eszközein a közösségi média oldalakat és külső webhelyeket, alkalmazásokat csak az ügyviteli tevékenységekkel, illetve azok támogatásával kapcsolatos feladatokra szabad használni. A hivatalos közösségi média oldalakon történő nyilvános tartalommegosztás a 2.124. Nyilvánosan elérhető tartalom pont szerint történik.
b) Tilos a Hivatallal kapcsolatos információk nyilvános webhelyen való engedély nélküli közzététele (ld. 13.4.1. Az Internet biztonsága).
c) Tilos a munkavállalók személyes e-mail címét, illetve a Hivatalnál használt jelszavait használni a külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor (ld. jelen fejezet, Az elektronikus levelezés biztonsága és 8.22.5. Felhasználók felelőssége a jelszóhasználat során).

13.4.1. Az Internet biztonsága

A Hivatal munkavállalói a 2.1. Hozzáférés-felügyeleti eljárásrend szerint hozzáférést kaphatnak az Internethez, ha a munkájuk indokolja. Az Internet hozzáférés az informatikai rendszerek biztonságára nézve az egyik fő veszélyforrás, ezért az alábbi előírásokat kell betartani:

a) A számítógépre telepített, naprakész (legalább naponta frissülő) vírusadatbázissal rendelkező vírusvédelmi szoftver nélkül tilos az Internetet használni. Jelenteni kell az IT Helpdesk-en a rendszergazdának, ha valamilyen oknál fogva a számítógépen nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.
b) Tilos gyanús (pl. illegális szoftvereket vagy erotikus tartalmat kínáló) webhelyekről fájlokat letölteni. Internetezés közben azonnal el kell hagyni azokat a webhelyeket, amelyekre vonatkozóan a vírusvédelmi szoftver vagy a webböngésző vírusveszélyre vagy adatok megszerzésére vonatkozó tevékenységre, adathalászatra figyelmeztet.
c) Internetezés közben el kell utasítani azokat a felbukkanó ablakokat, amelyek segédprogramok telepítését, vagy egyes biztonsági funkciók kikapcsolását kezdeményezik.
d) Tilos az Internet zóna biztonsági szintjét közepesnél alacsonyabbra állítani a webböngésző beállításaiban.
e) Tilos a webhelyek eléréséhez szükséges jelszavakat úgy megválasztani, hogy abból a Hivatalnál használt jelszóra következtetni lehessen.

Az Internet hozzáférés nem használható az alábbi tevékenységekre:

a) Szigorúan tilos az Interneten a szerzői jogokat sértő tartalmakat (pl.: szoftvereket, filmeket, zenéket stb.) le- vagy feltölteni.
b) Szigorúan tilos minden, a Hivatal jó hírnevét veszélyeztető, a közízlést sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó tartalmú fájlok le- vagy feltöltése.
c) Tilos az Interneten keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni vagy azokat engedély nélkül törölni, módosítani.
d) Tilos a Hivatallal kapcsolatos információk nyilvános webhelyen való engedély nélküli közzététele.
e) Tilos a hálózati eszközök, üzenetek hamisítása, olyan látszat keltése, mintha egy üzenet más eszköztől vagy felhasználótól származna.
f) Tilos az Internet hozzáférés magáncélú használata, az Internetet csak a szükséges mértékben, az ügyviteli tevékenységekkel, illetve azok támogatásával kapcsolatos feladatokra szabad használni. Tilos a munkavégzést nem támogató webhelyek felkeresése.
g) Tilos a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybevevő tevékenység, fájlcserélő alkalmazások futtatása, olyan internetes segédprogramok használata, melyek a Hivatal erőforrásainak engedély nélküli megosztására irányulnak (pl.: ftp, torrent).
h) Tilos olyan internetes tevékenységek folytatása, amelyek más természetes vagy jogi személyek adatainak, alkalmazásainak bizalmasságát, sértetlenségét, vagy rendelkezésre állását sérti.

Csak a rendszeresített internetes alkalmazások használhatók. A Hivatal korlátozza egyes fájltípustól (pl.: .avi, .mpg, .wmv kiterjesztésű fájlok), valamint mérettől függő letöltést, illetve megakadályozza bizonyos típusú, munkavégzést nem támogató webhelyekhez való hozzáférést.

13.4.2. Az Internet hozzáférések ellenőrzése

A Hivatal az informatikai rendszerek biztonsága és hatékony működtetése, az üzleti adatok védelme, valamint a jogszabályok és belső szabályozók rendelkezéseinek betartása érdekében naplózhatja, ellenőrizheti, korlátozhatja és letilthatja a felhasználók internethasználatát, és betekinthet az internetforgalom tartalmába is. Az ellenőrzéseket a rendszergazda biztonsági események és adatvédelmi incidensek vizsgálata, kártékony tartalmak kiszűrése, illetve a jegyző utasítására a munkavállalók munkáltatói ellenőrzése során végezheti az ezen célok teljesítéséhez szükséges mélységben.

Tilos az Internet hozzáférés magáncélú használata, de ha a tiltás ellenére a felhasználók magáncélra is használják az Internetet, akkor az internetforgalom a felhasználóhoz kötődő személyes adatokat is tartalmazhat, pl. a meglátogatott weboldalak és az ott megadott vagy lekérdezett adatok, lementett fájlok. Az internethasználat ellenőrzése során a munkáltató bármely internetforgalomba, adatba betekinthet, azonban magáncélú adatok észlelése során csak olyan mértékig, amely szükséges annak eldöntéséhez, hogy az adat magáncélúnak minősül-e. Az ellenőrzést lehetőség szerint (a munkavállaló munkáltatói ellenőrzése során minden esetben) a felhasználó jelenlétében kell végezni, hogy a felhasználó jelezni tudja valamely weboldal forgalmi adatainak vizsgálata előtt, hogy az személyes adatokat tartalmaz, és a Hivatal elkerülje, hogy a felhasználó személyes adataiba betekintsen. A munkáltatói ellenőrzés során csak azt a tényt lehet rögzíteni, hogy a felhasználó az Internet hozzáférést magáncélra használta, az viszont már nem rögzíthető, hogy pontosan milyen weboldalakat keresett fel, és ott milyen adatokat adatott meg vagy kérdezett le, milyen fájlokat mentett le.

13.4.3. Az elektronikus levelezés biztonsága

A Hivatal munkavállalói a 2.1. Hozzáférés-felügyeleti eljárásrend szerint hozzáférést kaphatnak az elektronikus levelezési rendszerhez, ha a munkájuk indokolja.

Az elektronikus levelezés biztonsága érdekében az alábbi előírásokat kell betartani:

a) A számítógépre telepített, naprakész (legalább naponta frissülő) vírusadatbázissal rendelkező vírusvédelmi szoftver nélkül tilos az elektronikus levelezés használata. Jelenteni kell a rendszergazdának, ha valamilyen oknál fogva a számítógépen nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.
b) Tilos megnyitni a vírusvédelmi szoftver által fertőzöttnek jelzett leveleket, azok mellékletét vagy a levélben található internetes hivatkozásokat.

c) A fokozott vírusveszély miatt tilos a nem megbízható forrásból származó levelet, azok levélmellékletét megnyitni, a levélben található internetes hivatkozásokra (linkekre) kattintani. A forrást nem megbízhatónak kell tekinteni, ha
   - a levél feladója nem ismert;
   - a levél nyelve nem várt, nem külföldi partnerrel folytat a felhasználó levelezést (sok veszélyes levél idegen nyelvű, ezért ezeket a leveleket fokozott figyelemmel kell vizsgálni);
   - a levél címzettje közt sok, nem ismert személy szerepel;
   - a levél tárgya nem illeszkedik az ügyviteli folyamatokhoz;
   - levélszemétre jellemző csalogató szövegeket tartalmaz nyereményről vagy erotikus képekről, vagy valamely megvásárolható terméket, szolgáltatást reklámoz stb.;
   - a felhasználó számára ismeretlen vagy tiltott kiterjesztésű csatolt fájlokat tartalmaz.

d) A „Levélszemét" mappába érkező leveleket a kéretlen leveleket szűrő szoftver minősítette levélszemétnek (ld. 18.8.2. Levélszemét szűrése). A szoftver nem minden esetben dolgozik helyesen, lehetnek az ügyviteli folyamathoz tartozó levelek is a mappában. Az itt található levelek megbízhatóságát fokozott figyelemmel kell vizsgálni.

e) Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a Hivatal biztonsági rendszeréről vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást.

f) A levelező szervert is el kell látni olyan hatékony vírusvédelmi szoftverrel, amely megakadályozza a fertőzések elektronikus levelekben történő terjedését.

Az elektronikus levelezés használata során nem engedélyezettek az alábbi tevékenységek:

a) Szigorúan tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely más természetes vagy jogi személy személyiségi, illetve egyéb jogait sérti (pl.: rágalmazás, szerzői jogok megsértése).

b) Szigorúan tilos a Hivatal jó hírnevét veszélyeztető, a közízlést sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét bántó tartalmú levelek küldése.

c) Tilos a levelező rendszeren keresztül belső használatú, bizalmas vagy titkos dokumentumokat, adatokat kijuttatni, illetéktelen személyek részére hozzáférhetővé tenni.

d) Tilos a levelező rendszer magáncélú használata, különösen az egyéni profitszerzést célzó, a szervezettől eltérő üzleti célú tevékenység és reklám, a levelezőrendszert csak az ügyviteli tevékenységekkel, illetve azok támogatásával kapcsolatos feladatokra szabad használni.

e) Tilos a beérkező leveleket a Hivatal levelező rendszerén kívüli postafiókba átirányítani (ez alól kivétel a technikai postafiókok rendszergazdai általi átirányítása és adatgazdai/jegyzői engedéllyel a levelek Hivatalon belüli átirányítása).

f) Tilos a levelező rendszerben lánclevelet, azaz olyan levelet továbbítani, amely arra szólít fel, hogy az minél több címzettnek kerüljön továbbküldésre.

g) Tilos az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni.

h) Tilos feliratkozni nem szakmai jellegű, nem az ügyviteli munkát segítő hírlevél küldő szolgáltatásra.

i) Tilos más szervezetekkel, hatóságokkal, szolgáltatókkal történő rendszeres kapcsolattartáshoz a munkavállalók személyes e-mail címét megadni, online szolgáltatásokra azzal regisztrálni. Ilyen célra a beosztásra, szervezeti egységre vagy szolgáltatásra utaló e-mail cím létrehozását (jellemzően terjesztési csoportot) kell igényelni, hogy a munkavállalók jogviszonyának megszűnése esetén is biztosítható legyen a kapcsolattartás, illetve szolgáltatás folytonossága.

j) Tilos engedély nélkül a Hivatal teljes címtára felhasználásával szervezeti szintű körlevelet küldeni. A szervezeti szintű (a „mindenki" terjesztési csoportnak címzett) körleveleket az erre kijelölt (és megfelelő jogosultságot kapott) személyek (moderátorok) hagyják jóvá.

k) Tilos másvalaki nevében levelet küldeni (kivéve vezetői utasítás alapján, a vezető postafiókjának kezelésére vonatkozó hozzáférési jogosultság megléte esetén).

l) Tilos az Interneten elérhető ingyenes levelezési oldalak vagy magán előfizetésekhez tartozó postafiókok hivatali informatikai eszközökön történő használata. Ezeket hivatalos ügyekben használni tilos.

Az elektronikus levelezés biztonsága és a levelező szerver védelme érdekében az alábbi levelezésre vonatkozó korlátozások vannak érvényben:

a) A postafiókok mérete alapértelmezett beállítás szerint optimálisan 5 Gb. Szükség esetén ettől nagyobb kapacitás vezetői kérésre biztosítható.
b) A beérkező levelek maximális megengedett mérete alapértelmezett beállítás szerint 15 Mb.
c) A küldött levelek maximális megengedett mérete alapértelmezett beállítás szerint 15 Mb.
d) A levelezésben nem fogadhatók és küldhetők levélmellékletként (még tömörített csomagban sem) az alábbi formátumú fájlok a vírusfertőzés veszélye miatt:
e) futtatható fájlok (pl. .exe, .com, .bat, .cmd, .vbs);
f) egyéb programkódot tartalmazó veszélyes fájlok (pl. .dll, .sys, .inf, .bin, .hta, .docm, .xlsm).

A felhasználók feladata gondoskodni a feleslegessé vált leveleik törléséről, a számára biztosított tárhely elfogyásakor a levelek archiválásáról. Az archiválás végrehajtásához segítség kérhető a rendszergazdától.

13.4.4. Az elektronikus levelezés ellenőrzése

A Hivatal az informatikai rendszerek biztonsága és hatékony működtetése, az üzleti adatok védelme, valamint a jogszabályok és belső szabályozók rendelkezéseinek betartása érdekében naplózhatja, ellenőrizheti, korlátozhatja és letilthatja a felhasználók elektronikus levelezését, és betekinthet a levelek tartalmába is.

Az ellenőrzéseket a rendszergazda informatika biztonsági események és adatvédelmi incidensek vizsgálata, kártékony levelek és mellékleteik eltávolítása, levelek mentése és visszaállítása, illetve a jegyző utasítására a munkavállalók munkáltatói ellenőrzése során végezheti, ezen célok teljesítéséhez szükséges mélységben.

A felhasználók elektronikus levelezésének (postafiójának) tartalmáról a Hivatal rendelkezik. A jogviszony megszüntetési folyamata részeként a kilépők postafiókjairól mentés készül, a mentés átadásra kerülhet más kijelölt felhasználóknak, a kilépők személyes e-mail címére érkező levelek átmenetileg átirányításra kerülhetnek másoknak, vagy mások hozzáférést kaphatnak a kilépők postafiókjához a felhasználói adatok mentésére vonatkozó eljárás szerint. Hasonló módon a tartósan távollévő alkalmazottak helyettesítése érdekében a munkahelyi vezető kértheti a távollévő alkalmazott érkező leveleinek átirányítását, vagy hozzáférés biztosítását a távollévő postafiókjához.

Tilos a levelező rendszer magáncélú használata, de ha a tiltás ellenére a felhasználók magáncélú levelezést folytattak, akkor a magáncélú levelek a felhasználóhoz kötődő személyes adatokat tartalmazhatnak. Az elektronikus levelezés ellenőrzése, illetve az átirányított levelekhez, a postafiókhoz vagy a levelek mentéséhez való hozzáférés során a Hivatal bármely levél tartalmába betekinthet, azonban magáncélú adatok észlelése során csak olyan mértékig, amely szükséges annak eldöntéséhez, hogy a levél magáncélúnak minősül-e (pl. a levél tárgya, feladója vagy címzettje alapján ez már eldönthető lehet a levél tartalmának megismerése nélkül is). Az elektronikus levelezés ellenőrzését lehetőség szerint (a munkavállalók munkáltatói ellenőrzése során minden esetben) a felhasználó jelenlétében kell végezni, hogy a felhasználó jelezni tudja valamely levél tartalmának megtekintése előtt, hogy a levél személyes adatokat tartalmaz, és a Hivatal elkerülje, hogy a felhasználó személyes adataiba betekintsen. A munkáltatói ellenőrzés során csak azt a tényt lehet rögzíteni, hogy a felhasználó magáncélú levelezést folytatott, az viszont már nem rögzíthető, hogy pontosan milyen levelezést.

13.4.5. Tiszta asztal és tiszta képernyő politika

A munkavégzés során az íróasztalokon és a munkaállomások képernyőjén mindig csak az éppen végzett munkával kapcsolatos dokumentumok lehetnek elhelyezve, megjelenítve. A Hivatallal kapcsolatos, a tevékenységek során keletkezett valamennyi dokumentumot, illetve szervezeti adatokat tartalmazó adathordozót (pl. CD/DVD, pendrive, külső merevlemez) a munka végeztével, illetve hosszabb távollét esetén el kell zárni.

Az informatikai eszközöktől történő fizikai távozás esetén megfelelő eljárással (automatikus időalapú zárolás, jelszavas képernyővédelem alkalmazásával) gondoskodni kell arról, hogy kívülállók ne tudjanak betekinteni a rendszerekbe, ne férjenek hozzá a rendszerekhez, ne lássák a képernyőn megjelenő adatokat.

Olyan számítógépet, amelyen adatfeldolgozás folyik, tilos bejelentkezett állapotban felügyelet nélkül hagyni. Ha a felhasználó távozik a számítógéptől vagy befejezi a munkát akkor zárolnia kell, illetve ki kell kapcsolnia számítógépet. Ha utolsóként távozik a helyiségből, zárnia kell a helyiséget.

Az elhelyezés során biztosítani kell a melegedő eszközök hűtését, ezért tilos az eszközön lévő szellőző réseket eltakarni (pl. az eszköz zárt helyre beépítésével vagy az eszközre történő rápakolással). Az egymáshoz közel elhelyezett informatikai eszközök működése sem fizikailag, sem elekromágneses sugárzással a másik eszköz működését nem zavarhatja. Az informatikai eszközöknek mindenféle előre betervezhető természeti, illetve emberi fenyegetésből származó rongálódásokkal szemben a biztonságban kell lenniük.

A számítógépes munkahelyek létesítésekor törekedni kell antisztatikus környezet kialakítására. Ezekben a helyiségekben kerülendők a műszálas szőnyegpadlók, bútorszövetek, ruhák.

A munkavégzés során keletkező dokumentumokat, vázlatokat, illetve példányokat – amennyiben már nincs szükség rájuk – iratmegsemmisítővel (vagy apróra tépve) meg kell semmisíteni oly módon, hogy a rajtuk lévő információ ne legyen többé felismerhető vagy visszanyerhető. Amennyiben a későbbiekben még szükség lehet egyes iratokra, azokat zárt szekrényben szükséges tárolni, hogy illetéktelen személyek ne férhessenek hozzá a dokumentumok tartalmához.

Megbeszélések után a tárgyalókból minden dokumentumot el kell távolítani, a táblákról a rajtuk szereplő információkat le kell törölni.

A nyomtatókból a kinyomtatott iratokat el kell távolítani.

13.10. Biztonsági követelmények kiválasztása

A Hivatal a 7/2024. (VI. 24.) MK rendelet Védelmi intézkedések katalógusa szerinti, az informatikai rendszer biztonsági osztálya alapján előírt védelmi intézkedéseket, biztonsági követelményeket alkalmazza.

13.11. Biztonsági követelmények testre szabása

A védelmi intézkedéseket kockázatelemzés alapján a Hivatal és a biztonságért Felelős személyre szabja, adott esetben eltéréseket állapít meg, illetve helyettesítő védelmi intézkedéseket alkalmaz, melyet a Rendszerbiztonsági tervben is dokumentálni szükséges.

14. SZEMÉLYI BIZTONSÁG

14.1. Személyi biztonságra vonatkozó eljárásrend

A Hivatal informatikai rendszereivel kapcsolatba kerülő személyekre vonatkozóan a jelen fejezetben meghatározott Személyi biztonságra vonatkozó eljárásrendet kell alkalmazni.

14.2. Munkakörök biztonsági szempontú besorolása

A Hivatal a munkaköröket biztonsági szempontból az alábbi módon sorolta be:

Munkakör biztonsági besorolása	Átvilágítási kritériumok
Alacsony	- a munkakör betöltésének feltételeit igazoló okiratok (pl. iskolai végzettség, szakképzettség, nyelvismeret, vezetői engedély stb.) ellenőrzése
Magas	- a munkakör betöltésének feltételeit igazoló okiratok (pl. iskolai végzettség, szakképzettség, nyelvismeret, vezetői engedély stb.) ellenőrzése - erkölcsi bizonyítvány (foglalkozás vagy tevékenység gyakorlásától való eltiltás) ellenőrzése - vagyonnyilatkozat (a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény szerint)

Az egyes munkakörök betöltésének feltételeit és a munkakörökhöz tartozó feladatokat, felelősségeket, valamint a munkakörök biztonsági besorolását a HR szervezet a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény és a Szervezeti és Működési Szabályzat alapján határozza meg és legalább éves gyakorisággal vagy szükség esetén (pl. méltatlansági eljárás során) soron kívül is ellenőriz.

A munkakörök biztonsági szempontú besorolásához a munkakör feladatait és felelősségeit kell alapul venni annak meghatározására, hogy a munkakör betöltőjének hibázása esetén milyen mértékben okozhat kárt a szolgáltatások hatékonyságában vagy sértetlenségében, illetve milyen mértékben lehet anyagilag káros.

A munkakörök fenti biztonsági szempontú besorolását legalább kétévente felül kell vizsgálni és szükség szerint frissíti kell. A munkakörök biztonsági besorolása és a besorolás felülvizsgálata az adott szakterület munkahelyi vezetőjének és a HR osztály feladata.

14.3. Személyek háttérellenőrzése

A HR szervezet feladata, hogy az egyes munkakörök betöltését megelőzően ellenőrizze, hogy az érintett személy az adott munkakör „Munkaköri követelménymátrix"-ban rögzített biztonsági besorolásához tartozóan, a 14.2. Munkakörök biztonsági szempontú besorolása pontban meghatározott átvilágítási kritériumokat teljesíti-e. Az átvilágítási kritériumoknak (háttérellenőrzéseknek) való megfelelés feltétele a munkakör betöltésének.

A hozzáférési jogosultságok kiosztása a 2.1.Hozzáférés-felügyeleti eljárásrend szerint történik.

14.5. Személyek munkaviszonyának megszűnése

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges.

Az alkalmazás megszűnését követő meghatározott időszakig történő titoktartást a munkatársaktól, szerződő partnertől, harmadik féltől az alkalmazás megkezdésekor kitöltött titoktartási nyilatkozatban kell rögzíteni, a titoktartásban vállalt felelősségekről a távozó munkatársat, szerződő partnert, harmadik felet távozáskor figyelmeztetni kell kötelezettségére. Tájékoztatni kell a munkavállalót, hogy a Hivatal informatikai rendszereinek használata során a tudomására jutott minden információ bizalmas adatnak minősül, azok illetéktelen, harmadik fél részére történő továbbadása büntetőjogi, illetve polgári jogi következményeket von maga után és a titoktartási kötelezettsége a munkaviszonya megszűnése után is fennáll. A munkavállaló tájékoztatásáért a HR szervezet felelős. Gondoskodni kell a jogviszony megszűnését követően a megszűnt jogviszonyú felhasználó azonosítójával történő visszaélések elkerüléséről. A jelentést vagy eszközök visszavételét elmulasztók, mulasztásuk arányában együttesen felelnek.

14.5.1. Hozzáférési jogosultságok megszüntetése

A kilépők informatikai rendszerekhez való hozzáférési jogosultságát meg kell szüntetni legkésőbb a munkaviszony megszűnésének napján, külső partnerek esetében a szerződés megszűnésekor, lejártakor.

A jogosultságok megszüntetésének normál folyamata, hogy a kilépő munkavállalóról a HR szervezet értesíti a rendszergazdát, aki megszünteti a felhasználók jogosultságait.

A hozzáférési jogosultságot a felhasználóhoz tartozó felhasználói fiók letiltásával kell megszüntetni. Ha a letiltott fiókok fenntartása szoftverlicencek és/vagy informatikai erőforrások felhasználásával jár, akkor a letiltott fiókok 6 hónap után, a felhasználói adatok mentését követően törölhetők.

Ha kiosztásra került, akkor a hozzáférési jogosultságok megszüntetésével egyidejűleg az elektronikus belépőkártyák jogosultságát is meg kell szüntetni, függetlenül attól, hogy a belépőkártya visszaadásra került-e.

14.5.2. Személyi hitelesítő eszközök, vagyontárgyak visszavétele

A 12.2.5. Belépési engedélyek visszavonása pontban leírt módon vissza kell venni a kilépő munkavállalótól a számára egyénileg kiosztott személyi hitelesítő eszközöket, belépőkártyát. A 8.22.7. A többtényezős hitelesítésre szolgáló eszközök, tanúsítványok kezelése pont szerint vissza kell venni a többtényezős hitelesítésre szolgáló eszközöket, illetve vissza kell vonni a tanúsítványokat.

Valamennyi kilépő munkavállalónak és külső partnernek vissza kell szolgáltatnia a Hivatal valamennyi, használatra átvett vagyontárgyát, amikor munkaviszonyuk megszűnik, illetve szerződésük megszűnik vagy lejár. A vagyontárgyakat a közvetlen (vagy felettes) munkahelyi vezetőnek kell átadni, akinek a rendszergazdától igényelnie kell az átvett informatikai eszközök ellenőrzését és az eszközön lévő felhasználói adatok mentését. A rendszergazdának azt is ellenőriznie kell, hogy az üzembe helyezési jegyzőkönyvben vagy a nyilvántartásban rögzített hardver és szoftver specifikációval adják-e vissza az informatikai eszközöket.

Amennyiben a munkavállaló használatában volt informatikai eszközök értékesítésre kerülnek a kilépő munkavállalók számára, a felhasználói adatok mentését követően a 11.8. Adathordozók törlése pontban leírtak szerint törölni kell az eszközön lévő adatokat.

14.5.3. Felhasználói adatok mentése

A távozó munkatárs a rendszergazda és munkahelyi vezetője, általa kijelölt személy jelenlétében jogosult ellenőrizni távozását megelőzően az elektronikus üzeneteket és dokumentumokat, a személyes adatait tartalmazókat törölni, de nem jogosult a munkavégzésével, feladatkörével kapcsolatos üzenetek és dokumentumok törlésére. Az informatikai eszközök ellenőrzése során be kell tartani a vonatkozó adatvédelmi előírásokat. Abban az esetben, ha a dolgozó saját eszközt használt, meg kell győződni arról, hogy az eszköz nem tartalmaz hivatali információt.

Az üzleti adatok védelme érdekében a felhasználó munkavégzéséhez használt dokumentumait, e-mailjeit le kell menteni az általa használt informatikai eszközökről és a központi tárhelyről.

A jogviszony megszüntetésekor mentést kell készíteni a munkaállomáson, a névre szóló felhasználói fiókhoz kötődő tárterületen (az ún. felhasználói profilban) lévő felhasználói dokumentumokról, fájlokról, archivált levelezésről, majd a munkaállomás újrafelhasználása előtt törölni kell a felhasználói profilt. Továbbá mentést kell készíteni a felhasználó használatába adott mobil adattárolókról (pl. pendrive, külső merevlemez) is, és az eszközök újrafelhasználása előtt visszaállíthatatlan módon törölni kell a tartalmukat a 11.8. Adathordozók törlése pontnak megfelelően.

A 2.2. Fiókkezelés pont alapján a mobil eszközökön (pl. mobiltelefon, PDA, táblagép) helyileg semmilyen olyan adatot nem szabad tárolni, amelynek megsemmisülése, törlése vagy kiszivárgása problémát okozhat, ezért az ezeken az eszközön tárolt adatokról nem kell mentést készíteni, hanem az eszköz gyári állapotba történő visszaállításával kell törölni az eszköz tartalmát.

A 13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások eljárása szerint tilos az informatikai eszközök magáncélú használata, ugyanakkor előfordulhat, hogy a felhasználók ennek ellenére az eszközökön mégis magáncélú dokumentumokat, fájlokat tárolnak, amelyek a felhasználóhoz kötődő személyes adatokat tartalmazhatnak. Ha a felhasználói adatok mentése vagy a mentett adatok későbbi felhasználása közben magáncélú adatokat észlelnek, akkor az adatokba csak olyan mértékig szabad betekinteni, amely szükséges annak eldöntéséhez, hogy az adat magáncélúnak minősül e. Az észlelt magáncélú adatokat ki kell hagyni a mentésből, illetve törölni kell az eszközről.

A Hivatal semmilyen felelősséget nem vállal az informatikai eszközein az előírások ellenére tárolt magáncélú adatokért. A jogviszony megszüntetésekor nem biztosítja a magáncélú adatok kimentését és a kilépőnek történő átadását, csak a magáncélú adatok törlését teszi lehetővé az eszközről a felhasználó jelzése esetén.

Az informatikai eszközök ellenőrzését lehetőség szerint (az alkalmazott munkáltatói ellenőrzése során minden esetben) a felhasználó jelenlétében kell végezni, hogy a felhasználó jelezni tudja valamely dokumentum, fájl tartalmának megtekintése előtt, hogy az személyes adatokat tartalmaz, és a Hivatal elkerülje, hogy a felhasználó személyes adataiba betekintsen.

Az üzleti folyamatok és a külső partnerekkel kapcsolattartás folytonosságának biztosítása érdekében a kilépő felhasználók személynevéből képzett e-mail címére érkező levelek, a feladó automatikus tájékoztatása mellett igény esetén 6 hónapig, ideiglenesen átirányíthatók más felhasználók számára, illetve más felhasználók számára hozzáférés biztosítható a kilépő felhasználó postafiókjához. Ezen időszakot követően azonban a személyes e-mail címeket (illetve postafiókokat) meg kell szüntetni, amely a felhasználói fiókok felülvizsgálata során a 6 hónapnál régebben kilépett felhasználói fiókok törlésével valósul meg. A kilépő munkavállaló közvetlen (vagy felettes) munkahelyi vezetője rendelkezik arról, hogy a mentett felhasználói adatokhoz a továbbiakban ki férhet hozzá, illetve kinek kell az érkező leveleket továbbítani vagy a kilépő postafiókjához hozzáférést biztosítani. Ha a közvetlen (vagy felettes) munkahelyi vezető másként nem rendelkezik, a mentett felhasználói adatok 6 hónap után archiválhatók és törölhetők a központi tárhelyről. Az archivált adatokat a jogszabályi és szervezeti előírásoknak megfelelően kell megőrizni és tárolni az Adatok hosszú távú megőrzése pontnak megfelelően.

A központi tárhelyen lévő dokumentumok és e-mail-ek mentésére a hozzáférési jogosultságok megszüntetését követően kerül sor, a felhasználó használatába adott informatikai eszközökön lévő adatok mentése a közvetlen (vagy felettes) munkahelyi vezető bejelentése alapján történik, melynek végrehajtásáért a rendszergazda felelős.

14.8. Az áthelyezések, átirányítások és kirendelések kezelése

Áthelyezések, átirányítások esetén, ha szükséges el kell végezni a munkakörnek megfelelően a 14.3 Személyek háttérellenőrzésére eljárását.

Az áthelyezett felhasználók részére az informatikai rendszerekhez történő hozzáférési jogosultságok igénylése, módosítása és visszavonása a 2.1. Hozzáférés-felügyeleti eljárásrend szerint történik.

Az áthelyezés során felül kell vizsgálni az áthelyezett felhasználó meglévő hozzáférési jogosultságait, fizikai belépési engedélyeit és a szükségtelen jogosultságokat és belépési engedélyeket meg kell szüntetni. Az erről való gondoskodás a munkatárs régi, valamint új munkahelyi vezetőjének egyetemleges felelőssége.

A jogviszony megváltozásáról és a jogosultságok, illetve belépési engedélyek felülvizsgálatának szükségességéről a HR szervezet értesíti a munkavállaló régi és új munkahelyi vezetőjét.

14.9. Hozzáférési megállapodások

Az informatikai rendszerekhez való hozzáférés szabályait Nyilatkozat az információbiztonsági és adatvédelmi előírások elfogadásáról dokumentum tartalmazza, amely szabályok megismertetése, elfogadtatása, felülvizsgálata és frissítése a 13.3. Viselkedési szabályok pont szerint történik.

14.11. Külső személyekhez kapcsolódó biztonsági követelmények

A Hivatal informatikai rendszereivel kapcsolatba kerülő külső partnerekkel kötött szerződésben meg kell követelni, hogy a külső partner határozza meg a Hivatal informatikai infrastruktúrájában számukra a szerződés teljesítéséhez szükséges információbiztonságot érintő szerep- és felelősségi köröket és a kapcsolódó elvárásokat. Szerződéses kötelezettségként meg kell követelni, hogy a külső partner feleljen meg a Hivatal információbiztosági előírásainak, és ezt dokumentáltan igazolja (ld. 13.3. Viselkedési szabályok)

A szerződésben elő kell írni, hogy ha a külső partnertől olyan személy lép ki, vagy kerül áthelyezésre, aki a Hivatal informatikai rendszereihez kapcsolódó hozzáférési jogosultsággal, hitelesítésre szolgáló eszközzel, tanúsítvánnyal, illetve belépőkártyával rendelkezik, akkor a hozzáférések megszüntetése érdekében soron kívül értesítse a Hivatalt a szerződésben meghatározott kapcsolattartón keresztül. A külső partnerek tevékenységét felügyelő munkatársnak a felügyelet során ellenőriznie kell a külső partner munkavállalóinak Hivatal információbiztonsági elírásainak való megfelelését. Ennek érdekében a szerződésben elő kell írni a külső partner részéről az ilyen ellenőrzések tűrését és támogatását.

14.12. Fegyelmi intézkedések

Minden munkavállalónak és külső partnernek (az Információbiztonsági szabályzat személyi hatálya alá tartozóknak) be kell tartania a Hivatal információbiztonsági szabályait. Minden ennek megtagadásából származó információbiztonsági incidens fegyelmi eljárást vonhat maga után. Az incidenseket jelenti szükséges a jegyző felé a 9.27. A biztonsági események jelentése pont szerint. A fegyelmi eljárás módját a jegyző 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. 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.

14.13. Munkaköri leírások

Az elektronikus információs rendszerek felhasználóinak munkaköri leírásába bele kell foglalni, hogy a felhasználó szerepkör kivételével az adott munkavállaló milyen információbiztonsági szerepköröket tölt be és ez milyen felelősségeket jelent. Az erről való gondoskodás a HR szervezet feladata a szerepkörökhöz rendelt munkaköröket vagy személyeket tartalmazó nyilvántartás alapján.

Ha a munkavállalók szerepkörében a felhasználó és munkahelyi vezető szerepkörök kivételével változás következik be, akkor munkavállaló munkahelyi vezetőjének jelentenie kell a változást a rendszergazda felé, akinek a feladata a szerepkör nyilvántartás, az informatikai rendszerek nyilvántartásának módosítása.

A felhasználó szerepkör esetén a biztonságtudatossági képzés keretében kell ismertetni a szerepkörökhöz tartozó feladatokat és felelősségeket (ld. 3.2. Biztonságtudatossági képzés).

15. KOCKÁZATKEZELÉS

15.1. Kockázatelemzési és kockázatkezelési eljárásrend

A Hivatal vezetője a helyes módszertan szerinti kockázatkezelést és az ehhez kapcsolódó ellenőrzések megvalósítását elősegítő eljárást az 1.10. Kockázatmenedzsment stratégia részeként az 1.10.1. Kockázat-elemzési és kockázatkezelési eljárásrendben határozta meg.

A törvényi célok teljesítése, a munkatársak, a lakosság és a partnerek bizalmának megtartása érdekében biztosítja az információk kockázataranyos 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.

15.2. Biztonsági osztályba sorolás

A biztonsági osztályba sorolás a kockázatok alapján az elektronikus információs rendszer védelmének, elvárt erősségének meghatározása. A Hivatal fontos szervezetnek minősül, a Kiberbiztonsági tv. 6. § (10) b) alapján legalább az „alap" biztonsági osztályra irányadó védelmi intézkedéseket kell teljesítenie.

A biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet határozza meg. Lehetőség van eltérésekkel vagy helyettesítő védelmi intézkedésekkel teljesíteni az MK rendelet 2. mellékletben meghatározott minimális követelményeket a rendszerre meghatározott biztonsági kockázati szintnek megfelelő intézkedések kiválasztásával. A Hivatal az MK rendeletben foglalt védelmi intézkedésektől nem tér el, helyettesítő védelmi intézkedéseket nem alkalmaz, amennyiben eltérő, meghatározott intézkedésekkel biztosítja az elektronikus információs rendszer egyenértékű biztonsági képességeit, kockázatokkal arányos biztonsági követelményszintjét, akkor azt az EIR nyilvántartásban és a Rendszerbiztonsági tervben is dokumentálja.

Az elektronikus információs rendszerek biztonsági osztályát a jegyző hagyja jóvá, aki felel azért, hogy az megfeleljen a jogszabályoknak és kockázatoknak, valamint a besorolásban felhasznált adatok teljeskörűek.

A rendszerek biztonsági osztályát a Rendszerbiztonsági terv és az EIR nyilvántartás tartalmazza. A besorolást legalább kétévente, vagy az elektronikus rendszer biztonságát érintő, jogszabályban meghatározott változás esetén soron kívül, dokumentált módon felül kell vizsgálni.

A nemzeti kiberbiztonsági hatóság a Kiberbiztonsági törvényben meghatározott feladatainak végrehajtása céljából nyilvántartja és kezeli többek között az alábbi adatokat:

a) a szervezet elektronikus információs rendszereinek megnevezését, rövid leírását, biztonsági osztályának besorolását, a nyilvántartásba vétel, valamint a felülvizsgálat időpontjában elért biztonsági osztály meghatározását,
b) az elektronikus információs rendszerben kezelt adatok osztályozásához kapcsolódó adatokat, azok adatkezelésének helyszínét, ideértve az ország megnevezését vagy a felhő típusát,

A biztonságáért Felelős által előkészített dokumentumok alapján a jegyző gondoskodik a hatósági nyilvántartáshoz történő adatszolgáltatásról vagy azzal megbízza a meglévő bejegyzése alapján arra jogosult biztonságért Felelőst.

15.4. Kockázatelemzés

A Hivatal az 1.10. Kockázatmenedzsment stratégia pont alapján végzett Kockázatelemzési és kockázatkezelési tevékenysége magában foglalja a rendszerszintű kockázatelemzést is, azaz:

a) a rendszerre vonatkozó fenyegetések és sérülékenységek azonosítását;
b) a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy a rendszer megsemmisítésének valószínűségének és káros hatásainak megállapítását, valamint az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan;
c) a személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségének és mértékének megállapítását.

15.5. Kockázatelemzés – Ellátási lánc

A Hivatal kockázatelemzése kiterjed az ellátási láncra vonatkozó kockázatok felmérésére és kezelésére. Ha az ellátási láncban, rendszerben történtek változások, akkor új kockázatfelmérést kell végezni az érintett kockázat-elemzési pontokra vonatkozóan. Egyes esetben előzetes kockázatfelmérés készítése is szükséges lehet. A megváltozott információkkal frissíteni kell a kapcsolódó dokumentációkat is (pl. Üzletmenet-folytonossági terv).

Az ellátási lánc kockázatkezelése az informatikai rendszerek létrehozásában, üzemeltetésében, karbantartásában vagy javításában közreműködőkre terjed ki. A biztonságért felelősnek a beszerzések során, ismétlődően legalább kétévente, valamint változások esetén ki kell értékelnie, felül kell vizsgálnia a közreműködőkkel és az általuk biztosított EIR-rel, rendszerelemmel vagy rendszerszolgáltatással kapcsolatos ellátási láncból eredő kockázatokat.

15.9. Sérülékenységek ellenőrzése

A biztonságért Felelős a jogszabályokban meghatározott információbiztonsági szervek figyelmeztetése/ riasztása, valamint a rendszergazdának, a rendszerben alkalmazott hardver/szoftver eszközök gyártóinak, szállítóinak figyelmeztetése, riasztása alapján figyelemmel kíséri az eszközök sérülékenységeit.

A valós sérülékenységeket a 18.2 Hibajavítás pont szerint, az eszközök gyártói által kiadott biztonsági frissítések telepítésével kell kijavítani.

A Hivatal külső hálózatból elérhető szolgáltatásainak (pl. weboldal, levelezés) sérülékenységvizsgálatát jegyzői döntésnek megfelelően a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete végezheti Automatizált Sebezhetőségdetektáló Rendszer (ASR) segítségével.

15.18. Sérülékenységmenedzsment – Sérülékenységi információk fogadása

A sérülékenységvizsgálatok eredményét tartalmazó dokumentumok bizalmas minősítésűek, ezért ezeket csak titkosított kommunikációs csatornán lehet továbbítani: pl. titkosított (HTTPS) kapcsolatot alkalmazó weboldalra feltöltve, vagy elektronikus levélben titkosított mellékletként küldve.

15.20. Kockázatokra adott válasz

A Hivatal az 1.10. Kockázatmenedzsment stratégia pont szerint többféle módon reagálhat a kockázatelemzésben feltárt kockázatokra (csökkentheti, elkerülheti, átháríthatja vagy elfogadhatja a kockázatot). Az egyes kockázatok kezelésére javasolt intézkedéseket a kockázatelemzés tartalmazza.

A kockázatelemzés jóváhagyása után a nem tolerálható kockázatok kezelésére Intézkedési tervet kell készíteni az 1.4. Az intézkedési terv és mérföldkövei pontban leírtak szerint.

16. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

16.1. Beszerzési eljárásrend

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

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 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 jegyző vagy megbízására a kijelölt felelős, a rendszergazda feladata. Ezekből a kellékekből mindig akkora készlettel kell rendelkezni, mely biztosítja a folyamatos ügyvitelt. 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.

16.1.1. A bevezetés kezdeményezése és projektterv készítése

Új alaprendszerek/rendszerszoftverek bevezetését a kitűzött és jóváhagyott fejlesztési célkitűzések alapján az illetékes adatgazda vagy a jegyző kezdeményezi és koordinálja. A rendszergazdák közreműködésével Projekttervet kell készítenie, a tervben részletezni kell:

a) a bevezetés szükségességét;
b) a várható felhasználói előnyöket;
c) az üzemeltetés technikai környezetének leírását és a szükséges erőforrásigényeket (hardverigény, licencek száma, stb.);

A bevezetés előtt lehetőség szerint meg kell győződni (pl. egy referencia helyen, vagy egy próbaverzió tesztelésével) arról, hogy a rendszer/szoftver az elvárt működési paramétereket valóban teljesíti. Az így nyert tapasztalatokat is rögzíteni kell a Projekttervben.

Amennyiben a bevezetés részeként szabad szoftvernek minősülő szoftver kerülne felhasználásra, a szoftvernek előzetesen át kell esnie a szabad szoftverek engedélyezési eljárásán.

Az elkészült tervet véleményeztetni kell:

a) az adatgazdával, az érintett szakterületekkel (amelyek a bevezetendő rendszerrel/szoftverrel találkozni fognak), illetve a beruházásban érintett vezetői körben;
d) és a biztonságért Felelőssel, aki biztosítja, hogy a bevezetendő rendszerre/szoftverre vonatkozóan teljesüljenek a rendszer biztonsági osztálya és jelen szabályzat alapján meghatározott biztonsági követelmények.

A véglegesített Projekttervet a beruházás megkezdése előtt a jegyző hagyja jóvá.

16.1.2. A beruházás és bevezetés folyamata

Az adatgazda/jegyző a rendszergazdák közreműködésével megtervezi a bevezetés végrehajtását (az informatikai rendszer éles üzembe állításának folyamatát), amely alapján a kijelölt felelős vagy külső partner végrehajtja a bevezetést. Ha a bevezetendő szoftver egy meglévő informatikai rendszerhez kapcsolódik, akkor a bevezetés a változáskezelés hatálya alá esik és frissíteni kell a vonatkozó dokumentumokat is.

Ha új informatikai rendszer kerül bevezetésre, el kell végezni mindazokat a feladatokat, amelyeket jelen szabályzat a rendszer biztonsági osztálya alapján előír:

a) ki kell jelölni az új rendszer rendszergazdáját, adatgazdáját és a kulcsfelhasználóját.
b) ki kell egészíteni az új rendszerre vonatkozóan az Informatikai rendszerek nyilvántartását (ld. 1.5. Elektronikus információs rendszerek nyilvántartása);
c) felül kell vizsgálni és szükség szerint módosítani kell az Információbiztonsági kockázatelemzést (ld. 1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend).
d) el kell végezni a rendszer biztonsági osztályba sorolását (ld. 15.2. Biztonsági osztályba sorolás).
e) felül kell vizsgálni és szükség szerint módosítani kell az üzletmenet folytonossági terveket (ld. 7.2. Üzletmenet-folytonossági terv).
f) gondoskodni kell a rendszer mentéséről (ld. 7.35. Az elektronikus információs rendszer mentései).
g) felül kell vizsgálni és szükség szerint módosítani kell az informatikai rendszerek Alapkonfigurációját (ld. 6.2. Alapkonfiguráció);
h) ki kell egészíteni a hardver- és szoftver nyilvántartásokat (ld. 6.36. Rendszerelem leltár).
i) felül kell vizsgálni és szükség szerint módosítani kell jelen szabályzatot (ld. 1.1. Információbiztonsági szabályzat).

Az éles üzembe állítás előtt tesztelni kell a bevezetendő rendszer megfelelő működését. Az éles üzembe állítást a tesztelés eredménye alapján az adatgazda és a jegyző engedélyezi. A Tesztelési jegyzőkönyvek és a bevezetéshez kapcsolódó dokumentációk megőrzéséről a jegyző gondoskodik.

A Hivatal tevékenységét közvetlenül támogató alkalmazói rendszerek és a rendszerek részét képező alkalmazói szoftverek, illetve a felhasználói munkaállomásokon egyedileg futó és önálló rendszernek nem tekintett egyéb alkalmazói szoftverek (pl.: irodai szoftverek, segédprogramok) bevezetésére vonatkozóan a következőket kell alkalmazni.

16.1.3. Alkalmazói rendszerek/szoftverek bevezetése

Az alkalmazói rendszerek/szoftverek bevezetésére sor kerülhet:

a) a Hivatal igényei alapján készített, fejlesztő/külső fejlesztő cég közreműködésével történő szoftverfejlesztéssel (továbbiakban: fejlesztés);
b) kész rendszer/szoftver beszerzésével és a Hivatalra történő testreszabásával, adaptálásával (továbbiakban: beszerzés);
c) dobozos szoftver vásárlásával vagy bérlésével;
d) szabad szoftver használatával.

A bevezetést a munkahelyi vezető kezdeményezheti. Ezt írásban kell megtenni a jegyző felé, amelyben:

a) részletesen ki kell fejteni a bevezetés szükségességét, felhasználási célját;
b) meg kell határozni azokat a munkafolyamatokat, amelyek során a szoftvert/rendszert használni kívánják, és azokat a munkatársakat, akik használni fogják;
c) a bevezetés javasolt módját.

Az alkalmazói rendszerek/szoftverek bevezetésének koordinátora és felelőse a jegyző vagy az általa kijelölt személy, akinek egyeztető megbeszélést kell összehívnia a fejlesztésben résztvevőkkel, az érintett szakterületek és a biztonságért Felelőssel.

A megbeszélésen közös véleményt kell kialakítani:

a) a bevezetés szükségességéről és pontos tárgyáról;
b) a bevezetés módjáról;
c) több szakterület érintő rendszerek esetén ki kell jelölni az adatgazdai területet, az adatgazdát és a rendszer kulcsfelhasználóját;
d) meg kell határozni a rendszer működtetésének és üzemeltetésének feltételeit, a szükséges hardver környezetet;
e) a biztonságért Felelős segítségével meg kell határozni a rendszer várható biztonsági osztályát.

A szabad szoftverek bevezetését, használatba vételét, az egyéb módon bevezetésre kerülő, szükségesnek ítélt rendszerek/szoftverek bevezetését a jegyző hagyja jóvá a bevezetés kezdeményezésének vagy az egyeztető megbeszélés emlékeztetőjének az aláírásával, illetve a beruházás engedélyezésével.

16.1.4. Alkalmazói rendszerek/szoftverek fejlesztése

A Hivatal igényei szerint készített szoftverek fejlesztésével (továbbiakban: belső fejlesztés) kapcsolatos előírások a következők. Jóváhagyott fejlesztési igény esetén a rendszer kulcsfelhasználója az érintett szakterületekkel közösen, írásban meghatározza a fejlesztendő szoftverrel szemben támasztott szakmai (funkcionális) követelményeket az alábbi szempontokat is figyelembe véve:

a) funkcionálisan illeszkedjen a munkafolyamathoz;
b) illeszthető legyen a már működő alkalmazói rendszerekhez.

A funkcionális követelmények mellett a biztonságért Felelősnek a bevezetendő rendszerekkel/szoftverekkel szembeni biztonsági követelményeket is meg kell határoznia. A megfogalmazott követelmények alapján a kijelölt munkatárs a kulcsfelhasználóval egyeztetve elkészíti a fejlesztendő szoftver Rendszertervét.

A Rendszertervnek az alábbi követelményeket is teljesítenie kell:

a) legyen összhangban az Informatikai stratégiában megfogalmazottakkal;
b) legyen pontosan definiálva a szoftver többi alkalmazói rendszerhez való kapcsolata;
c) legyen pontosan definiálva az összes nyilvántartásra, illetve megjelenítésre szánt adat;
d) ne kerüljön sor duplikált adatbevitelre.

Az elkészült tervet véleményeztetni kell:

a) a kulcsfelhasználóval és az érintett szakterületekkel;
b) a biztonságért Felelősnek, aki biztosítja, hogy a fejlesztendő szoftverre vonatkozóan teljesüljenek a rendszer biztonsági osztálya és jelen szabályzat alapján meghatározott biztonsági követelmények.

A véglegesített Rendszertervet az adatgazda vagy a jegyző hagyja jóvá. A fejlesztéssel megbízott alkalmazásfejlesztő az elfogadott Rendszerterv alapján elkészíti a szoftver prototípusát. A szoftvernek a Hivatal által birtokolt, legális szoftverlicenccel rendelkező fejlesztői környezetben kell készülnie.

A szoftver elkészítése során az alábbi szempontokat is figyelembe kell venni:

a) a bevitt adatokat formai és tartalmi szempontból ellenőrizni kell, és a feldolgozás során nyert adatoknak tartalmilag helyesnek kell lenniük.
b) a szoftvert megértést segítő kísérő információkkal (megjegyzésekkel) kell ellátni, hogy a későbbi módosítások könnyebben elvégezhetők legyenek.
c) a szoftvert strukturáltan kell felépíteni.
d) a szoftvernek igazodni kell a Hivatal egységes megjelenítéshez.
e) a szoftverek forráskódjának egységes kialakítása, és a munkatársak egymást helyettesítésének biztosítása érdekében követni kell a fejlesztőeszközökre vonatkozó, a jegyző által jóváhagyott fejlesztési konvenciókat.
f) a szoftverfejlesztés során alkalmazni kell a biztonságos kódolásra vonatkozó elveket.

A szoftver prototípusának teljes körű tesztelése terjedjen ki a szoftver minden funkciójára, valamint a többi alkalmazói rendszerrel való kapcsolatára. A felhasználói (funkcionális) tesztelést a leendő felhasználók végzik, a szoftver kulcsfelhasználójának segítségével és iránymutatásával. Az üzemeltetői teszteket a rendszergazda végzi, a biztonsági teszteket pedig a biztonságért Felelős végzi el vagy koordinálja az elvégzését.

A tesztelés során talált hibák javítását a kulcsfelhasználó a fejlesztőtől igényli, melynek alapján az végrehajtja a szükséges módosításokat. A tesztelés során felmerült – a Rendszertervben rögzítettekhez képest eltérést jelentő – módosítási igényeket a kulcsfelhasználónak a kijelölt vezetővel kell egyeztetnie. Csak a közösen elfogadott, írásban rögzített módosítási igények teljesíthetők.

Ha több egymáshoz kapcsolódó szoftver kerül egyidejűleg fejlesztésre, a teljes rendszer teszt anyagát a rendszer próbaüzemének végéig meg kell őrizni.

A fejlesztő elkészíti a szoftver Felhasználói kézikönyvét és saját üzemeltetés esetén az Üzemeltetői kézikönyvét. A Felhasználói kézikönyv a szoftver felhasználóinak készül, ez alapján az átlagos alkalmazói informatikai ismeretekkel rendelkező munkatársnak biztonsággal és önállóan kell tudnia használni a szoftvert. Az Üzemeltetői kézikönyv a szoftver üzemeltetői számára szükséges.

Csak minden tekintetben ellenőrzött, hibátlanul működő és megfelelően dokumentált szoftvert szabad használatra átadni. A fejlesztett szoftvert az adatgazdának kell átvennie. Az éles üzembe állítást az adatgazda és a jegyző engedélyezi.

Belső fejlesztés esetén a fejlesztésében részt vevők a fejlesztés során tudomásukra jutott, a Hivatalra vonatkozó semminemű adatot kívulálló harmadik személy tudomására semmiféle módon nem hozhatnak, ellenkező esetben fegyelmi és büntetőjogi felelősség terheli őket. Belső fejlesztés esetén az alkalmazásfejlesztő által ilyen módon munkaviszonyban létrehozott művének vagyoni jogai a szerzői jogi törvény (továbbiakban: Szjt.) vonatkozó rendelkezései szerint a Hivatalt illetik. A megszerzett vagyoni jogokkal a Hivatal köteles az Szjt. előírásai szerint bánni és gazdálkodni.

16.1.5. Kiszervezett fejlesztés

A jóváhagyott fejlesztési feladat végrehajtására részben (pl.: csak rendszerszervezés, csak programozás) vagy teljes egészében külső fejlesztő cég is megbízást kaphat (továbbiakban: külső fejlesztés).

Külső fejlesztésre vonatkozóan minden esetben szerződést kell kötni a fejlesztővel, amelyben rögzíteni kell:

a) az elvégzendő fejlesztési feladatokat;
b) a 13.3. Viselkedési szabályok pont szerint a titoktartási kötelezettségvállalást és a Hivatal információbiztonsági előírásainak megismerésére és betartására vonatkozó kötelezettségvállalást;
c) a 16.7. Beszerzések pontban meghatározott előírásokat (amely tartalmazza a funkcionális biztonsági követelményeket, a garanciális biztonsági követelményeket, a dokumentációs követelményeket, valamint a dokumentumok bizalmasságára és a fejlesztői környezetre vonatkozó követelményeket);
d) hogy az elkészült szoftverre vonatkozó vagyoni jogokkal a külső fejlesztő rendelkezik-e, vagy azt a szoftver az átadással egyidejűleg átruházza a Hivatalra.

A szerződés megkötése csak a jegyző engedélyével történhet. A külső fejlesztési munka menetére értelemszerűen kell alkalmazni az előző pontban leírtakat, annyi eltéréssel, hogy a fejlesztett szoftvert, a Rendszertervet, Felhasználói kézikönyvet, Üzemeltetői kézikönyvet a külső fejlesztő készíti el.

16.1.6. Alkalmazói rendszerek/szoftverek beszerzése

Kész rendszer/szoftver szállítására és a Hivatalra történő testreszabására, adaptálására vonatkozóan minden esetben szerződést kell a kötni a szállító céggel, amelyben rögzíteni kell az elvégzendő feladatokat, valamint ezzel összefüggésben a 13.3. Viselkedési szabályok pont szerinti védelmi és titoktartási előírásokat, továbbá a 16.7. Beszerzések pontban meghatározott előírásokat. A szerződés megkötése csak a jegyző engedélyével történhet. A bevezetési munka menetére szintén alkalmazni kell a 16.1.4. Alkalmazói rendszerek/szoftverek fejlesztése pontban leírtakat, annyi eltéréssel, hogy a szoftver elkészítése helyett a kész szoftver testreszabását kell elvégezni.

16.1.7. Dobozos szoftverek vásárlása vagy bérlése

Dobozos szoftverek vásárlása vagy használati jogának bérlése beruházásnak minősül, és a Hivatal vonatkozó előírásai szerint kell a beruházási és a beszerzési eljárást lefolytatni.

A szakterületek éves beruházási tervezetükben adják meg szoftver igényeiket. Mivel a beruházási tervben már indoklásra kerül a bevezetés szükségessége és a felhasználás célja, ezért a tervben szereplő szoftverek esetén nem kell végrehajtani a 16.1.1. A bevezetés kezdeményezése és projektterv készítése pontban leírt kezdeményezési eljárást, viszont szükség lehet egyeztető megbeszélés összehívása.

A szoftver beszerzési igényeket a jegyző jóváhagyólag véleményezi a beruházási döntés előtt, jóváhagyása nélkül szoftvert beszerezni tilos. A beszerzendő szoftverrel szemben támasztott követelmények:

a) legyen összhangban a megfogalmazott célokkal;
b) feleljen meg a jelenlegi technikai fejlődésnek;
c) illeszthető legyen a már működő alkalmazói rendszerekhez;
d) legyen megfelelően dokumentálva (a 16.1.4. Alkalmazói rendszerek/szoftverek fejlesztése pont szerinti Felhasználói kézikönyv és szükség esetén Üzemeltetői kézikönyv megléte);
e) feleljen meg a bevezetendő rendszerekkel/szoftverekkel szembeni biztonsági követelményeknek, amelyet a biztonságért Felelős a rendszer biztonsági osztálya és jelen szabályzat alapján határoz meg.

16.1.8. Szabad szoftverek bevezetése

A Hivatalnál vásárolt vagy fejlesztett szoftverek helyett gazdasági megfontolásból szabadon, illetve korlátozással használható szoftverek is bevezethetők, használatba vehetők. Az ilyen szoftverek keresése alapvetően a rendszergazda feladata, de bármelyik felhasználó tehet javaslatot ezekre vonatkozóan.

A szoftvereket csak biztonságos forrásból – lehetőség szerint a szoftver készítőjének webhelyéről szabad beszerezni. A használatbavétel előtt a szoftvert a rendszergazdának biztonságos körülmények között (naprakész vírusvédelmi szoftverrel ellátott számítógépen) különös körültekintéssel kell tesztelnie:

a) Meg kell vizsgálnia a szoftver licencszerződését, és ez alapján eldönteni, hogy a szoftver szabadon használható (freeware), időbeli korlátozással használható (shareware), funkcióbeli korlátozással használható (demo), vagy nem használható. Nem használható a szoftver, ha a licencszerződése az üzleti célú felhasználást nem engedi meg. A vizsgálatához a licencszerződést PDF formátumban le kell menteni és a felhasználást engedélyező vagy tiltó lényegi részeket a szerződésben kiemeléssel kell jelölni.
b) Ellenőriznie kell, hogy a szoftver használata jelent-e biztonsági kockázatot (pl.: a számítógépre telepített és a „virustotal.com" weboldalon online elérhető számos vírusvédelmi szoftver nem jelzi-e kártékonynak a szoftver telepítőjét, a telepítő próbál-e kéretlen programokat telepíteni, vagy próbál-e a szoftver külső szerverre adatokat feltölteni vagy szinkronizálni).

A tesztelés elvégzését Tesztelési jegyzőkönyv űrlapon kell dokumentálni. A szoftver bevezetését, használatba vételét a jegyző a jegyzőkönyvön jóváhagyja vagy elutasítja. A szabad szoftverek nyilvántartásában rögzíteni kell a szoftver adatait, valamint bizonylatként meg kell őrizni a Tesztelési jegyzőkönyvet és a szoftver licencszerződését, a megőrzési idő a szoftver kivezetéséig tart.

A szabad szoftverek nyilvántartásának az alábbi adatokat kell minimálisan tartalmaznia:

a) a szoftver nevét és verziószámát;
b) a szoftver funkciójának rövid leírását;
c) a vizsgálat eredményét (engedélyezett-e a szoftver belső használata);
d) a licenc típusát (freeware, shareware, demo, fizetős);
e) a szoftver forrását (a későbbi frissítések érdekében).

A szabadon használható (freeware) és a csak funkcióbeli korlátot tartalmazó (demo) szoftverek bármelyik felhasználói számítógépre telepíthetők és használhatók, az időbeli korlátozással használható szoftverek (shareware) viszont csak ideiglenesen telepíthetők a számítógépekre kipróbálás és későbbi megvásárlás céljából, a licencszerződés előírásainak betartásával. A fizetős szoftverek nem számítanak szabad szoftvernek, ezek csak a szoftver licencének megvásárlását követően használhatók.

16.1.9. Alkalmazói rendszerek/szoftverek módosítása

A már üzemelő, belső vagy külső fejlesztéssel készült alkalmazói rendszereknél utólag felmerülhet a szoftver módosításának igénye. A felmerülő fejlesztési, módosítási igényeket a rendszer kulcsfelhasználója fogja össze és képviseli a jegyző a fejlesztők felé. Amennyiben a módosítás más kapcsolódó alkalmazói rendszereket is érint, a rendszer kulcsfelhasználója egyeztető megbeszélést hív össze az érintett szakterületek részére. A megbeszélésen közös véleményt kell kialakítani a módosítás pontos tárgyáról.

A módosítási igényt a kulcsfelhasználó hagyja jóvá. A módosítás során a 16.1.4. Alkalmazói rendszerek /szoftverek fejlesztése pontban leírt, új szoftver fejlesztésére vonatkozó lépéseket kell értelemszerűen, részben vagy egészben végrehajtani.

Amennyiben a módosított adatállományok száma eléri vagy meghaladja az adatállományok teljes számának egyharmadát, a tesztelésnek nemcsak a módosított programfunkcióra, hanem a teljes szoftverre ki kell terjednie. Csak a minden tekintetben ellenőrzött, hibátlanul működő szoftvert szabad használatra átadni.

A szoftver módosítása során a változtatásokat a Felhasználói kézikönyvön és ha készül, akkor az Üzemeltetői kézikönyvön is át kell vezetni. Az új dokumentációt változatszámmal kell megkülönböztetni az előzőtől. A szoftver fejlesztőjének új verziószámmal kell ellátni a módosított szoftvert, és az új verzióban történt változásokról a felhasználóknak tájékoztatást kell adnia. A rendszergazdának a verziószámmal azonosítva mentenie kell minden szoftververziót. A központi mentés keretében a mentett szoftververziók archiválásáról a központi mentőrendszer rendszergazdája gondoskodik.

16.2. Erőforrások rendelkezésre állása

A Hivatal biztonsági beruházásainak tervezését a megfogalmazott célok alapján kell elkészíteni (pl. elavult hardver/szoftver eszközök rendszeres cseréje, új biztonsági rendszerek bevezetése).

Az éves költségvetési terv elkészítése során biztosítani kell az informatikai rendszerek és annak szolgáltatásai védelméhez szükséges erőforrásokat (pl. vírusvédelmi szoftverek frissítése, tűzfalak frissítése, többtényezős hitelesítési szolgáltatás, központi mentőrendszer támogatása, kiemelten fontos hardver/szoftverek eszközök támogatása/követése, szerverterem környezeti infrastruktúra elemek karbantartása, külső biztonsági auditok végzése, stb.), oly módon, hogy ezek az erőforrások a tervben elkülönítetten szerepeljenek. A jegyző feladata arról gondoskodni, hogy az adott évben informatikai fejlesztésre fordított költségek legalább 5%-ának megfelelő összeget a Hivatal a tárgyév során kiberbiztonsági fejlesztésekre fordítson.

Szükség esetén a biztonságért Felelős bevonásával a rendszergazda feladata, hogy a védelemhez szükséges költségekre javaslatot tegyen a költségvetési terv készítésekor. 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.

16.3. A rendszer fejlesztési életciklusa

A Hivatal informatikai rendszereinek teljes életútján, azok minden életciklusában figyelemmel kell kísérni azok információbiztonsági helyzetét.

A rendszerek életciklus szakaszai a következők:

1) követelmény meghatározás;
2) fejlesztés vagy beszerzés;
3) megvalósítás vagy értékelés;
4) üzemeltetés és fenntartás;
5) kivezetés (archiválás, megsemmisítés).

A rendszerek életciklusát megvalósító folyamatokban részt vevő információbiztonsági szerepköröket és a felelősségüket, valamint a szerepköröket betöltő személyeket Szerepkörök, feladatok, felelősségek pont, a Rendszerbiztonsági terv és/vagy az Informatikai rendszerek nyilvántartása jelöli ki.

A folyamatok közben fokozott figyelmet kell fordítani az alábbiakra:

1) Követelmény meghatározás: keretében a szakmai (funkcionális) követelmények mellett a bevezetendő rendszerekkel/szoftverekkel szembeni információbiztonsági kövelményeket is meg kell határozni. A rendszerek tervezéskor figyelembe kell venni a biztonságos rendszerarchitektúra tervezésének alapelveit.
2) Fejlesztés vagy beszerzés: a Rendszerterv készítése során, illetve beszerzés esetén az ajánlatkérés, az ajánlatok értékelése és a szerződéskötés során a biztonsági követelmények teljesülését is biztosítani kell. A szoftverek elkészítéséhez létre kell hozni egy éles környezettől elkülönített fejlesztési környezetet, amelyben biztosítani kell a forráskód bizalmasságát és sértetlenségét, továbbá a biztonságos kódolás érdekében képezni kell az alkalmazásfejlesztőket és alkalmazni kell a biztonságos kódolás elveit.
3) Megvalósítás vagy értékelés: az éles üzembe állítás előtt a funkcionális és üzemeltetői tesztek mellett biztonsági teszteket is kell végezni, amelyek a biztonsági követelmények teljesülésének bizonyítására szolgálnak.
4) Üzemeltetés és fenntartás: az üzemeltetés és fenntartás során valamennyi érintett félnek be kell tartania jelen szabályzatban foglalt információbiztonsági előírásokat. A szoftverek utólagos módosítása során a változáskezelési folyamatot követve kell biztosítani, hogy a változtatással ne sérüljenek a biztonsági követelmények.
5) Kivezetés (archiválás, megsemmisítés):
   - az archív online rendszerek esetén is biztosítani kell a rendszer és környezete biztonsági frissítéseinek telepítését (vagy ha ez nem lehetséges, a rendszert el kell szigetelni a többi informatikai rendszertől), illetve figyelmet kell fordítani a hozzáférési jogosultságok kezelésére is.

- a rendszer megsemmisítése esetén gondoskodni kell az informatikai rendszerhez tartozó programok, adatok, adathordozók, dokumentációk visszaállíthatatlan törléséről vagy megsemmisítéséről.

Az informatikai rendszerek biztonságos kialakítása érdekében a rendszerek tervezése során az alábbi alapelveket kell figyelembe venni:

a) Az informatikai rendszereket a „szükséges minimum" elv alapján úgy kell konfigurálni, hogy csak azok a szolgáltatások, portok, protokollok legyenek engedélyezve, melyek a rendszerek biztonságos működéséhez szükségesek.
b) Alkalmazni kell a legkisebb jogosultság elvét, azaz a hozzáférési jogosultságok kialakításakor csak a feladat ellátásához szükséges és elégséges mértékű jogosultságokat kell biztosítani.
c) Bizalmatlanul kell kezelni és ellenőrizni kell a felhasználói adatbevitelt és a külső forrásból származó adatokat.
d) Azt feltételezve, hogy a Hivatal informatikai rendszerei már sérültek, nem lehet kizárólag a határvédelmi eszközökre támaszkodni (a szervereken is kell tűzfalat és vírusvédelmet alkalmazni).
e) Biztosítani kell, hogy az informatikai rendszerekhez intézett kérések végponttól végpontig titkosítva legyenek.
f) Törekedni kell az informatikai rendszerek redundáns, hibatűrő kialakítására.
g) A védendő adatok értékének megfelelő erősségű hitelesítési technikát kell választani a felhasználók és egyéb entitások (szoftverek, szolgáltatások, hardver eszközök) hitelesítésére (pl. többfaktoros hitelesítés, tanúsítványok).
h) A rendszerbe való bejelentkezési eljárást úgy kell megtervezni, hogy minimalizálja a jogosulatlan hozzáférés kockázatát (pl. sikertelen belépési kísérletek esetén a fiók zárolása, CAPTCHA alkalmazása).

Az elkülönített fejlesztési környezeten kívül a szoftverek felhasználói teszteléséhez tesztkörnyezetet kell létrehozni. A fejlesztési, teszt és éles környezeteket el kell különíteni egymástól, hogy az éles környezet és adatok védettek legyenek a fejlesztési és tesztelési tevékenységek által okozott veszélyektől, illetve a fejlesztés és a tesztelés ne akadályozzák egymást.

A környezeteket az alábbi szempontok figyelembevételével kell kialakítani:

a) Lehetőség szerint eltérő fizikai vagy virtuális eszközökkel kell megvalósítani a környezeteket.
b) A fejlesztési és tesztkörnyezetben jól látható módon fel kell tüntetni a környezet típusát, hogy elkerülhetők legyenek a környezetek összetévesztéséből adódó hibák (pl. teszt adatokat rögzítenek az éles környezetben).
c) Ha nincs rájuk szükség, az éles környezetben le kell tiltani a fejlesztéshez használt eszközöket.
d) Az éles környezethez hasonlóan a fejlesztési és tesztkörnyezet megfelelő védelméről is gondoskodni kell (pl. szoftverfrissítések telepítése, szoftverek biztonságos konfigurálása, hozzáférések felügyelete, változtatások nyomonkövetése, biztonsági mentések készítése).
e) Tilos az éles környezetben tesztelni, illetve a fejlesztői környezetben közvetlenül az éles környezetben lévő adatokkal tesztelni (ez utóbbi esetben nem valósulna meg maradéktalanul a környezetek szétválasztása).
f) A fejlesztési és tesztkörnyezethez tartozó jogosultság nem biztosíthat jogosultságot az éles környezethez.

A jogosulatlan programfunkciók bevezetésének megakadályozása, a nem szándékos vagy rosszindulatú változtatások elkerülése, valamint az forráskódhoz kapcsolódó szellemi tulajdon bizalmas jellegének megőrzése érdekében a következő módon kell felügyelni a szoftverek forráskódjához és a közösen használt szoftverkönyvtárakhoz (továbbiakban együttesen: forráskódok) és fejlesztőeszközökhöz való hozzáféréseket:

a) Hozzáférési jogosultságokkal kell szabályozni, hogy személy szerint ki, és milyen módon férhet hozzá az informatikai rendszerek fejlesztési, teszt és éles környezetéhez, és ezeken belül a forráskódokhoz.
b) A szoftverfejlesztés során az alkalmazásfejlesztők a legkisebb jogosultság elve alapján csak olyan módosítási vagy olvasási jogosultságokkal rendelkezhetnek az egyes informatikai rendszerek forráskódjához, amely és amilyen jogosultság a fejlesztési feladataik ellátásához szükséges.

c) Azon forráskódokhoz, amelyekhez jellegüknél fogva a felhasználóknak is hozzá kell férniük (ilyenek a rendszerek üzemeltetéséhez tartozó scriptek is), a felhasználók csak olvasási jogosultsággal rendelkezhetnek.
d) A szoftverfejlesztés során a forráskód módosítását követően vagy a munkanap végén a módosított forráskódot fel kell tölteni a központi verziókövető rendszerbe. A verziókövető rendszer biztosítja a forráskódok bizalmas tárolását, a változások nyomonkövethetőségét és lehetővé teszi a forráskódok rendszeres biztonsági mentését.
e) A fejlesztési, teszt és éles környezetek naplózásának ki kell terjednie a forráskódokhoz történő hozzáférések naplózására.

16.7. Beszerzések

Az informatikai rendszerek és a rendszerek részét képező szoftverek beszerzésének folyamatát a 16.1.2. A beruházás és bevezetés folyamata és a 16.1.3. Alkalmazói rendszerek/szoftverek bevezetése pont tartalmazza. A Hivatal az informatikai rendszerre, rendszerelemre vagy rendszerszolgáltatásra irányuló beszerzési (ideértve a fejlesztést, a beszerzést és adaptálást, rendszerkövetést, vagy karbantartást is) szerződéseiben szerződéses követelményként meg kell határozni az alábbi követelményeket:

1) Funkcionális biztonsági követelmények - A kockázatokkal arányos védelem kialakítása érdekében a biztonságért Felelőst már az informatikai rendszerek bevezetésének (fejlesztésének vagy beszerzésének) indításakor be kell vonni a projektbe.

   A biztonságért Felelősnek az adatgazdával együttműködve biztonsági osztályba kell sorolni a bevezetni kívánt informatikai rendszert, majd a megállapított biztonsági osztály és jelen szabályzat alapján meg kell határoznia a rendszert fejlesztő vagy szállító külső partner (továbbiakban: szállító) felé a teljesítendő biztonsági követelményeket.

   A szállító által teljesítendő biztonsági követelményeket a szerződés mellékletévé kell tenni.
2) Mechanizmusok erőssége - A szállító felé elő kell írni, hogy a biztonsági mechanizmusok fejtsék ki hatásukat, és teljesítsék a megfogalmazott funkcionális biztonsági követelményeket.
3) Garanciális biztonsági követelmények

   A szállítónak a következő garanciális követelményeket kell a szerződésben vállalnia:
   - Együtt kell működnie a funkcionális biztonsági követelmények teljesítésének vizsgálatában (kifejtve, hogy az adott követelményeket konkrétan hogyan, milyen módon teljesíteni a rendszer), a biztonsági funkciók tesztelésében, a külső biztonsági auditok teljesítésében, és a feltárt biztonsági hibák javításában.
   - Együtt kell működnie a rendszerre vonatkozó ismerté vált, illetve sérülékenységvizsgálatok során feltárt sérülékenységek javításában.
   - Együtt kell működnie a változó információbiztonsági jogszabályok előírásainak teljesítésében és az elfogadott iparági ajánlásoknak (pl. titkosítási protokollokra és algoritmusokra vonatkozóan) való megfelelésben.
   - A rendszerkövetés során a rendszert úgy köteles továbbfejlesztenie, hogy a rendszer mindig kompatibilis legyen az operációs rendszer és a kiegészítő segédprogramok (pl.: Java Runtime Environment, Adobe Acrobat Reader, PHP) támogatásának megszűnésével azok új verziójával.
   - A fejlesztési folyamat részeként gyártói teszteket kell végeznie a rendszer elvárt működésének ellenőrzésére.
   - A rendszer módosítása során a változásokat át kell vezetnie a rendszer dokumentációján és a módosított dokumentációt a Szervezet rendelkezésére kell bocsátania.
4) Biztonsági osztály és védelmi intézkedések - a szerződésnek tartalmaznia kell az érintett informatikai rendszer megállapított biztonsági osztályát, és az ahhoz tartozó védelmi intézkedéseket.
5) Dokumentációs követelmények

   A szállítónak a következő dokumentumokat kell elkészítenie és elektronikus formában a Hivatalnak átadnia a rendszer átadás-átvétele előtt:
   a) Rendszerterv (amennyiben a rendszer tervezését a szállító végzi);
   b) Felhasználói kézikönyv;

c) Üzemeltetői kézikönyv.

A szállítónak gondoskodnia kell arról, hogy a rendszerre vonatkozó dokumentumok (különösen a belső fejlesztői dokumentáció, a Rendszerterv és az Üzemeltetői kézikönyv) jogosulatlanok számára ne legyen megismerhető, módosítható.

6) Fejlesztői környezet - A szállított szoftvernek megfelelően biztonságos környezetben, auditálható körülmények között, a szállító által birtokolt, legális szoftverlicenccel rendelkező fejlesztői környezetben kell készülnie. A fejlesztések során csak olyan szoftverkomponensek használhatóak fel, amelyek nemzetközileg széles körben elfogadottak, és rendelkeznek megfelelő gyártói támogatással a felfedezett sérülékenységek javítására. A szállított szoftver nem tartalmazhat a dokumentációkban nem rögzített szükségtelen funkcionalitást, nem tartalmazhat hátsó kaput, illetve egyéb kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan a Hivatalnak bármilyen kára keletkezne, akkor azért a szállító felelősséggel tartozik.

7) Üzemeltetési környezet - a szállítónak egyeztetnie kell a rendszer kijelölt rendszergazdával a Hivatal által támogatható technikai környezetet és a rendszer erőforrásigényét. Ezeket rögzíteni kell az Üzemeltetői kézikönyvben.

8) Információbiztonsággal és az ellátási lánc kockázatkezelésével kapcsolatos felelőssége - a szállítónak teljesítenie kell az általa a Hivatal informatikai rendszereivel kapcsolatosan ellátott tevékenységével összefüggésben szükséges, jogszabályokban foglalt biztonsági követelményeket.

   Ezen kötelezettség teljesítése érdekében a következőkről kell gondoskodni:
   - Ha a szállítónál olyan esemény merül fel, amely jelentős mértékben befolyásolja a szállítónál fennálló információbiztonsági kockázatokat (akár negatív, akár pozitív irányba) haladéktalanul köteles írásban jelezni azt a Hivatal szerződéses kapcsolattartójának.
   - Szükség esetén a Hivatal információt kérhet a szállítótól a szerződés kapcsán releváns információbiztonsági kockázatokról, személyesen, írásban, vagy (titoktartási kötelezettséget vállaló) megbízott külső szakértő útján. Ilyenkor a szállító köteles ésszerű határidőn belül információt szolgáltatni, a releváns dokumentumokba betekintést engedni, akár egy helyszíni audit keretei között is.
   - Amennyiben a szállító az informatikai rendszer létrehozásában, üzemeltetésében, karbantartásában vagy javításában további közreműködőt (alvállalkozót) vesz igénybe, a szállítóra vonatkozó biztonsági követelményeknek a további közreműködő esetében is szerződéses kötelezettségként teljesülniük kell.
   - A szállító kérésre köteles adatot szolgáltatni a Kiberbiztonsági tv.-vel kapcsolatos kötelezettségei teljesítéséről.

9) Teljesítési kritériumok - a szerződésnek tartalmaznia kell a szerződés szállító általi teljesítésének kritériumait.

   Az informatikai eszközök beszerzése során a következők szerint kell eljárni:
   - Az informatikai eszközök beszerzésére vonatkozó igényeket a beszerzés kezdeményezője köteles előzetesen egyeztetni a rendszergazdával és a jegyzővel.
   - A beszerzési folyamat szerint az informatikai tárgyú beszerzéseket a jegyzőnek is minden esetben jóvá kell hagynia.
   - A Windows operációs rendszerrel igényelt munkaállomások esetén, biztosítani kell, hogy a Hivatal hálózati környezetébe illeszkedő verziójú Windows kerüljön a számítógéppel együtt beszerzésre.
   - Az informatikai eszközök nyilvántartásának alapja az eszköz számlája, mellyel igazolhatónak kell lennie a számítógépekkel együtt vásárolt OEM Windows operációs rendszerek legális használatának. Ha az OEM Windows nem szerepel külön tételként a számlán (pl. a hordozható számítógépek konfigurációjának gyakran része az operációs rendszer), akkor a számlán a számítógép műszaki paramétereiben vagy a számla mellé adott szállítói nyilatkozatban kell szerepelnie, hogy a számítógép milyen operációs rendszert tartalmaz.
   - A szoftverlicencek igazolását akkor is meg kell követelni, ha a számítógép egy speciális rendszer részeként kerül beszerzésre.
   - Az informatikai eszközhöz tartozó dokumentációt (pl.: garancia jegyet, telepítő adathordozót, egyéb gyártói dokumentációt) a számlával együtt kell átadni és meg kell őrizni.

16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonsággal

A kockázatokkal arányos védelem kialakítása érdekében a biztonságért Felelőst már az informatikai rendszerek bevezetésének (fejlesztésének vagy beszerzésének) indításakor be kell vonni a projektbe. A Felelősnek az adatgazdával együttműködve biztonsági osztályba kell sorolni a bevezetni kívánt informatikai rendszert, majd a megállapított biztonsági osztály és jelen Információbiztonsági Szabályzat alapján meg kell határoznia a rendszert fejlesztő vagy szállító külső partner felé a teljesítendő biztonsági követelményeket.

A szállító által teljesítendő biztonsági követelményeket a szerződés mellékletévé kell tenni.

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

Az informatikai rendszerekre vonatkozó dokumentáció kulcsfontosságú szerepet játszik a rendszerek hatékony működtetésében és biztonságos üzemeltetésében. A dokumentáció két fő eleme a felhasználói dokumentáció és az üzemeltetési dokumentáció, amelyek részletes információkat tartalmaznak a rendszer különböző aspektusairól.

Az üzemeltetési dokumentáció átfogó képet nyújt a rendszer technikai környezetéről, felépítéséről és működéséről. Tartalmazza a hardver és szoftver komponensek részletes leírását, beleértve az architektúra rajzot, amely vizuálisan ábrázolja a rendszerelemek kapcsolatait. A kézikönyv kitér a hálózati kommunikációra, a biztonsági beállításokra, valamint a rendszer telepítésének és karbantartásának folyamataira. Fontos részei a jogosultsági rendszer ismertetése, a mentési és archiválási eljárások, valamint a hibaelhárítási útmutatók.

A felhasználói dokumentáció ezzel szemben a rendszer mindennapi használatára összpontosít. Részletesen bemutatja a felhasználói felületet, a különböző modulokat és funkciókat. Emellett tájékoztatást nyújt a felhasználók számára elérhető biztonsági funkciókról és azok helyes alkalmazásáról, valamint a felhasználók felelősségéről a rendszer biztonságának fenntartásában.

A dokumentáció kezelése és tárolása kiemelt figyelmet igényel. A rendszergazda feladata, hogy a dokumentumokat elektronikus formában tárolja és rendszeresen mentse. A biztonságos tárolás és a hozzáférési jogosultságok megfelelő szabályozása elengedhetetlen annak érdekében, hogy a dokumentáció - különösen az érzékeny információkat tartalmazó részek - ne kerülhessenek illetéktelen kezekbe.

Biztosítani kell, hogy a dokumentáció elérhető legyen mindazok számára, akiknek szükségük van rá a munkájuk során. Ez magában foglalja a rendszer használóit, üzemeltetőit, fejlesztőit és ellenőrzőit, akiknek szerepkörüknek megfelelően kell hozzáférést biztosítani a releváns információkhoz. Ha a fenti dokumentációk nem elérhetőek, akkor azok beszerzésére tett kísérletről és végrehajtott intézkedésekről kell dokumentációt készíteni.

16.16. Biztonságtervezési elvek

Az informatikai rendszerek teljes életciklusában alkalmazni kell a 16.3. A rendszer fejlesztési életciklusa pontban szereplő előírásokat.

16.49. Külső elektronikus információs rendszerek szolgáltatásai

Külső informatikai rendszer szolgáltatási szerződés alapján történő igénybevétele esetén szerződéses kötelezettségként meg kell követelni, hogy a külső informatikai rendszer szolgáltatásai megfeleljenek a rendszer biztonsági osztálya és jelen szabályzat alapján meghatározott biztonsági követelményeknek.

A külső informatikai rendszer használata során a felhasználók feladatait és kötelezettségeit a Nyilatkozat az információbiztonsági és adatvédelmi előírások elfogadásáról dokumentum tartalmazza.

16.99. Támogatással nem rendelkező rendszerelemek

A Hivatal lecseréli azokat a rendszerelemeket, amelyekhez már nem érhető el támogatás a fejlesztőtől, szállítótól vagy gyártótól. Ez magában foglalja a szoftverfrissítések, firmware-frissítések, alkatrészcserék és karbantartási szerződések hiányát. A csere célja a biztonsági kockázatok minimalizálása, mivel a nem támogatott elemek sebezhetőségeit a támadók kihasználhatják. Ha a rendszerelemek cseréje nem lehetséges, de azok továbbra is létfontosságúak a Hivatal működéséhez, alternatív támogatást kell biztosítani (belső erőforrás vagy külső szolgáltató bevonásával), illetve kockázatcsökkentő intézkedéseket kell alkalmazni.

Azon rendszerelemekkel kapcsolatban, amelyek támogatása már nem elérhető a fejlesztőtől, szállítótól vagy gyártótól, a következők szerint kell eljárni:

a) A rendszergazda felelőssége, hogy a saját területükre vonatkozóan évente felmérésre kerüljön az informatikai rendszerekben alkalmazott hardver/szoftver eszközök támogatottsága.

b) Ha az eszközök támogatása egy éven belül megszűnik (vagy már megszűnt), akkor a rendszergazdák közreműködésével tervet kell készíteniük a megszűnő támogatású eszközök kezelésére, amely többféle módon is történhet:
   - a szükségtelen hardver/szoftver eszközök selejtezésével;
   - a hardver eszközök cseréjével, illetve a szoftverek új verzióra történő migrációjával (ezek rendszerint beruházással járnak);
   - a hardver eszközök a gyártói támogatása helyett alternatív szolgáltatótól történő támogatás beszerzésével, illetve a szoftverekhez kiterjesztett gyártói támogatás beszerzésével;
   - ha az eszközök nem selejtezhetők, de sem az eszközök cseréje, sem külső alternatív támogatás beszerzése nem megoldható (pl. fenn kell tartani egy archív, már nem támogatott informatikai rendszert), akkor az eszközök hálózati elszigetelésével.

c) A rendszergazda feladata, hogy a megszűnő támogatású hardver/szoftver eszközök terv szerinti kezeléséhez szükséges beruházásokra javaslatot tegyen az éves költségvetési tervének elkészítésekor (16.2. Erőforrások rendelkezésre állása).

17. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

17.1. Rendszer- és kommunikációvédelmi eljárásrend

Az informatikai rendszerek és a kommunikációjuk védelme érdekében a jelen fejezetben meghatározott Rendszer- és kommunikációvédelmi eljárásrendet kell alkalmazni.

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem

A szolgáltatás megtagadó, más néven túlterheléses támadás (Denial of Service, DoS) során a támadó célja, hogy a felhasználók ne tudjanak elérni egy bizonyos szolgáltatást (pl.: a levelezést, bizonyos webhelyeket, online felhasználói fiókokat). Ennek során a támadó felesleges kérésekkel árasztja el, és túlterheli a rendszert, amely így nem tudja a felhasználói kéréseket kiszolgálni.

A túlterhelés támadások esetén a Szervezet a következő eszközöket alkalmazhatja:

a) IPS képességekkel rendelkező tűzfal használata, amely képes bizonyos támadási mintákat felismerni és blokkolni;
b) Amennyiben a hálózati forgalom elemzése azt mutatja, hogy a támadás túlnyomó részben egyetlen, vagy kis számú felső szintű domain-ről (pl. adott országokból) érkezik, akkor az azokról érkező minden forgalom blokkolása a Hivatal tűzfala segítségével. Drasztikus esetben szükség lehet a teljes „külföldről érkező" forgalom blokkolására. Ilyen módon a tűzfal terhelése továbbra is magas, de legalább maga a webszerver visszakaphatja feldolgozó teljesítményének egy részét, és a tűzfalon továbbjutó legitim lekérdezések kiszolgálhatók lehetnek.
c) Kapcsolatfelvétel az Internet szolgáltatóval (különösen a Nemzeti Távközlési Gerinchálózaton keresztül szolgáltatott Internet esetén), hogy van-e szolgáltatás megtagadás elleni védelemi megoldásuk, illetve be tudják-e állítani a szolgáltató tűzfalán az előző pont szerinti blokkolásokat.
d) Kapcsolatfelvétel a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel, szakmai segítségkérés a túlterheléses támadás elemzéséhez és elhárításához (nagyobb tapasztalattal, illetve országos rálátással és nemzetközi kapcsolatokkal rendelkeznek a támadások kezelése terén).
e) A kritikus weboldalak tükrözése külső felhő szolgáltatónál létrehozott virtuális szerverekre a DRP tervben meghatározott módon.

17.17. A határok védelme

Az informatikai rendszerek Internet felőli és kulcsfontosságú pontokon belső határvédelmét tűzfalakkal kell biztosítani oly módon, hogy a tűzfalon keresztül csak az engedélyezett szolgáltatások legyenek elérhetők.

A hálózat szegmentálása fizikai, területi alapon túl történhet logikai alapon is VLAN (virtuális helyi hálózat) szeparációs technológia alkalmazásával.

VLAN-ok kialakításával kell szétválasztani egymástól:

a) a normál felhasználói tevékenységekhez tartozó adatforgalmat (szerverek, munkaállomások);
b) az üzemeltetési tevékenységek (pl.: hálózati eszközök, szerverek, tárolórendszerek, stb. menedzselése) céljára szolgáló menedzsment hálózat adatforgalmát;
c) a külső hozzáférések (pl. vendég WiFi) adatforgalmát (ld. 2.108.2. Vendégek vezeték nélküli hozzáférése);
d) a hálózati forgalom funkcionálisan elkülönülő részeit (pl.: IP telefonhálózat, kamerarendszer, stb.).

A VLAN-ok használata biztosítja, hogy egy támadás esetén az esetleges kár csak az adott részterületre korlátozódjon.

A tűzfalak szabályrendszereinek kialakítása, a beállítások folyamatos karbantartása, a tűzfalak folyamatos felügyelete, az eseménynaplók elemzése, a betörési kísérletek kiszűrése és a szükséges intézkedések megtétele a rendszergazda feladata (ld. 18.13. Az EIR monitorozása).

A határvédelmi eszközök üzembiztonságáért, az eszközök karbantartásáért és javításáért, a beállítások mentéséért a rendszergazda felel. A lehetőségek szerint valamennyi telephelyen törekedni kell a határvédelmi eszközök Alapkonfiguráció szerinti azonos beállítására és a naplózás rendjének betartására.

17.49. Kriptográfiai kulcs előállítása és kezelése

A Hivatal kriptográfiai kulcsokat (tanúsítványokat) az alábbi célokból kezelhet:

a) szerverek és egyéb rendszerelemek (pl. webszerverek, levelező szerverek, hálózati eszközök) kommunikációjának titkosítására;
b) személyre szóló és szervezeti szintű elektronikus aláírás létrehozására;
c) Linux szervereken tanúsítvány alapú hitelesítéséhez a rendszergazdák számára (a tanúsítvány és a használatához szükséges jelszó többtényezős hitelesítésként működik);
d) külső szolgáltatások eléréséhez (szervezeti authentikációs tanúsítványok, többtényezős hitelesítés).

Mind az elektronikus aláírás létrehozásához, mind a szerverek/rendszerelemek kommunikációjának titkosításához és a tanúsítvány alapú hitelesítéshez, amikor a hozzáférés külső hálózatból (pl. Internet felől) történik, kizárólag megbízható hitelesítés szolgáltatótól beszerzett tanúsítványok használhatók. A belső hálózatban alkalmazhatók a Hivatal által generált (önaláírt) tanúsítványok is.

Az aláíró tanúsítványok hitelesítés szolgáltatótól történő igénylését a rendszergazda vagy a jegyző által kijelölt felelős koordinálja, az elkészült tanúsítványok informatikai eszközökön történő beállítását a rendszergazda végzi.

A személyes és szervezeti aláíró tanúsítványokat és hitelesítő tanúsítványokat, valamint a hozzájuk tartozó jelszavakat az érintett személyek feladata biztonságos módon tárolni és kezelni. Tanúsítványt nem szabad átadni, megosztani illetéktelen személlyel. A tanúsítvány és/vagy a jelszó illetéktelen általi hozzáférése, kompromittálódása biztonsági esemény, amelyet jelenteni kell.

Az önaláírt tanúsítványok generálását a rendszergazda végzi figyelembe véve a 17.53. Kriptográfiai védelem pont előírásait.

A szükségtelen tanúsítványokat (pl. a jogviszony megszűnésével a kilépő alkalmazottak aláíró és hitelesítő tanúsítványait) vissza kell vonni, amennyiben releváns meg kell semmisíteni.

17.53. Kriptográfiai védelem

Az informatikai rendszerekben csak olyan kriptográfiai (titkosítási) megoldás alkalmazható, mely megfelel az elektronikus aláírásról szóló törvény előírásainak, illetve az elektronikus aláírást felügyelő hatóság ajánlásainak és állásfoglalásainak.

Minden olyan hordozható eszközt, amelyet a Hivatal területén kívül használnak, szállítanak, a kockázatelemzés eredménye alapján kriptográfiai (hardver titkosítási) mechanizmusokkal kell védeni a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének védelme érdekében a hordozható adattároló, pl. okostelefon, laptop, pendrive stb. esetén teljes eszköztitkosítást, tároló alapú titkosítást, vagy más technológiai eljárást kell alkalmazni (pl. Win10 Pro esetén BitLocker, ESET Endpoint Encryption). A titkosítás elvégzése a rendszergazda feladata a biztonságáért Felelőssel egyeztett eljárás alkalmazásával.

A Hivatal a mobil eszközök adattároló egységein (laptopok, adathordozók, pl. külső HDD) lehetőség szerint hardveres titkosítást, más esetben fizetett szoftveres titkosítást alkalmaz, a mobil eszközökön tárolt információk bizalmasságának és sértetlenségének a védelmére, illetve az információk hozzáférhetetlenné tételére. Továbbá a mobil eszközöket hitelesítési eljárással védi (pl. BIOS jelszó). A felhasználók számára kizárólag hardveres titkosítású pendrive használat engedélyezett.

17.54. Együttműködésen alapuló informatikai eszközök

A Hivatal csak olyan együttműködésen alapuló informatikai eszközöket (pl.: a számítógép kameráját és mikrofonját használó kommunikációs szoftvereket; vagy a számítógép képernyőjének, billentyűzetének és egerének távoli elérését biztosító, távsegítség nyújtására szolgáló szoftvereket) alkalmaz, amelyek:

a) vezérlő szoftvere az engedélyezett szoftverek körébe tartozik;
b) működését a munkatársak ismerik;
c) aktiválásához a felhasználó jóváhagyása szükséges.

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

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

17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)

A Domain Name System (DNS) olyan rendszer, amely az Interneten vagy a belső hálózaton a számítógépekhez, egyéb eszközökhöz vagy szolgáltatásokhoz tartozó, az emberek számára értelmes neveket a hálózati eszközök számára érthető címekre (IP címekre) „fordítja le", „oldja fel", melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. Az informatikai rendszerek névfeloldási szolgáltatását úgy kell kialakítani, hogy a hiteles forrást biztosító DNS szerver (autoritatív DNS) kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat valósítson meg, amely nemcsak hiteles adatokat biztosít a név/cím feloldási kérésekre, hanem az információ eredetét és sértetlenségét is igazolja.

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

A névfeloldási szolgáltatást megvalósító rekurzív vagy gyorsítótáras DNS szervereknek kriptográfiai (titkosítási) megoldással kiegészített, biztonságos tranzakciókat kell megvalósítaniuk, amely segítségével a hiteles forrásból származó név/cím feloldó válaszokra vonatkozóan ellenőrizniük kell és maguknak is biztosítaniuk kell az információ eredetének és sértetlenségének igazolását.

17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén

Az informatikai rendszerek név/cím feloldási szolgáltatását redundáns, hibatűrő módon kell kialakítani, azaz tartalék DNS szervert kell alkalmazni, amely biztosítja a szolgáltatás magas rendelkezésre állását.

A külső és a belső szerepköröket szét kell választani, vagyis külön DNS szervert kell használni a belső hálózat kiszolgálására, és külön szervernek kell ellátnia az internetes DNS szerverekkel történő kapcsolattartást.

17.108. A folyamatok elkülönítése

Az informatikai rendszerekben elkülönített végrehajtási tartományt kell fenntartani minden programfolyamat (process) számára, vagyis az egy számítógépen futó, megosztott erőforrásokat használó folyamatok nem szerezhetnek jogosulatlanul információkat más folyamatoktól. Ennek érdekében a Hivatalnál csak olyan modern operációs rendszerek alkalmazhatóak, amelyek ezt biztosítják.

A hálózati támadástól való védelem érdekében a szakrendszeri munkaállomások különálló védett hálózatba elhelyezése (VLAN) szükséges, lásd 17.17. A határok védelme.

18. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

18.1. Rendszer- és információsértetlenségi eljárásrend

Az elektronikus információs rendszerek, illetve az azokban kezelt adatok sértetlenségének biztosítása érdekében jelen eljárásrendet kell alkalmazni.

18.2. Hibajavítás

Az informatikai rendszerekben keletkező hibákat a következőek szerint kell kezelni:

a) Az informatikai rendszer kulcsfelhasználója, vagy sürgős esetben közvetlenül a felhasználók a rendszerhibát bejelentik a rendszergazdának, aki megvizsgálja, szükség esetén pontosítja a hibát, majd belső üzemeltetésű rendszerek esetén gondoskodik a hiba javításáról. Ha a hibát nem tudja a saját hatáskörében megoldani, akkor a jegyzővel egyeztve külső szakértőt, szakszervízt von be.

b) A külső üzemeltetésű rendszerek esetén a vonatkozó szerződés alapján értesíteni kell az üzemeltetőt és koordinálni a hiba kijavítását.

c) A belső üzemeltetésű rendszerek esetén is szükség lehet a hiba kijavításához külső partnerek (pl.: speciális szakismeretet, szerszámokat vagy anyagokat igénylő hardver javítások esetén külső szakszerviz; vagy szoftverhibák esetén a külső szoftverfejlesztő; vagy a rendszer üzemeltetéséhez támogatást nyújtó szerződéses partner) bevonására. Ilyen esetben a rendszergazda vagy a kijelölt felelős feladata a külső partner által végzett javítás koordinálása, a javított hardver eszközök, illetve szoftverfrissítések éles üzembe állítás előtti tesztelése, a szoftverfrissítések telepítése.

d) A külső szervizben elvégzett alkatrész cserék, módosítások nyomon követése érdekében a szerviz munkalapokat papír alapon vagy digitalizálva, visszakereshető módon kell tárolni és az archiválásra vonatkozó ideig meg kell őrizni.

Amennyiben az informatikai rendszert üzemeltető, vagy ahhoz támogatást nyújtó külső partner a rendszerrel kapcsolatos hibák bejelentésére, a hibajavítás koordinálására és dokumentálására szolgáló saját űrlapot vagy rendszert használ, akkor a fent leírtaktól eltérően azon hibák javítására, amelyekhez nem szükséges a rendszergazda közreműködése, a külső partner űrlapját vagy bejelentő rendszerét is lehet használni.

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

Az operációs rendszerek vagy üzletileg kritikus alkalmazások verziófrissítése csak megtervezett módon történhet meg. A biztonságkritikus szoftvereket a frissítésük kiadását követő meghatározott időtartamon belül, lehető leghamarabb telepíteni szükséges (a frissítések történhetnek automatikusan is az adott operációs rendszer frissítési beállításainak megfelelően). Egyéb biztonsági kockázatot nem jelentő frissítéseket csak abban esetben kell telepíteni, ha azok üzleti szempontból lényeges hibák, sérülékenységek kijavítását, funkcióbővítést eredményeznek. A nem kritikus frissítések telepítését a kialakított gyakorlat szerint 3 frissítésnyi lemaradással a rendszergazda végzi el, ezzel biztosítva a rendszerekre gyakorolt negatív hatások minimálisra csökkentését.

A rendszerben bekövetkezett változásokat dokumentáltan kell kezelni, a módosításoknak megfelelően a dokumentációkat is frissíteni kell. (pl. frissítési/telepítési útmutatók, konfigurációs beállítások). A verzióváltással járó alapszoftver módosítással egy időben a változásokat a dokumentációban is át kell vezetni Munkalap vagy egyéb feljegyzés alapján az Alapkonfiguráció nyilvántartásban. Ha nem a módosítást elvégző rendszergazda felelős a nyilvántartás aktualizálásáért, akkor a Munkalapot el kell juttatni a felelős felé.

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

A felhasználóknak együttműködési kötelezettségük van a rendszergazdával/üzemeltetővel, csökkenteniük kell az esetleges hardveres hiba és az adatvesztés mértékét: ennek érdekében pl. tilos a szoftverek futását a számítógép kikapcsolásával vagy hardveres újraindításával (a Reset gombbal) megszakítani. A számítógép kikapcsolása előtt mindig ki kell lépniük az alkalmazói szoftverekből, az operációs rendszerből és a hálózatból.

Minden esetben meg kell próbálniuk szabályosan kilépni a szoftverekből, amennyiben ez nem lehetséges, akkor meg kell próbálni a nem válaszoló alkalmazást leállítani, majd a számítógépet újraindítani.

18.8. Kártékony kódok elleni védelem

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

a) a fertőzés elkerülése, illetve megbízható megszüntetése érdekében vírusvédelmi szoftverrel kell ellátni minden szervert és munkaállomást (beleértve mind a Windows, mind a Linux operációs rendszerű számítógépeket). Vírusvédelmi szoftver nélkül sem hálózati, sem önálló számítógép nem üzemeltethető. Ezen felül, ha műszakilag lehetséges és információbiztonsági szempontból indokolt egyéb mobil eszközökre is megfelelő védelmet kell biztosítani (pl. okos telefonok);

b) A vírusvédelmi rendszer kiválasztása, és megfelelőségének ellenőrzése a rendszergazda feladata, figyelembe véve, hogy az ingyenes alkalmazások nem biztosítják az optimális védelmet; A kiválasztásnál figyelembe kell venni, hogy a védendő rendszer eszközeinek teljesítményét csak elfogadható mértékben korlátozza, a hatékony munkavégzést ne gátolja;

a) A vírusvédelmi szoftvereket úgy kell telepíteni és beállítani, hogy a háttérben folyamatosan futva (rezidens módban) működjenek, azaz a számítógép indításakor a szoftver aktivizálódjon, és állandó védelmet biztosítson.

b) A vírusvédelmi szoftver ellenőrzésének minden írási és olvasási műveletre ki kell terjednie. Mappák, fájlok vagy folyamatok kizárása a kártevők elleni védekezés alól csak a legkorlátozottabb módon, előzetes jóváhagyást és tesztelést követően, az informatikai rendszerek Alapkonfigurációjában rögzített módon történhet.

c) A vírusvédelmi szoftverek vírusdefiníciós adatbázisát a lehető leggyakrabban frissíteni kell, ezért vírusvédelmi szoftvereket úgy kell beállítani, hogy a frissítés letöltése automatizáltan történjen a vírusvédelmi rendszert menedzselő szerverről, amely a vírusvédelmi szoftver és a vírusdefiníciós adatbázis szétosztására szolgál. A frissítések letöltésének időintervalluma nem lehet nagyobb 1 munkanapnál.

d) A rendszergazdának gondoskodnia kell arról, hogy ha működik, akkor a vírusvédelmet menedzselő szerveren a vírusvédelmi szoftver lehető legfrissebb program- és vírusadatbázis verziója álljon rendelkezésre.

e) A vírusvédelmi szoftvereket úgy kell beállítani, hogy folyamatosan sor kerüljön valamennyi helyi háttértárolójára kiterjedő, teljes körű vírusellenőrzésre.

f) A cserélhető adathordozókon (pl.: CD, DVD, pendrive, külső merevlemez) a használat előtt minden esetben vírusellenőrzést kell végezni. A vírusvédelmi szoftverek beállításával kell gondoskodni arról, hogy az ellenőrzés automatikusan megtörténjen.

g) A vírusvédelmi szoftvereket olyan módon kell beállítani, hogy fertőzés esetén a szoftver elsődleges akcióként próbálja megtisztítani, ha az sikertelen, akkor helyezze karanténba vagy törölje a fertőzött fájlokat (a karanténba helyezett fájlok csak a vírusvédelmi szoftver által elérhetők, és később egy újabb vírusdefiniciós adatbázissal a szoftver képes lehet a karanténba helyezett fájlok megtisztítására).

h) Az egyéb infokommunikációs eszközök (pl. határvédelmi eszközök) tekintetében a gyártói ajánlások és a lehetőségek figyelembevételével kell kártevők elleni megoldást alkalmazni.

i) A felhasználókat a biztonságtudatossági képzés keretében meg kell ismertetni a kártevők kezelésére vonatkozó előírásokkal (ld. 3.2. Biztonságtudatossági képzés). A felhasználóknak tisztában kell lenniük azzal, hogy vírusfertőzést kapva a számítógépük maga válik vírusgazdává, ezzel veszélyeztetve a környezetükben dolgozó munkatársakat és a hálózat többi felhasználóját.

18.8.1. A felhasználók feladatai a vírusfertőzés megelőzése érdekében:

a) A felhasználóknak tilos a vírusvédelmi szoftvert a számítógépről eltávolítaniuk, indításukat megakadályozniuk, illetve a háttérben futó állandó védelmet kikapcsolniuk.

b) A felhasználónak jelentenie kell a rendszergazdának, ha valamilyen oknál fogva a számítógépén nem fut vírusvédelmi szoftver, vagy nem frissül a vírusdefiníciós adatbázisa és a szoftver azt jelzi, hogy az adatbázis elavult.

c) Vírusfertőzésre utaló jelek esetén a fertőzött számítógépet haladéktalanul le kell választani a hálózatról.
d) Ha a vírusvédelmi szoftver a cserélhető adathordozón fertőzést jelez, tilos az adathordozót használni! Ilyen esetben a rendszergazdától kell az adathordozó vírusmentesítését igényelni, amelyet az soron kívül köteles elvégezni
e) Tilos gyanús (pl. illegális szoftvereket vagy erotikus tartalmat kínáló) webhelyekről fájlokat letölteni. Internetezés közben azonnal el kell hagyni azokat az webhelyeket, amelyekre vonatkozóan a vírusvédelmi szoftver vírusveszélyre figyelmeztet (ld. 13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások).
f) Tilos a nem megbízható forrásból származó (pl. ismeretlen feladótól érkezett, sokszor idegen nyelvű) levelet, azok levélmellékletét megnyitni, a levélben található internetes hivatkozásokra (linkekre) kattintani (ld. 13.4.3. Az elektronikus levelezés biztonsága).
g) Tilos megnyitni a vírusvédelmi szoftver által fertőzöttnek jelzett leveleket, azok levélmellékletét vagy a levélben található internetes hivatkozásokat.
h) Az Office irodai szoftverekben le kell tiltani/nem szabad engedélyezni a makrók futtatását, szükség esetén a rendszergazdával egyeztetve csak megbízható forrásból származó, ismert makrókat tartalmazó fájlokat szabad makrók futtatásával megnyitni.

A vírusok és egyéb kártevők általi fertőzés biztonsági eseménynek számít. Ha a felhasználó fertőzésre utaló jelet észlel, vagy a vírusvédelmi szoftver fertőzést jelez a számítógépen és nem tudja azt eltávolítani, illetve fertőzést jelez a hálózati mappákban, akkor az eseményt a 9.27. A biztonsági események jelentése pont előírásai szerint azonnal jelenteni kell.

A fertőzött vagy fertőzéssel gyanúsítható számítógéppel mindennemű további tevékenységet (ide tartozóan a hordozható eszközök, adattárolók le és felcsatlakoztatását) fel kell függeszteni és a számítógépet ki kell kapcsolni! A fertőzés megszüntetését a rendszergazda végzi.

A fertőzés megszüntetése az alábbi lépések végrehajtásával történik:

a) Kártevők általi fertőzés vagy ennek gyanúja esetén az érintett számítógépet a fertőzés továbbterjedésének megelőzése érdekében azonnal le kell választani a hálózatról.
b) Biztosítani kell, hogy a fertőzött számítógépen a vírusvédelmi szoftver lehető legfrissebb program- és vírusadatbázis verziója legyen telepítve.
c) A vírusvédelmi szoftver segítségével a számítógép valamennyi helyi háttértárolójára kiterjedő, teljes körű vírusellenőrzéssel meg kell szüntetni a fertőzést.
d) A fertőzés megszüntetése elsősorban a fertőzött fájlok megtisztításával (a fájl kártevő eltávolításával történő javításával), ha ez sikertelen, a fájl karanténba helyezésével vagy törlésével történhet. Utóbbi esetekben figyelni kell arra, hogy nem rendszerfájlról van-e szó, amelyet más számítógépről átmásolással vagy újratelepítéssel kell pótolni.
e) A vírusellenőrzést addig kell végezni, amíg a vírusvédelmi szoftver úgy nem fut végig az összes fájlon, hogy már nem talál fertőzött fájlt.
f) Ha a vírusvédelmi szoftver nem tudja a fertőzést megszüntetni, a vírusvédelmi szoftverek gyártóinak webhelyén tájékozódni kell az azonosított kártevő viselkedéséről és eltávolításának módjáról. Szükség esetén igénybe vehető speciálisan az adott kártevő eltávolítására készült szoftver vagy más vírusvédelemi gyártó terméke.
g) Ha a fertőzés a fenti módszerekkel nem szüntethető meg, vagy túl sok rendszerfájlt érint, a számítógép háttértárolóinak törlésével és a számítógép teljes újratelepítésével kell a fertőzést megszüntetni.
h) A fertőzött számítógépben használt cserélhető adathordozókat (CD, DVD, pendrive, külső merevlemez) is meg kell vizsgálni, és az esetleges fertőzéseket meg kell szüntetni. Az adathordozók kizárólag a vírusellenőrzést követően használhatók más számítógépeken.

Ha a kártevők olyan módon fertőzik meg a hálózati rendszert, hogy a fertőzés a munkaállomások hálózatra csatlakozásával terjed, a rendszert azonnal le kell állítani, és a vírusellenőrzést a szervereken kell megkezdeni. A rendszer újraindítása után az újrafertőzés elkerülése érdekében csak a vírusellenőrzés által fertőzésmentesnek talált munkaállomásokat szabad a hálózatra csatlakoztatni és a rajtuk a munkát elkezdeni.

A biztonságért Felelősnek szükség szerint tájékoztatnia kell a felhasználókat a vírusok és egyéb kártevők felbukkanásáról, a velük szemben követendő magatartásról és az esetleges téves riasztásokról (ld. 9.31. Segítségnyújtás a biztonsági események kezeléséhez).

A kártevők észlelésével és elhárításával kapcsolatban tett intézkedéseket, a fertőzés okának vizsgálatát és a megelőzésre vonatkozó intézkedéseket a 9.9 Biztonsági események kezelése pontban leírtak szerint kell dokumentálni.

18.8.2. Levélszemét szűrése

A nagy mennyiségben érkező kéretlen levelek, levélszemetek (spam-ek) komoly fennakadást okozhatnak a levelező szerverek működésében és képesek ellehetetleníteni a felhasználói postafiókokat, valamint a kéretlen levelek gyakran tartalmaznak kártevőkkel fertőzött levélmellékletet vagy kártevők letöltésére szolgáló Internetes hivatkozásokat (linkeket), különböző csábító ajánlatokkal, trükkökkel próbálják rávenni a felhasználót, hogy a mellékletet megnyissa, illetve a hivatkozásra kattintson.

A levélszemét központi szűréséről a rendszergazdának vagy a levelezésért felelősnek kell gondoskodnia az alábbi módszerek, beállítások alkalmazásával:

a) Ellenőrizni kell, hogy a beérkező levél feladójának tartománya (domain-je) létezik-e, valóban annak a levelező szerverétől jött-e a levél. El kell dobni az összes dinamikus IP címről érkező levelet. Levél fogadása csak statikus, regisztrált levelező szerverrel (MX rekorddal) rendelkező IP címekről engedélyezett.
b) Ajánlott fekete listás szűrést végezni a feladó címére vonatkozóan. Az Interneten számos olyan fekete lista (Realtime Black List, RBL) adatbázis elérhető, amely olyan címeket tartalmaz, amelyekről bizonyítottan levélszemetet küldtek. A kiválasztott fekete listákon szereplő címekről érkező leveleket vissza kell utasítani.
c) Ajánlott szürke listás szűrést végezni, amely során az adott levelező szervertől, adott feladótól és adott címzettnek érkező levelek az első alkalommal visszautasításra kerülnek és csak egy meghatározott idő utáni próbálkozásra lesznek elfogadva. A következő leveleket már késleltetés nélkül elfogadja a szerver egy beállított időtartamig. A normál levelező szerverek újrapróbálkoznak a levél elküldésével, de a nagy mennyiségű levélszemetet küldők nem tolerálják az ilyen késleltetést, így a levélszemét jelentős hányada szűrhető ezzel a módszerrel. A nagy levelezés szolgáltatók (pl.: Google, Yahoo!, Microsoft, stb.) sok levelező szervert üzemeltetnek, ami túl nagy késleltetést eredményezhet a levélküldésben, és ezért esetükben nem alkalmazható ez a technika.
d) Tartalom alapú szűrést kell végezni a levélforgalmon, amely a különböző kéretlen levelekre utaló jelek (pl. jellemző szavak) alapján megjelöli a valószínűleg levélszemétnek minősülő leveleket és a felhasználó „Levélszemét" mappájába kézbesíti a levelet.
e) Le kell tiltani a nem engedélyezett formátumú levélmellékleteket és el kell utasítani a túl nagy méretű leveleket (ld. 13.4.3. Az elektronikus levelezés biztonsága)

18.13. Az EIR monitorozása

Az informatikai rendszerek napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése, illetve hiba esetén a javítást végzők bevonása. Az informatikai rendszer felügyelete az alkalmazói szoftverek, az adatbázisok, a szerverek, az alapszoftverek, a hálózat, a határvédelmi eszközök és a munkaállomások működésének folyamatos figyelemmel kísérését kívánja meg.

A fenti feladatok végrehajtásának megszervezése és koordinálása a biztonságért Felelős, végrehajtása a rendszergazda feladata.

A rendszergazda ezzel kapcsolatos felelőssége:

a) Ismerni kell az informatikai rendszer és a rendszerelemek működését és azok figyelmeztető és hibaüzeneteit. Tudni kell alkalmazni a szükséges reagálásokat tartalmazó leírásokat.
b) Rendszeresen el kell végezni azokat az ellenőrzéseket, amelyek alapján meg lehet győződni arról, hogy az informatikai rendszer üzemszerűen működik.
c) Rendszeresen ellenőrizni kell az informatikai eszközök rendelkezésre álló kapacitását (szabad háttértár, memória- és processzorkapacitás) és szükség esetén gondoskodni kell a kapacitások bővítéséről vagy

felszabadításáról. A jövőbeli kapacitásigényeket a jelenlegi helyzetnek, trendeknek és elvárásoknak megfelelően kell megtervezni.

d) Rendszeresen át kell vizsgálni az informatikai rendszer eseménynaplóit, és a rendszerhibákat, illetve a behatolásra utaló jeleket a 4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel pont szerint kell kezelni.
e) Rendszeresen ellenőrizni kell az informatikai rendszer naplóinak tárkapacitását és a naplók mentését, hogy a naplók betelése és a naplóbejegyzések felülírása miatt naplóbejegyzések ne veszhessenek el (ld. 4.5 Naplózás tárkapacitása).
f) Erősíteni kell az informatikai rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jel észlelhető.

Az informatikai rendszerek felügyeletének támogatására javasolt a kritikus események bekövetkezése esetén rendszergazdának küldendő e-mail riasztást beállítani azokban a rendszerekben/rendszerelemekben, amelyek ezt lehetővé teszik. Erősíteni kell a rendszer felügyeletét és ellenőrizni kell a naplóbejegyzéseket minden olyan esetben, amikor fokozott kockázatra utaló jel tapasztalható.

Meghibásodás/nem megfelelő üzemelés, esetleges támadás esetén közvetlenül az észlelést követően a rendszer felügyeletéből gyűjtött információkat a biztonságért Felelős felé kell kommunikálni.

18.37. Biztonsági riasztások és tájékoztatások

A biztonságért Felelős feladata a jogszabályban kijelölt szervezettel, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel történő kapcsolattartás. A Felelős folyamatosan figyelemmel kíséri a tájékoztatásokat, kiadott riasztásokat és gondoskodik az informatikai rendszerekre vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről. Amennyiben a riasztás érinti a Hivatal felhasználóit, akkor a Hivatalnál szokásos módon, elektronikus levélben és/vagy intranetén keresztül értesíti a felhasználókat a riasztásban foglaltakról, a megtett védelmi intézkedésekről, valamint felhívja a felhasználók figyelmét a felhasználói oldalról követendő magatartásra.

18.67. Információ kezelése és megőrzése

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

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

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

A kimeneti információk kezelése során figyelembe kell venni az információ minősítését. A mindenkori biztonsági osztályok függvényében kerülnek meghatározásra a szabályozások arra vonatkozóan, hogy miként kell eljárni a bizonyos adatokkal, dokumentumokkal.
További elvárásokat a Hivatal további szabályzatai tartalmaznak (pl. Iratkezelési Szabályzat).

19. ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSE

19.1. Ellátási láncra vonatkozó kockázatelemzési és kockázatkezelési eljárásrend

Az ellátási láncból eredő kockázatok kezelése érdekében a jelen eljárásrendet kell alkalmazni. A Hivatal kockázatkezelése az ellátási lánc kockázataira is kiterjed, az 1.10. Kockázatmenedzsment stratégia részeként a céljainak, az ellátási láncnak a biztosításához szükséges kritikus technológiák, termékek és szolgáltatások beszállítóit azonosította, mely alapesetben a Hivatal által üzemeltetett informatikai rendszereket biztosító rendszerelemek. Az elektronikus információs rendszerek alapfunkcióit támogató kritikus rendszerelemek azonosítása az üzletmenet-folytonossági tervben történik, jelen fejezetben foglalt eljárások ezen informatikai rendszerekre vonatkoznak.

19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat

A Hivatal jelen Információbiztonsági szabályzatban dolgozta ki az ellátási láncra vonatkozó szabályokat, az 1.10.1. Kockázatelemzési és kockázatkezelési eljárásrend részeként kezeli az ellátási láncra vonatkozó követelményeket, az arra vonatkozó felülvizsgálati és megismerési előírásokkal.

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

A Hivatal olyan folyamatokat hoz létre, amelyek lehetővé teszik az ellátási lánc elemeiben és folyamataiban rejlő gyengeségek feltárását, az ellátási lánccal kapcsolatos kockázatok csökkentését, az esetleges eseményekből eredő károk minimalizálását (pl. beszállítók biztonsági követelményeinek meghatározásával, a szállítási folyamatok ellenőrzésével vagy a konfigurációk eredetiségének biztosításával). Ez magában foglalja a hardver-, szoftver- és firmware-fejlesztési folyamatok, szállítási eljárások, konfigurációs menedzsment eszközök, valamint a fizikai és személyi biztonsági programok vizsgálatát. A folyamatot az Ellenőrzési nyomvonal szabályzat szerint készített Ellenőrzési nyomvonalban kell dokumentálni és a folyamat folyamatgazdája felelős a meghatározott feladatok, tevékenységek megfelelő végrehajtásáért. Az ellátási láncért felelős személyt a jegyző jelöli ki.

19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók

A Hivatal a rendelkezésében lévő, az ellátási lánc biztosításához szükséges elektronikus információs rendszereivel kapcsolatos szerződések esetében gondoskodik arról, hogy az információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák, szükség esetén szerződésben is kiköti, hogy a fővállalkozóra vonatkozó információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozónak is teljesítenie kell.

19.13. Beszerzési stratégiák, eszközök és módszerek

A beszerzések során alkalmazandó stratégiákat, követelményeket és módszereket a 16.7. Beszerzések pont tartalmazza.

19.19. Értesítési megállapodások

A Hivatal nyilvántartja a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezeteket és azok elérhetőségét az Üzletmenet-folytonossági tervben. Olyan megállapodást kell kötni a szervezetekkel, amelyben meghatározzák a felelősségi köröket, biztonsági követelményeket és kommunikációs protokollokat (gyakorlat alapján a szerződés részeként kezelve valósul meg), szerződésben meg kell követelni a közreműködőtől, hogy a közreműködőnél fennálló információbiztonsági kockázatokat jelentős mértékben befolyásoló eseményeket haladéktalanul jelentse a Hivatal felé.

19.22. Rendszerek vagy rendszerelemek vizsgálata

A rendszergazdának új hardver/szoftver rendszerelemek beépítését megelőzően, ill. ha az informatikai rendszerek üzemeltetése, karbantartása során a rendszerelemek hamisítására utaló jeleket észlelnek, az 19.23. Rendszerelem hitelessége pont szerint ellenőrizniük kell a rendszerelemek sértetlenségét, hamisítástól mentességét. A rendszer kockázata (pl. Hivatal területén kívüli használat) és a benne tárolt adatok minősítése, mennyisége alapján a rendszergazda rendszeres ellenőrzést végez, minimálisan az éves karbantartási feladatok alkalmával. Gyanús esemény észlelését követően szintén ellenőriznie kell a rendszer sértetlenségét, hamisítástól való mentességét.

19.23. Rendszerelem hitelessége

A rendszergazdának az esetleges hamisítás felderítése érdekében minden új hardver/szoftver rendszerelemet ellenőriznie kell, mielőtt azt beépítené, alkalmazná az informatikai rendszerekben.

A rendszerelemek hamisítására utaló jelek lehetnek:

a) hardver eszközök gyanús eredete (pl. nem hivatalos forgalmazótól vagy ismeretlen forrásból származó eszközök; gyanúsan alacsony ár);
b) hardver eszközök gyanús csomagolása (pl. hiányzó vagy sérült gyári plombák; rossz minőségű logók; rossz minőségben nyomtatott dokumentáció; helyesírási hibák a címkéken vagy a dokumentációban);
c) hardver eszközök eltérő gyártói azonosítói (pl. szokatlan sorozatszámok; hiányzó vagy manipulált QR-kódok, hologramok);
d) hardver eszközök gyártási eltérései (pl. eredetitől eltérő specifikáció; silány anyagminőség);
e) hardver eszközök gyanús működése (pl. elvárnál alacsonyabb teljesítmény; instabil működés, gyakori meghibásodás);
f) szoftverek gyanús forrása (nem hivatalos weboldalról letöltés);
g) szoftverek gyanús telepítési folyamata (feltört vagy generált licenckulcsok, ismeretlen kódok futtatása a szoftver telepítésekor);
h) szoftverek digitális aláírásának hiánya (hiányzó vagy érvénytelen digitális aláírás; az operációs rendszer figyelmeztetése a szoftver indításakor);
i) szoftverek gyanús működése (gyanús hálózati forgalom ismeretlen szerverekkel; nem kívánt hirdetések vagy felugró ablakok; vírusírtó vagy tűzfal riasztásai);
j) szoftverek felhasználói felületének eltérései (rossz minőségű ikonok; a felhasználói felület elavult dizánja; eredetihez viszonyítva hiányzó vagy extra funkciók).

Amennyiben a rendszergazda a hamisított rendszerelemet észlel, tilos ezeket a rendszerelemeket beépíteni vagy alkalmazni az informatikai rendszerben, és értesítenie kell a hamisított rendszerelemről és a forrásáról a biztonságért Felelőst, aki szükség szerint felveszi a kapcsolatot a hatóságokkal.

19.24. Rendszerelem hitelessége – Hamisítás elleni képzés

A rendszergazda számára tartott szerepkör alapú képzés keretében ismertetni kell a hamisított rendszerelemek (beleértve a hardvert, szoftvert és firmware-t) felismerésének módszereit (ld. 3.9. Szerepkör alapú biztonsági képzés)

19.25. Rendszerelem hitelessége – Konfigurációfelügyelet

Az informatikai rendszerek rendszerelemeire vonatkozóan a szervizelés és javítás folyamán is figyelemmel kell kísérni a rendszerelemek konfigurációjának változásait az alábbi előírások betartásával:

a) A Hardver és szoftver nyilvántartás vezetésével naprakész nyilvántartást kell vezetni az informatikai eszközök hardver/szoftver konfigurációjáról (ld. 6.36. Rendszerelem leltár).
b) Az eszközök szervizelését dokumentálni kell és a külső szervizben elvégzett alkatrész cserék, módosítások nyomon követése érdekében a szerviz munkalapokat meg kell őrizni a 18.2. Hibajavítás pont szerint.
c) A külső szervizből visszaérkezett, javított eszközök konfiguráció változását az üzembe helyezés során ellenőrizni kell, és a módosult konfigurációt át kell vezetni a hardver és szoftver nyilvántartásokon.

19.27. Rendszerelem selejtezése, megsemmisítése

A felhasználóknak a feleslegessé vált informatikai eszközeiket a rendszergazdának kell átadni, aki a tartalék eszközök tárolására kijelölt helyiségbe helyezi át.

Az informatikai rendszerek részét képező informatikai eszközöket, adathordozókat, dokumentációkat olyan technikákkal és módszerekkel kell selejtezni, amely megakadályozza, hogy az informatikai rendszerből származó adatok illetéktelen személyek tudomására jussanak. Ennek érdekében a selejtezés során a 11.1. Adathordozók védelmére vonatkozó eljárásrend szerint kell eljárni.

A rendszergazda kezdeményezi az eszköz selejtezését amennyiben az eszköz

a) elhasználódott,
b) hibás és nem – vagy csak gazdaságtalanul – javítható (mellékelendő a javítással megbízott külső szerviz szakvéleménye);
c) vagy az eszköz technikailag elavult és a Hivatalon belül már nem hasznosítható.

Az informatikai eszközök selejtezése csak a jegyző tudtával és jóváhagyásával történhet.

A selejtezés előtt a rendszergazda az eszköz még hasznosítható tartozékait, alkatrészeit kiszereli és az 11.8. Adathordozók törlése pontban leírtak szerint gondoskodik az informatikai eszközben lévő adathordozók törléséről. Az eszköz selejtezését a vonatkozó szabályzatok szerint kell lefolytatni és az eszközt a hardver- és szoftver nyilvántartásokból is ki kell vezetni (ld. 6.36. Rendszerelem leltár).

MELLÉKLET

1. melléklet: Elektronikus információs rendszerek nyilvántartása, jegyzői nyilatkozat
(A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet felé a Kiberbiztonsági tv. 8. § (4) bekezdésben meghatározott bejelentés része)

Hatályos: 2025.11.26.

Szerencsi Közös Önkormányzati Hivatal

3900 Szerencs, Rákóczi út 89.

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

1. melléklet

Elektronikus információs rendszerek nyilvántartása, jegyzői nyilatkozat

jóváhagyta:

.....

Dr. Béni Gyula

jegyző

Dokumentum története

Verzió	Készült	Változás oka
1.0	2025.11.03.	Új kiadás Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény alapján

1. melléklet - Elektronikus információs rendszerek nyilvántartása, jegyzői nyilatkozat

A Szerencsi Közös Önkormányzati Hivatal Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) 1. § (1) bekezdés a) pontja szerinti, az 1. mellékletben felsorolt, közigazgatási ágazathoz tartozó szervezet. Az 1. § (3) bekezdése alapján - a település által nyújtott szolgáltatásnak az állam, a társadalom, a gazdaság működése szempontjából való kritikussága, valamint a Hivatal mérete alapján - **fontos szervezetnek minősül.**

A Hivatal meghatározta a Kiberbiztonsági tv. 8. § (4) alapján a meglévő, rendelkezésében lévő elektronikus információs rendszereinek biztonsági osztályát, valamint felmérte az elektronikus információs rendszerekhez kapcsolódó védelmi intézkedéseket, azok megfelelőségét és státuszát. A Hivatal az MK rendeletben foglalt védelmi intézkedésektől nem tér el, helyettesítő védelmi intézkedéseket nem alkalmaz.

Jelen dokumentum a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet felé a 7/2024. (VI. 24.) MK rendeletben meghatározott tartalmú bejelentés, az Elektronikus információs rendszerek biztonsági osztályba sorolása kérelem és az NBSZ-OVI űrlapokhoz tartozó adatszolgáltatás része.

A Hivatal az elektronikus információs rendszerei biztonsági osztályát a Kiberbiztonsági tv. 6. § (10) c) alapján „alap" biztonsági osztályban határozta meg, legfeljebb csekély káresemény következhet be, mivel:

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

A Szerencsi Közös Önkormányzati Hivatal jegyzője a táblázatokban szereplő, szakfeladatai támogatására használt üzemelő és archív elektronikus információs rendszerekről nyilatkozik, kéri a felsorolásban szereplő EIR-ek elektronikus információs rendszerek biztonsági osztályba sorolásának hatósági nyilvántartásba történő bejegyzését.

Jelenleg nincsen tervezett elektronikus információs rendszer, a Hivatal nem kéri fejlesztés alatt álló elektronikus információs rendszer előzetes biztonsági osztályba sorolásának hatósági nyilvántartásba történő bejegyzését.

A Hivatal kéri a hatóságtól, hogy jelen Elektronikus információs rendszerek nyilvántartásában nem szereplő, korábban az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) 8. § (1) bekezdésének megfelelően benyújtott adatok alapján **hatósági nyilvántartásba bejegyzett elektronikus információs rendszereket a hatósági nyilvántartás működő rendszerei közül törölje**: azokat a Hivatal nem használja, kivezetését kéri és/vagy azok nem Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény hatálya alá tartozó EIR-ek, ill. más néven/ csoportosításban tartja nyilván.

A Hivatal az EIR nyilvántartást egy korlátozottan, csak az érintetteknek hozzáférhető belső elektronikus nyilvántartásban kezeli, mely jelen Elektronikus információs rendszerek nyilvántartásában szereplő adatok alátámasztásán kívül tartalmazza az adatgazdai terület nevét/ az adatgazda nevét és elérhetőségét, ill. az adatgazdai terület részéről a rendszerben kezelt adatokért felelős kulcsfelhasználó nevét és elérhetőségét is.

Az adatosztályozás a Hivatal rendelkezésében lévő elektronikus információs rendszerekben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából. Célja, hogy a rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szempontjából értékelésre kerüljenek és azok biztonsági súlyának megfelelően kerüljön kialakításra a kockázatarányos védelem. Hozzájárul az elektronikus információs rendszerben kezelt adatok külföldön vagy felhőben történő kezelésének egyértelmű meghatározásához.

Az adatosztályozást a biztonságért Felelős az adatgazdák bevonásával végezte. Ennek keretében azonosították a rendszer által feldolgozott, tárolt és továbbított adatok típusait, majd az adatok és a rendszer tekintetében vizsgálták a bizalmasság, sértetlenség vagy rendelkezésre állás hatásértékét (alap, jelentős, magas). Figyelembe vették a logikailag együtt, egységben kezelt elektronikus adatok – ideértve az adatbázist, adattárat, egyedi dokumentumot és egyéb adatállományt – együttes biztonsági igényét, valamint az alábbi meghatározást:

- A kezelt adatok fajtája lehet személyes adat vagy különleges személyes adat,
- Az EIR-ben kezelt adatok mennyisége lehet csekély, közepes vagy nagy. Az EIR-ben kezelt adatok mennyisége akkor csekély, az adatkezelés akkor nem nagy számban történik, ha az adatkezelés érintettjeinek száma az adott népesség arányában csekély, az adatok mennyisége / az adatkezeléssel érintett természetes személyek száma nem éri el a Hivatal székhely település lakosságszámának 5%-át. Az adatkezelés mértékének meghatározása során figyelembe kell venni az adatkezelési tevékenység időtartamát vagy állandóságát, ill. azt, hogy az adatkezelési tevékenység földrajzi kiterjedése alapján a rendszerben tárolt adatok bizalmasságának sérülése vagy elvesztése milyen mértékben okozhat anyagi vagy reputációs veszteséget a szervezetnek vagy az érintetteknek.

A Hivatal nem privát felhőszolgáltatást vagy külföldi adatkezelést kizárólag az adatosztályozás alapján, annak eredményére figyelemmel vehet igénybe, amennyiben más jogszabály a felhőszolgáltatás igénybevételét, vagy a külföldi adatkezelést nem tiltja vagy korlátozza. A tervezett külföldi adatkezelésre vagy nem privát felhőhasználatra irányuló döntést megelőzően költség-haszon elemzést és kilépési tervet szükséges készíteni. A költség-haszon elemzés keretében a szervezet vizsgálja és kimutatja az aktuálisan alkalmazott technológiához képest a nem privát felhőszolgáltatás igénybevételével járó előnyöket és hátrányokat, a kilépési terv keretében megtervezi a felhőszolgáltatás alkalmazásáról a helyi környezetre vagy privát felhő használatára történő visszaállás lépéseit, annak következményeit és költségvonzatát.

A Hivatal vezetője abban az esetben dönthet a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele mellett, amennyiben a költség-haszon elemzés és a kilépési terv eredményei alapján a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele a szervezet számára megalapozottan előnyökkel jár. Az adatosztályozás felülvizsgálata a biztonsági osztályba sorolás vagy az elektronikus információs rendszerben kezelendő adatok körében bekövetkezett változás esetén szükséges.

Az adatok bizalmasság szerinti besorolása:

B1 szintű adatok: az adatok bizalmasságának sérülése vagy elvesztése nem, vagy csak elhanyagolható mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek.

B2 szintű adatok: az adatok bizalmasságának sérülése vagy elvesztése csak kis mértékben okozhat anyagi vagy reputációs veszteséget a szervezetnek.

B3 szintű adatok: az adatok bizalmasságának sérülése vagy elvesztése jelentős anyagi vagy reputációs veszteséget okozhat a szervezetnek.

B4 szintű adatok: az adatok bizalmasságának sérülése vagy elvesztése kritikus mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek.

Az adatok sértetlenség és rendelkezésre állás szerinti értékelése:

SR1: az adatok SÉRTETLENSÉGE VAGY RENDELKEZÉSRE ÁLLÁSA NEM KRITIKUS, az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek nem, vagy csak elhanyagolható mértékben okozhat anyagi vagy reputációs veszteséget.

SR2: az adatok SÉRTETLENSÉGE VAGY RENDELKEZÉSRE ÁLLÁSA KRITIKUS, az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek jelentős, vagy kritikus mértékű anyagi vagy reputációs veszteséget okozhat.

Az adatosztályozás eredménye:

Titkosítás:

A B2 szintű adatok esetén: ha technológiai szempontból lehetséges, gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

A B3–4 szintű adatok esetén: minden esetben gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

Az adatkezelés helyszíne: SR2 besorolású adatok esetén: Ha jogszabály másként nem rendelkezik, az adatok kezelésére földrajzi korlátozással kerülhet sor. Az adatok csak EGT-tagállam területén tárolhatók. Külföldi adat-tárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is.

Az adatkezelés lehetséges helyszínének meghatározásához összeadandó az adat B és SR kategóriájának megnevezésében szereplő számértéke. Ha jogszabály másként nem rendelkezik, a kapott eredmény alapján az adatok az alábbi F1–F4 kategóriákba sorolhatók, melyekre a következő előírások alkalmazandók:

F1: ha a B és SR összesített értéke: 2

Az F1 besorolású adatok:

- földrajzi korlátozás nélkül kezelhetők és tárolhatók
- nem privát felhőszolgáltatás igénybevétele esetén: korlátozás nélkül kezelhetők és tárolhatók.

F2: ha a B és SR összesített értéke: 3

Az F2 besorolású adatok:

- SR1 besorolású adatok esetén földrajzi korlátozás nélkül, SR2 besorolású adatok esetén kizárólag EGT tagállam területén,
- nem privát felhőszolgáltatás igénybevétele esetén:
- EGT tagállam területén kívül kizárólag az igénybe vett szolgáltatás vonatkozásában harmadik fél általi, a kiberbiztonsági hatóság honlapján közzétett lista szerinti kiberbiztonsági tanúsítással, audittal vagy engedélyezéssel rendelkező (a továbbiakban: harmadik fél által tanúsított) nem privát felhőben, vagy
- EGT tagállam területén belül akár nem tanúsított nem privát felhőben is kezelhetők és tárolhatók.

F3: ha a B és SR összesített értéke: 4

Az F3 besorolású adatok

- kizárólag EGT tagállam területén belül
- nem privát felhőszolgáltatás igénybevétele esetén:
- harmadik fél által tanúsított nem privát felhőben, vagy
- nem tanúsított nem privát felhőszolgáltatás igénybevétele esetén kizárólag Magyarország területén kezelhetők és tárolhatók.

F4: ha a B és SR összesített értéke: 5 vagy 6

Az F4 besorolású adatok

- kizárólag Magyarország területén,
- nem privát felhőszolgáltatás igénybevétele esetén:
- harmadik fél által tanúsított privát felhőben vagy
- kormányzati felhőben kezelhetők.

	A	B	C
1	B1	F1	F2
2	B2	F2	F3
3	B3	F3	F4
4	B4	F4	F4

A Hivatal az EIR nyilvántartást egy korlátozottan, csak az érintetteknek hozzáférhető belső elektronikus nyilvántartásban kezeli, mely jelen Elektronikus információs rendszerek nyilvántartásában szereplő adatok alátámasztásán kívül tartalmazza az adatgazdai terület nevét/ az adatgazda nevét és elérhetőségét, ill. az adatgazdai terület részéről a rendszerben kezelt adatokért felelős kulcsfelhasználó nevét és elérhetőségét is.

A Hivatal rendelkezésében lévő, üzemelő vagy archív (lekérdezésre, átmeneti ideig használt) elektronikus információs rendszerek, támogató rendszerek:
azon rendszerek, amelyek felett a Hivatal rendelkezik, a rendszerek védelméhez kapcsolódó követelményeket maga határozza meg és gondoskodik azok alkalmazásáról

#	EIR / EIR modul, alrendszer				Adatosztályozás			
	megnevezése	leírása, az alapfeladat és biztosítandó szolgáltatások	állapota	BO	kezelt adatok	B szerint	SR szerint	eredmény
1.	**Alap informatikai infrastruktúra (Infra)** Alkalmazói rendszereket kiszolgáló hardver- és hálózati eszközök, alap informatikai szolgáltatások és biztonságtechnikai alrendszerek. Üzleti cél: Alap informatikai szolgáltatások, védelmi megoldások biztosítása							
1/1	Munkaállomások	Felhasználói számítógépek és perifériák, kliens operációs rendszerek	üzemelő	alap	Adathordozókon lévő adatok	B2	SR1	F2
1/2	Nyomtatók	Helyi és hálózati nyomtatók	üzemelő	alap	Címjegyzékben szereplő adatok (név, email)	B1	SR1	F1
1/3	Hálózat	Helyi vezetékes és vezetéknélküli hálózat, aktív eszközök, optikai hálózati elemek, tűzfalak	üzemelő	alap	Hálózaton továbbított adatok	B2	SR1	F2
1/4	Vírusirtó	Vírusdefiníciós adatbázisok frissítése, kliens számítógépek menedzselése	üzemelő	alap	Számítógépek vírusvédelmi információi	B1	SR1	F1
1/5	Mentőszerver (MS)	Mentőszerver (hálózati adattároló NAS/fájlszerver) Központi adatmentés	üzemelő	alap	Felhasználók által tárolt adatok	B2	SR1	F2
1/6	Fájlszerver (FS)	Fájlszerver (fájlmegosztó NAS/szerver) Hálózati fájlmegosztást végző szerver, osztott munkavégzést támogató hálózati erőforrások	üzemelő	alap	Felhasználók által tárolt adatok	B2	SR1	F2
1/7	Levelező szerver	Hivatali ügyintézéssel kapcsolatos levelezés	üzemelő	alap	E-mailcímek, levéltörzsben és csatolmányban szereplő személyes adatok	B2	SR1	F2
1/8	HK Control Beléptetőrendszer	Hikvision beléptető rendszer belépésre jogosult munkavállalók és munkaidő nyilvántartása céljából	üzemelő	alap	Munkavállalók adatai (név). Belépőkártyák, belépési jogosultságok, belépési napló adatok. Személyes, csekély.	B2	SR1	F2
2.	**Ügyviteli rendszer (Ügyviteli)**							
2/1	HVR	Helyi Vizual Regiszter Személyiadat- és lakcímnyilvántartás	üzemelő	alap	Személyi- és lakcímadatok	B2	SR1	F2
2/2	WEBIKSZ	Szociális igazgatásban szereplő ellátások nyilvántartása	üzemelő	alap	Szociális ellátásban részvevő személyek személyes adatai, az ellátás típusa, annak folyósítási ideje, határozatai. Különleges személyes adatot nem kezel	B2	SR1	F2
2/3	Mikrovoks	Intelligens szavazatszámláló és konferencia rendszer; Tanácsteremben használt szavazórendszer	üzemelő	alap	Közérdekből nem nyilvános információk, testületi ülések hanganyagai, képviselők adatai. Személyes, csekély, nem kerül sor különleges adatok kezelésére	B2	SR1	F2

Más szervezet rendelkezésében lévő elektronikus információs rendszerek

azon rendszerek, amelyeket a Hivatal feladatai ellátásához igénybe vesz, használ, a rendszerek védelméhez kapcsolódó követelményeket nem maga határozza meg, azokat kötelezően betartja:

#	**központi rendszer** az egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan igénybe vesz a Hivatal		
	megnevezése	**leírása (alapfeladat, biztosítandó szolgáltatások)**	**rendelkezési jogot gyakorló szervezet**
1	ASP	Önkormányzati ASP rendszer: - ASP KERET, Keretrendszer, ASP szolgáltatások menedzsment rendszere - ASP Adó, központi és helyi adók, az adók módjára behajtandó köztartozások, díjak, pótlékok, bírságok, a közigazgatás hatósági eljárási illeték elszámolása, kezelése, az adókötelezettségek teljesítésével kapcsolatos ügyek elektronikus úton történő intézése - ASP Gazdálkodási, az államháztartás szervezeteinek pénzügyi és számviteli feladatainak ellátása, a jogszabályokban előírt adatszolgáltatási kötelezettségek ellátásának biztosítása - ASP Hiba- és Igénybejelentő, Önkormányzati ASP- támogató rendszer - ASP Ingatlanvagyon-kataszter, az önkormányzati tulajdonban lévő ingatlanok helyrajzi számon alapuló egységes szerkezetben történő egyedi nyilvántartása - ASP Ipar-kereskedelmi, önkormányzati hatáskörbe utalt ipari és kereskedelmi igazgatási ügyek ügyintézésének teljes körű elektronikus támogatása - Települési Portál (opc.) települési hír- és információs honlap, közvetlen hozzáférés az elektronikus ügyintézői felületet (E-önkormányzat portál) szolgáltatásaihoz - ELÜGY Elektronikus ügyintézési Portál, E-önkormányzat portál - ASP Hagyatéki leltár, az önkormányzatok hagyatéki ügyekkel kapcsolatos nyilvántartási és ügyintézési feladatainak támogatása - ASP Iratkezelő, iratkezelési és általános ügyintézési tevékenységek támogatása - ASP NTAK Turisztikai Adatszolgáltató Központ, a turisztikai ágazat adatszolgáltatásával kapcsolatos jegyzői feladatok, ellenőrzések támogatása	Magyar Államkincstár
2	ASZA	Anyakönyvi Szakrendszer: - ASZA - Anyakönyvi Szolgáltató Alrendszer - TSZR - Települési Szolgáltató Rendszer - KCR - Központi Címregiszter - EAK - Elektronikus Anyakönyvi Rendszer - Cím és Körzetnyilvántartás - Választási üzemmód alkalmazásai: - NVR - Nemzeti Választási Rendszer - VÁKIR - Választási Kommunikációs és Információs Rendszer - VPIR/VLOG - Választási pénzügyi és logisztikai feladatok ellátására szolgáló rendszer	Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
3	CSTINFO	Családtámogatási Ellátási és Támogatási Információs Rendszer A családtámogatási ellátásokban részesülők nyilvántartása – szociális nyilvántartás	Magyar Államkincstár
4	E-adat	Magyar Államkincstár Internetes információs és adatszolgáltatási portál	Magyar Államkincstár

5	EBR 42	BM Önkormányzati információs Rendszer Helyi önkormányzatok és Többcélú Kistérségi Társulások hozzájárulásainak és normatív, kötött felhasználású támogatásainak igénylési, elszámolási rendszere. Pályázati lehetőségek pl. Vis Maior benyújtása	Belügyminisztérium Nyilvántartások Vezetéséért Felelős Helyettes Államtitkárság
6	E-ING	Elektronikus ingatlan-nyilvántartás, a Takarnet Földhivatali Információs Rendszer felváltására Elektronikus úton történő Földhivatali szolgáltatások, tulajdonjog bejegyzés, módosítás és törlés	Közigazgatási és Területfejlesztési Minisztérium
7	EKR	Elektronikus Közbeszerzési Rendszer Közbeszerzési eljárások elektronikus lebonyolításának támogatása, tenderfelhívások közzététele	Közigazgatási és Területfejlesztési Minisztérium
8	EPER BURSA	Eper Bursa Hungarica Bursa Hungarica ösztöndíjban részesülő hallgatók nyilvántartása	Emberi Erőforrás Támogatáskezelő Köznevelési és Felsőoktatási Támogatások Igazgatósága
9	EPER IPR	Eper Elektronikus Pályázatkezelési és Együttműködési Rendszer	Nemzeti Kulturális Támogatáskezelő
10	EPTK	Elektronikus Pályázó Tájékoztató és Kommunikációs Rendszer. FAIR alrendszer, kommunikációs felület a támogatást igénylő, kedvezményezett, valamint a fejlesztéspolitikai intézményrendszer között;	Közigazgatási és Területfejlesztési Minisztérium
11	ESZENY	Egészségügyi szolgáltatás nyújtásával kapcsolatos elektronikus ügyintézéshez használt rendszer. HENYIR alrendszer, az alkalmazás segítségével az egészségügyi dolgozók foglalkoztatásával kapcsolatos adatokat tartalmazó űrlap beküldését lehet elvégezni.	Nemzeti Népegészségügyi és Gyógyszerészeti Központ
12	HKP	Hivatali kapu, értesítési tárhely NISZ biztonságos kézbesítési szolgáltatás és kapcsolódó kézbesítési tárhelyek. KÜNY-tárhely, hivatali tárhely-, cégkapu szolgáltatás. Földbérlet, föld adás-vétel kifüggesztése, közzététele, kapcsolattartás a felügyeleti szervekkel	Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
13	KHRR	Közszolgálati Személyügyi Szolgáltatási Keretrendszer, Kormányzati Személyügyi Központ - TARTINFOR - Tartalékállomány információs rendszer - TÉR - Közszolgálati Teljesítmény Értékelő Rendszer - KÖZSZOLGÁLLÁS - Közszolgálati állásportál	Kormányzati Személyügyi Központ
14	IJR LocLex	IJR Integrált Jogalkotási Rendszer - LocLex: Az önkormányzati rendeletek előkészítése, a módosításokkal egységes szerkezetű önkormányzati rendeletek szövegének előállítása és publikálása.	Igazságügyi Minisztérium
15	KBA	Közbeszerzési Adatbázis Közbeszerzési eljárások központi nyilvántartása, közbeszerzési eljáráshoz és az ajánlatkérő szervezethez kapcsolódóan tárolja a közbeszerzésekkel kapcsolatos adatokat és dokumentumokat	Közbeszerzési Hatóság
16	KGR K11	Költségvetési Gazdálkodási Rendszer Online adatszolgáltató rendszer (pénzügyi adatszolgáltatások, mérlegjelentések, költségvetés, beszámolók). Jelentés a támogatás alapú közpénzek felhasználásáról (normatív támogatás) MÁK felé	Magyar Államkincstár
17	KIR	Köznevelési Információs Rendszer Az Oktatási Hivatal által működtetett, a köznevelés feladataiban közreműködők által szolgáltatott adatokra épülő országos elektronikus nyilvántartási és adatszolgáltatási rendszer. A fenntartó vagy a köznevelési intézmény képviseletére jogosult személy, a közigazgatási szerv képviselője és a jegyző együttes adatszolgáltatása KIR szakrendszerekbe (gyermek, tanulói, illetve alkalmazotti és intézményi adatok). nyilvántartása	Oktatási Hivatal
18	KIRA	Központosított illetményszámfejtési rendszer Foglalkoztatottak, jogviszonyban állók személyi juttatásainak (illetmények, juttatások), egészségbiztosítási ellátások és a munkáltatókat terhelő közterheknek elszámolása	Magyar Államkincstár
19	KSH-Elektra	Központi Statisztikai Hivatal Adatgyűjtő és Adatszolgáltató rendszere. Statisztikai célú elektronikus adatgyűjtés, statisztikai jelentések, kimutatások	Központi Statisztikai Hivatal

20	KSZDR	Kormányzati Személyügyi Döntéstámogató Rendszer Személyi és szervezeti adatok feltöltése, személyzetpolitikához létszám- és illetményadatok, előmeneteli és illetményrendszer országos működtetéséhez szükséges létszám- és illetményadatok, esetenkénti adatszolgáltatás, statisztikai lekérdezések biztosítása	Kormányzati igazgatási szerv
21	KSZNY	KSZNY közigazgatási szankciók nyilvántartása Hatósági eljárásban kiszabott helyszíni bírság szankciók nyilvántartása, szankciót megállapító döntések (figyelmeztetés, közigazgatási bírság, tevékenység végzésétől eltiltás, elkobzás, egyéb közigazgatási szankció) bejegyzése	Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
22	KTK	Közfoglalkoztatási Támogatások Keretrendszere Közfoglalkoztatási Támogatások, közfoglalkoztatásban részt vevők bérköltség elszámolása a munkaügyi központ felé, pályázatok benyújtása (Foglalkoztatási osztály)	Nemzeti Foglalkoztatási Szolgálat
23	MEKH-EMIS	Energy Management Information System (EMIS) A Magyar Energetikai és Közmű-szabályozási Hivatal a közintézmények energiafelhasználásának és épületenergetikai, gépészeti adatainak összegyűjtését, kiértékelését és az arra épülő tanácsadást végzi a rendszerrel	Magyar Energetikai és Közmű-szabályozási Hivatal
24	NJT	Nemzeti Jogszabálytár Nemzeti rendelet-, jogszabálytár, kapcsolattartás a törvényességi felügyelettel üzenet formájában, rendeletek, jegyzőkönyvek, határozatok felvitele - NJT TFIK Törvényességi Felügyelet Írásbeli Kapcsolattartás Modul	Igazságügyi Minisztérium
25	OKNYIR	Országos kereskedelmi rendszer. Üzletek, kereskedők, vásárok, piacok, működési engedéllyel rendelkező és bejelentett üzletek kereskedelmi és szolgáltatási tevékenységgel összefüggő nyilvántartása	Jász-Nagykun-Szolnok Vármegyei Kormányhivatal
26	Önegm	Önkormányzati előirányzat-gazdálkodási modul, MÁK felé adatközlés. Szociális ellátások igénylése	Magyar Államkincstár
27	PROBONO	Közszolgálati tisztviselői, vezetői képzések nyilvántartása, tervezése	Nemzeti Közszolgálati Egyetem
28	PTR	Pénzbeli és Természetbeni Ellátások Rendszere Államigazgatás hatáskörében nyújtott, pénzbeni és természetbeni szociális juttatások, ellátások egységes nyilvántartása	Magyar Államkincstár
29	TeIR	Országos Területfejlesztési és Területrendezési Információs Rendszer Országos statisztikai adatok alapján a területfejlesztési és területrendezési döntések előkészítéséhez és meghozatalához nyújt segítséget	Közigazgatási és Területfejlesztés Minisztérium
30	TKKI	Helyi esélyegyenlőségi program Esélyegyenlőségi program nyilvántartásának kezelése, kapcsolattartás Szociális és Gyermekvédelmi Főigazgatóság	Helyi esélyegyenlőségi program Esélyegyenlőségi program nyilvántartásának kezelése, kapcsolattartás Szociális és Gyermekvédelmi Főigazgatóság

#	**központi szolgáltatás, támogató rendszer** a Hivatal részére jogszabály alapján kizárólagos joggal informatikai és elektronikus hírközlési szolgáltatást nyújtó központi szolgáltató által biztosított, jogszabályi kötelezés vagy egyedi megállapodás alapján igénybe vett szolgáltatás (az EIR alapműködési céljához kapcsolódó IT funkciók összessége) és támogató rendszerek		
	megnevezése, rövid neve	**leírása (alapfeladat, biztosítandó szolgáltatások)**	**rendelkezési jogot gyakorló szervezet**
1.	**Alap informatikai infrastruktúra (Infra)** Alkalmazói rendszereket kiszolgáló hardver- és hálózati eszközök, alap informatikai szolgáltatások és biztonságtechnikai alrendszerek. Üzleti cél: Alap informatikai szolgáltatások, védelmi megoldások biztosítása		
1	NTG	Nemzeti Távközlési Gerinchálózat NISZ Internet, kormányzati célú hírközlési szolgáltatás	NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
2	SZEÜSZ/KEÜSZ	SZEÜSZ Szabályozott elektronikus ügyintézési szolgáltatások KEÜSZ Központi elektronikus ügyintézési szolgáltatások - Űrlapbenyújtás-Támogatási Szolgáltatás (e-Űrlap Szolgáltatás) - Ügyintézői Azonosításra Visszavezetett Dokumentumhitelesítés - DHSZ (AVDH-DHSZ) - Biztonságos Kézbesítési Szolgáltatás (BKSZ) - DÁP eAzonosítás (Digitális Adattárca) - ePapír (EP) - Hozzájárulás Alapú Adatszolgáltatás (HAASZ) - Kormányzati Elektronikus Aláírás, Elektronikus Bélyegzés És Aláírás-Ellenőrzési Szolgáltatás (KEASZ-KEAESZ) - Központi Kormányzati Szolgáltatás Busz (KKSZB) - Összerendelési Nyilvántartás (ÖNY) - Rendelkezési Nyilvántartás (RNY)	Digitális Magyarország Ügynökség