579/4/2020. (V.05.) Igazgatói Utasítás

a Bükki Nemzeti Park Igazgatóság

INFORMATIKAI BIZTONSÁGI SZABÁLYZATÁRÓL

Hatálybalépés: 2020. május 05.

Készítette: .....
Misák István IBF

Szakmai ellenőrző:

.....
Kovács Károly

.....
Dudás György

Gazdasági ellenőrző: .....
Hegyi Tünde

BÜKKI NEMZETI PARK Igazgatóság 5. Eger

.....
Rónai Kálmánné
igazgató

Melléklet: Megismerési nyilatkozat

Kapják: Bükki Nemzeti Park Igazgatóság munkatársai elektronikus formában

Dokumentum leíró adatok			
Szervezet neve	Bükki Nemzeti Park Igazgatóság		
Dokumentum címe	NEMZETI PARK SZINTŰ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT		
Ügyiratszám:	579/4/2020		
Készítette:	Misák István IBF	Dátum:	2020.04.29.
Jóváhagyta:	Rónai Kálmánné igazgató	Dátum:	2020. 05. 05.
Adatvédelmi minősítés:	nem nyilvános	Verzió:	v4.0
A dokumentum leírása:	A BNPI minden szervezeti egységére érvényes informatikai biztonsági szabályok, ill. módszertani útmutatók		
A dokumentum felülvizsgálatának szükségessége:	1. Jogszabály változás, szervezeti változás		
	2. Évente		
	3. Lényeges informatikai fejlesztés megvalósulás		
A dokumentum karbantartásáért felelős:	általános igazgatóhelyettes		

A dokumentum változásai

Verzió:	Dátum:	Készítette:	Jóváhagyta:	A változások leírása:
v1.0	2014.02.03.	Kovács Károly informatikus	Dr. Horváth Ákos igazgató	Első, jóváhagyott változat
v2.0	2017.11.27	Dorkó Zsolt informatikus	Rónai Kálmánné igazgató	Jogszabályi követelmények változása miatt felülvizsgált változat
v3.0	2020.02.07	Kovács Károly informatikus	Rónai Kálmánné igazgató	Felülvizsgált változat
V4.0	2020.04.29.	Misák István IBF	Rónai Kálmánné igazgató	AM-tól kapott vélemények átvezetése, jogszabályi követelmények pontosítása

Tartalomjegyzék

I. ÁLTALÁNOS RÉSZ 7

I.1. AZ IBSZ CÉLJA 7
I.2. HATÁLY 7
I.2.1. Szervezeti-személyi hatály 7
I.2.2. Tárgyi hatály 8
I.2.3. Területi hatály 8
I.2.4. Időbeni hatály 8
I.3. AZ IBSZ FELÜLVIZSGÁLATA 8
I.3.1. Hatásköri és illetékességi szabályok 9
I.4. KAPCSOLÓDÓ DOKUMENTUMOK 9
I.4.1. Jogszabályok 9
I.4.2. Kapcsolódó szabványok, ajánlások 10
I.4.3. Az IBSZ-hez kapcsolódó belső dokumentumok 10
I.5. AZ IBSZ ÁLTALÁNOS KÖVETELMÉNYEI 12

II. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK 13

II.1. INFORMATIKAI BIZTONSÁGI SZABÁLYZAT 13
II.2. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY 13
II.3. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI 13
II.4. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA 13
II.5. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS 14
II.6. KOCKÁZATELEMZÉS 14
II.6.1. Kockázatelemzési és kockázatkezelési eljárásrend 14
II.6.2. Biztonsági osztályba sorolás 14
II.6.3. Biztonsági szintbe sorolás 15
II.6.4. Kockázatelemzés 16
II.7. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS – BESZERZÉSI ELJÁRÁSREND 17
II.7.1. Erőforrás igény felmérés 17
II.7.2. Beszerzések 17
II.7.3. Az elektronikus információs rendszerre vonatkozó dokumentáció 20
II.7.4. A védelem szempontjainak érvényesítése a beszerzés során 23
II.7.5. Külső elektronikus információs rendszerek szolgáltatásai 23
II.7.6. Folyamatos ellenőrzés 23
II.8. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK ÜGYMENET FOLYTONOSSÁGÁNAK TERVEZÉSE 23
II.8.1. Ügymenet folytonosságra vonatkozó eljárásrend 23
II.8.2. Folyamatos működésre felkészítő képzés 24
II.8.3. Az elektronikus információs rendszer mentései 24
II.8.4. Az elektronikus információs rendszer helyreállítása és újraindítása 25
II.9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – BIZTONSÁGI ESEMÉNYKEZELÉSI TERV 26
II.9.1. Biztonsági események figyelése 26
II.9.2. Biztonsági események meghatározása 26
II.9.3. Biztonsági események kategorizálása 26
II.9.4. Jelentés a biztonsági eseményekről 27
II.9.5. Jelentés a biztonság gyenge oldalairól 27
II.9.6. Jelentés a szoftverzavarokról 27
II.9.7. Tanulságok levonása a biztonsági eseményekből 28
II.9.8. Képzés a biztonsági események kezelésére 28
II.10. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ – SZEMÉLY – BIZTONSÁG 28
II.10.1. Információbiztonsági tevékenységek 28
II.10.2. Az információbiztonsági felelősségi rend meghatározása 29
II.10.3. Az Igazgató 29
II.10.4. Az IBF 30
II.10.5. Üzemeltetési Osztály vezetője 32
II.10.6. A rendszergazda 33
II.10.7. Az adatgazda 34
II.10.8. A szervezeti egység vezetője 34
II.10.9. A felhasználó 34
II.10.10. A munkaköri felelősség és az alkalmazás feltételei 35

II.10.11. Munkakörök, feladatok biztonsági szempontú besorolása ... *36*
II.10.12. A személyek ellenőrzése ... *36*
II.10.13. Eljárás jogviszony megszűnésekor ... *37*
II.10.14. Áthelyezések, átirányítások és kirendelések kezelése ... *38*
II.10.15. Harmadik felekkel kapcsolatos előírások ... *38*
II.10.16. Fegyelmi intézkedések ... *40*
II.10.17. Belső egyeztetés ... *40*
II.10.18. Viselkedési szabályok az interneten ... *40*
II.11. TUDATOSSÁG ÉS KÉPZÉS ... 44
II.11.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel ... *44*
II.11.2. Biztonság tudatossági képzés ... *44*
II.11.3. Belső fenyegetés ... *45*
II.11.4. Szerepkör vagy feladat alapú biztonsági képzés ... *45*
II.11.5. A biztonsági képzésre vonatkozó dokumentációk ... *45*

III. FIZIKAI VÉDELMI INTÉZKEDÉSEK ... 45

III.1. ALAPELVEK ... 45
III.2. A TERÜLETEK FIZIKAI BIZTONSÁGI KÖVETELMÉNYEI ... 46
III.2.1. Fizikai biztonság védősávja ... *46*
III.2.2. Belső terület ... *46*
III.2.3. Védett terület ... *46*
III.2.4. Érzékeny terület ... *47*
III.3. FIZIKAI BELÉPÉSI ENGEDÉLYEK ... 47
III.4. FIZIKAI BELÉPÉS ELLENŐRZÉSE ... 48
III.4.1. Fizikai belépések ... *48*
III.4.2. Fizikai belépések naplózása ... *48*
III.4.3. Vendégek kísérete ... *48*
III.4.4. Kulcsok megóvása ... *48*
III.4.5. Rendellenességek jelentése ... *49*
III.5. AZ INFOKOMMUNIKÁCIÓS ESZKÖZÖK BIZTONSÁGA ... 49
III.5.1. Az infokommunikációs eszközök elhelyezése és védelme ... *49*
III.5.2. „Üres asztal - üres képernyő" szabály ... *49*
III.6. FELÜGYELET ALÓL KIKERÜLŐ ESZKÖZÖK ... 50
III.7. ÁRAMELLÁTÓ BERENDEZÉSEK ÉS KÁBELEZÉS ... 50
III.8. VÉSZVILÁGÍTÁS ... 50
III.9. TŰZVÉDELEM ... 50
III.10. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM ... 51
III.11. HŐMÉRSÉKLET ÉS PÁRATARTALOM ELLENŐRZÉS ... 51
III.12. KARBANTARTÓK ... 51

IV. LOGIKAI VÉDELMI INTÉZKEDÉSEK ... 51

IV.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK ... 51
IV.1.1. Engedélyezés ... *51*
IV.1.2. Elektronikus információs rendszer kapcsolódásai ... *52*
IV.1.3. Belső rendszerkapcsolatok ... *52*
IV.1.4. Külső kapcsolódásokra vonatkozó korlátozások ... *52*
IV.2. TERVEZÉS - BIZTONSÁGTERVEZÉSI ELJÁRÁSREND ... 53
IV.2.1. Rendszerbiztonsági terv ... *53*
IV.2.2. Cselekvési terv ... *53*
IV.2.3. Személybiztonság ... *53*
IV.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS ... 54
IV.3.1. A rendszer fejlesztési életciklusa ... *54*
IV.3.2. Funkciók, portok, protokollok, szolgáltatások ... *55*
IV.4. BIZTONSÁGI ELEMZÉS – BIZTONSÁGELEMZÉSI ELJÁRÁSREND ... 55
IV.4.1. Biztonsági értékelések ... *55*
IV.4.2. A biztonsági teljesítmény mérése ... *56*
IV.5. TESZTELÉS, KÉPZÉS, FELÜGYELET ... 59
IV.5.1. Tesztelési, képzési és felügyeleti eljárások ... *59*
IV.5.2. Sérülékenység teszt ... *59*

IV.5.3. Frissítési képesség *59*
IV.5.4. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően *60*
IV.5.5. Privilegizált hozzáférés *60*
IV.5.6. Felfedhető információk *60*
IV.6. KONFIGURÁCIÓKEZELÉSI ELJÁRÁSREND 60
IV.6.1. Alapkonfiguráció *60*
IV.6.2. A konfigurációváltozások felügyelete (változáskezelés) *60*
IV.6.3. Előzetes tesztelés és megerősítés *61*
IV.6.4. Biztonsági hatásvizsgálat *62*
IV.6.5. Konfigurációs beállítások *62*
IV.6.6. Legszűkebb funkcionalitás *62*
IV.6.7. Elektronikus információs rendszerelem leltár *62*
IV.6.8. A szoftver használat korlátozásai *62*
IV.6.9. A felhasználó által telepített szoftverek *63*
IV.7. RENDSZER KARBANTARTÁSI ELJÁRÁSREND 63
IV.7.1. Rendszeres karbantartás *63*
IV.7.2. A karbantartások engedélyezése *63*
IV.7.3. A karbantartások dokumentálása, nyilvántartása *63*
IV.7.4. A karbantartások ütemezése *64*
IV.7.5. Kiszállítás *64*
IV.7.6. A karbantartás ellenőrzése *64*
IV.7.7. Karbantartók *64*
IV.8. ADATHORDOZÓK VÉDELMÉRE VONATKOZÓ ELJÁRÁSREND 64
IV.8.1. Hozzáférés az adathordozókhoz, adathordozók használata *65*
IV.8.2. Adathordozók tárolása *65*
IV.8.3. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése *65*
IV.8.4. A hordozható infokommunikációs eszközök védelme *66*
IV.8.5. Mobil infokommunikációs eszközök ellopása esetén *66*
IV.8.6. Infokommunikációs eszköz elvesztése *66*
IV.9. AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁSREND 66
IV.9.1. Azonosítás és hitelesítés (szervezeten belüli felhasználók) *66*
IV.9.2. Hálózati hozzáférés privilegizált fiókokhoz *66*
IV.9.3. Azonosító kezelés *67*
IV.9.4. A hitelesítésre szolgáló eszközök kezelése *67*
IV.9.5. A felhasználó felelősségi köre a jelszó használat során *68*
IV.9.6. A hitelesítésre szolgáló eszköz visszacsatolása *68*
IV.9.7. Hitelesítés kriptográfiai modul esetén *69*
IV.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) *69*
IV.9.9. Hitelesítés szolgáltatók tanúsítványának elfogadása *69*
IV.10. HOZZÁFÉRÉS ELLENŐRZÉSI ELJÁRÁSREND 69
IV.10.1. Felhasználói fiókok kezelése *69*
IV.10.2. Kiemelt jogosultságok kezelése *71*
IV.10.3. Hozzáférési jogok igénylésének eljárásrendje *71*
IV.10.4. Hozzáférés ellenőrzés érvényre juttatása *72*
IV.10.5. Sikertelen bejelentkezési kísérletek *73*
IV.10.6. A rendszerhasználat jelzése *73*
IV.10.7. A munkaszakasz zárolása *73*
IV.10.8. Képernyőtakarás *73*
IV.10.9. A munkaszakasz lezárása *73*
IV.10.10. Távoli hozzáférés *73*
IV.10.11. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek *74*
IV.10.12. Vezeték nélküli hozzáférés *74*
IV.10.13. Mobil eszközök hozzáférése *74*
IV.10.14. Titkosítás *75*
IV.10.15. Külső elektronikus információs rendszerek használata *75*
IV.10.16. Nyilvánosan elérhető tartalom *75*
IV.11. RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉGRE VONATKOZÓ ELJÁRÁSREND 75
IV.11.1. Hibajavítás *76*
IV.11.2. Kártékony kódok elleni védelem *76*

IV.11.3. Az elektronikus információs rendszer felügyelete *78*
IV.11.4. Biztonsági riasztások és tájékoztatások *79*
IV.11.5. A kimeneti információ kezelése és megőrzése *79*
IV.12. NAPLÓZÁSI ELJÁRÁSREND 79
IV.12.1. Naplózható események *79*
IV.12.2. Naplóbejegyzések tartalma *80*
IV.12.3. Napló tárkapacitás *80*
IV.12.4. Naplózási hiba kezelése *80*
IV.12.5. Időbélyegek *80*
IV.12.6. Szinkronizálás *80*
IV.12.7. A napló információk védelme *81*
IV.12.8. A naplóbejegyzések megőrzése *81*
IV.12.9. Naplógenerálás *81*
IV.13. RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELMI ELJÁRÁSREND 81
IV.13.1. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem *81*
IV.13.2. A határok védelme *82*
IV.13.3. Kriptográfiai kulcs előállítása és kezelése *84*
IV.13.4. Kriptográfiai védelem *84*
IV.13.5. Együttműködésen alapuló számítástechnikai eszközök *85*
IV.13.6. A folyamatok elkülönítése *85*
V. MELLÉKLETEK 86
1. SZÁMÚ MELLÉKLET – ÉRTELMEZŐ RENDELKEZÉSEK 87
2. SZÁMÚ MELLÉKLET – AZ IGAZGATÓSÁG ELEKTRONIKUS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGI OSZTÁLYBA SOROLÁSA 92
3. SZÁMÚ MELLÉKLET – BIZTONSÁGI ESEMÉNYEK JELENTÉSE 95
4. SZÁMÚ MELLÉKLET – KOCKÁZATELEMZÉSI ÉS KEZELÉSI MÓDSZERTAN 96
5. SZÁMÚ MELLÉKLET – JOGOSULTSÁGIGÉNYLÉSI ŰRLAP 100
6. SZÁMÚ MELLÉKLET – HOZZÁFÉRÉSEK NYILVÁNTARTÁSA ŰRLAP 101
7. SZÁMÚ MELLÉKLET – FELHASZNÁLÓI INFORMATIKAI BIZTONSÁGI HÁZIREND 102
8. SZÁMÚ MELLÉKLET – FELHASZNÁLÓI NYILATKOZAT 115
9. SZÁMÚ MELLÉKLET – INFORMÁCIÓBIZTONSÁGI TÁJÉKOZTATÓ JOGVISZONY MEGSZŰNÉSE ESETÉN 116
10. SZÁMÚ MELLÉKLET – TITOKTARTÁSI NYILATKOZAT 117
11. SZÁMÚ MELLÉKLET – IRATOK NEM KORMÁNYZATI E-MAIL CÍMRE TÖRTÉNŐ KIKÜLDÉSÉNEK IGÉNYLÉSE ŰRLAP 118

I. Általános rész

I.1. AZ IBSZ CÉLJA

Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) biztonságkezelési elveket, követelményeket és szabályokat tartalmaz a Bükki Nemzeti Park Igazgatóságnál (továbbiakban: az Igazgatóság) tevékenykedő személyek (bizonyos feltételek esetén külső közreműködők) számára, akik felelősek az információbiztonság fejlesztéséért, megvalósításáért és megtartásáért. Az IBSZ hatékonyan támogatja az Igazgatóság biztonságkezelésének mindennapi gyakorlatát, illetve megfelelő kereteket biztosít az Igazgatóság teljes körű biztonsági szabályozásához.

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

a) A jogkövető magatartás és a jó hírnév érdekében védeni a szervezet értékeit,

b) A tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot,

c) A megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel segíteni az intézkedések érvényesítését.

A jelen IBSZ az Igazgatóság szervezeti szintű információbiztonsági szabályozó rendszerének egyik alapvető eleme. Az IBSZ a hatályos jogszabályokkal, az Igazgatóság működési és ügyrendi előírásaival összhangban megteremti az elektronikus információs rendszerek (továbbiakban: EIR vagy elektronikus információs rendszer) és az azokban kezelt adatok kockázatokkal arányos biztonságát. Tartalmazza az Igazgatóság elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, továbbá meghatározza azokat az elvárásokat, kötelezettségeket és a felelősséget, amelyekre a biztonságos információellátás érdekében szükség van.

Az Igazgatóságnak az Agrárminisztérium megfelelő anyagának figyelembe vételével, annak szerkezetét követve kellett elkészítenie saját szabályzatát. Ezek kialakításakor jelen anyagban szereplő tartalmi és formai elemeket kötelezően szerepeltetnie kellett, melyeket ki kellett egészíteni szervezetei sajátosságaiknak megfelelő szabályozási rendszerükkel. Kötelező formai elem az IBSZ kialakítása során a szerkezet, ez biztosítja, hogy az Ágazat valamennyi szervezetének IT biztonsági működését azonos felépítésű, a szabványnak megfelelő dokumentum szabályozza.

Az Igazgatóság informatikai szolgáltatóival kötött szolgáltatási szerződéseknek és azok mellékleteinek összhangban kell lenniük jelen IBSZ-szel.

I.2. HATÁLY

I.2.1. Szervezeti-személyi hatály

Az IBSZ szervezeti hatálya az Igazgatóság valamennyi olyan szervezeti egységére kiterjed, amely az Igazgatóság elektronikus információs rendszereit használja, üzemelteti, fejleszti, továbbá ilyen tevékenységeket irányít és ellenőriz.

Az IBSZ személyi hatálya kiterjed az Igazgatósággal munkavégzésre irányuló bármely jogviszonyban álló természetes és jogi személyre, tehát azokra, akik kapcsolatba kerülnek az Igazgatóság elektronikus információs rendszereivel (használják, fejlesztik, telepítik, üzemeltetik, javítják stb.), így:

a) a kormányzati szolgálati jogviszony alapján foglalkoztatott munkatársakra,

b) a közalkalmazotti jogviszony alapján foglalkoztatott munkatársakra,

c) a munkaviszony alapján foglalkoztatott munkatársakra,

d) az Igazgatósággal szerződéses kapcsolatban álló természetes és jogi személyekre,

e) más szervezetek képviseletében az Igazgatóság munkahelyein tartózkodó személyekre.

I.2.2. Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed az Igazgatóság adataival és adatainak kezelésével összefüggésben használt bármilyen adatrögzítésre, tárolásra, feldolgozásra vagy továbbításra képes elektronikus információs rendszerre és ezek működési környezetére.

A tárgyi hatály kiterjed továbbá az ezen rendszerek működéséhez alkalmazott szoftverekre, illetve az ezekkel rögzített, tárolt, feldolgozott vagy továbbított adatokra és információkra.

I.2.3. Területi hatály

Az IBSZ területi hatálya kiterjed az Igazgatóság egri székhelyére, valamint összes információbiztonsági szempontból releváns helyiségére (egyéb létesítmények), kirendeltségeire, illetve bizonyos feltételek mellett az elektronikus információs rendszerek szolgáltatóinak telephelyeire is.

I.2.4. Időbeni hatály

Jelen IBSZ a kiadás napján lép hatályba.

I.3. AZ IBSZ FELÜLVIZSGÁLATA

Az IBSZ eseti módosítására kerül sor, ha a benne szereplő adatok megváltoztak, illetve ha az IBSZ olyan kisebb mértékű kiegészítésekre szorul, amelyek nem érintik az aktuális biztonsági követelményeket.

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

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

Az IBSZ eseti módosításának, felülvizsgálatának kezdeményezése és a felülvizsgálat, valamint a módosítás elvégzése az elektronikus információs rendszerek biztonságáért felelős személy (továbbiakban: információbiztonsági felelős, rövidítve IBF) feladata. A módosítások engedélyezése és az újabb változat jóváhagyása az Igazgató hatásköre.

I.3.1. Hatásköri és illetékességi szabályok

Az IBSZ belső használatú dokumentum: az Igazgatóság elektronikus információs rendszerének felhasználói, illetve egyéb érintettek (az Igazgatósággal szerződéses kapcsolatban álló természetes és jogi személyek, más szervezetek képviseletében az Igazgatóság munkahelyein tartózkodó személyek) megismerhetik és birtokolhatják, de illetékteleneknek nem adhatják tovább.

I.4. KAPCSOLÓDÓ DOKUMENTUMOK

I.4.1. Jogszabályok

a) 2018. évi CXXV. törvény a kormányzati igazgatásról

b) 2012. évi I. törvény a munka törvénykönyvéről

c) 2012. évi C. törvény a Büntető Törvénykönyvről

d) 2013. évi V. törvény a Polgári Törvénykönyvről

e) 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

f) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (továbbiakban: Ibtv.)

g) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

h) AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

i) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Info tv.)

j) 2016. évi CL. törvény az általános közigazgatási rendtartásról

k) 1999. évi LXXVI. törvény a szerzői jogról

l) 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól;

m) 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

n) 146/1993. (X. 26.) Korm. rendelet a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény végrehajtásáról

o) 451/2016. (XII.19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól;

p) 466/2017. (XII.28.) Korm. rendelet az elektronikus ügyintézéssel összefüggő adatok biztonságát szolgáló Kormányzati Adattrezorról;

q) 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről (továbbiakban: technológiai vhr)

r) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról (továbbiakban: képzési rendelet)

I.4.2. Kapcsolódó szabványok, ajánlások

a) MSZ ISO/IEC 27002:2017: Az információbiztonság irányítási gyakorlatának kézikönyve;

b) MSZ ISO/IEC 27001:2014: Az információbiztonság irányítási rendszerei. Követelmények;

c) NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations;

d) NIST Special Publication 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations;

e) NIST Special Publication 800-55 –Performance Measurement Guide for Information Security

f) Open Web Application Security Project Testing Guide aktuális verziója

g) Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója

h) Open Web Application Security Project Mobile Security Testing Guide aktuális verziója

i) Open Web Application Security Project Mobile Application Security Verification Standard aktuális verziója

I.4.3. Az IBSZ-hez kapcsolódó belső dokumentumok

a) Szervezeti és Működési Szabályzat;

b) Adatvédelmi és Adatbiztonsági Szabályzat;

c) Iratkezelési Szabályzat;

d) Selejtezési Szabályzat;

e) Cselekvési terv a Bükki Nemzeti Park Igazgatóság elektronikus információs rendszereinek elvárt biztonsági osztályainak, illetve az Igazgatóság elvárt biztonsági szintjének elérésére;

f) Elektronikus információs rendszerek ügymenet-folytonossági terve;

g) Információbiztonsági kockázatelemzés.

Az Igazgatóságnak Igazgatósági Szintű Informatikai Biztonsági Szabályzattal, és ehhez szorosan kapcsolódó szabályozási dokumentum rendszerrel kell rendelkeznie. Ennek megfelelően az Informatikai Biztonsági Szabályzat a következő dokumentumokra hivatkozik:

Szabályozási terület		Szabályozás célja
•	Adathordozó kezelési szabályzat	Formális eljárás biztosítása a cserélhető adathordozók kezelésére a teljes életciklusukra vonatkozóan. Jelen dokumentumban szabályozva. /ld. 16. fej./
•	Az információbiztonsággal kapcsolatos intézkedések a projektvezetési szabályzatban	Az információbiztonsággal foglalkozni kell a projektvezetésben - tekintet nélkül a projektek típusára.
•	Beszerzési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **beszerzését** is.
•	Biztonsági szabályzat (fizikai biztonságra vonatkozóan)	Megelőzni a jogosulatlan fizikai hozzáférést, károkozást és zavarást a szervezet információi és információ feldolgozó eszközei vonatkozásában.
•	Eszközhasználati szabályzat	Biztosítani az információ feldolgozó eszközök helyes és biztonságos üzemelését.
•	Fejlesztési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **fejlesztését** is.
•	Felhasználói informatikai biztonsági útmutató	A felhasználók tájékoztatása a mindennapi munkájuk során betartandó szabályokról. Az IBSZ kivonata.
•	Hálózathasználati szabályzat	Minden hálózati szolgáltatásra meg kell határozni a biztonsági mechanizmusokat, a szolgáltatási szinteket és a kezelési követelményeket, és be kell építeni a hálózati szolgáltatási megállapodásokba.
•	Hozzáférés-felügyeleti szabályzat	Biztosítani a hozzáférést az arra jogosult felhasználók számára, és megelőzni a jogosulatlan hozzáférést a rendszerekhez és szolgáltatásokhoz.
•	IBSZ (Informatikai Biztonsági Szabályzat) a szervezetekre vonatkozóan	Az ágazati szintű biztonsági szabályozáshoz (jelen dokumentum) kapcsolódva a szervezeti szintű szabályozás megvalósítása.
•	Incidenskezelési szabályzat (biztonsági incidensre vonatkozóan)	Biztosítani egy következetes és hatásos módot az információbiztonsági incidensek kezelésére, beleértve a biztonsági események és gyengeségek kommunikációját is.
•	IT Üzemeltetési szabályzat	1. Biztosítani az információ feldolgozó eszközök helyes és biztonságos üzemelését; 2. Biztosítani, hogy az információk és az információ feldolgozó eszközök védettek legyenek a rosszindulatú szoftverek ellen (vírusvédelem); • Védekezni az adatvesztés ellen (mentés szabályozása); • Nyilvántartani az eseményeket, és létrehozni bizonyítékokat (naplózás szabályozása); • Biztosítani az üzemelő rendszerek sértetlenségét (telepítés szabályozása); • Megelőzni a műszaki sebezhetőségek kihasználását;

Szabályozási terület		Szabályozás célja
		• Ágazat specifikus szakrendszerek üzemeltetési szabályozása (üzemeltetési szabályozás).
•	IT változáskezelési szabályzat	Biztosítani kell, hogy az információbiztonság szerves része legyen az információs rendszereknek a teljes életciklus során, beleértve a rendszerek **fejlesztését** is.
•	Kockázatkezelési szabályzat	A szervezetnek fel kell mérnie azokat a kockázatokat, melyekkel foglalkozni kell ahhoz, hogy: 1. biztosítsák az információbiztonság-irányítási rendszertől elvárt eredmények elérhetőségét; 2. megelőzzék vagy csökkentsék a nem kívánt hatásokat. A szervezetnek szabályoznia kell az ezen kockázatokkal kapcsolatos tevékenységeket.
•	Mobil és távmunka biztonsági szabályzat	Biztosítani a távmunka és a mobil eszközök használatának biztonságát.
•	Munkaköri leírások, álláshelyen ellátandó feladatok	Az egyes munkakörökben elvárt információbiztonsági felelősségek, feladatok.

Amennyiben az Igazgatóság úgy ítéli meg, hogy esetében célszerűbb a fenti dokumentumok kialakítása helyett valamely kérdéskört közvetlenül az IBSZ-ben szerepeltetni, úgy ezt az adott helyen jelzi.

I.5. AZ IBSZ ÁLTALÁNOS KÖVETELMÉNYEI

Az IBSZ és a jelen IBSZ *{7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* melléklete (továbbiakban: FIBH) előírásainak alkalmazása, betartása, illetve betartatása, a *{I.2.1. Szervezeti-személyi hatály}* pontban megjelöltek számára kötelező.

Az információbiztonsági előírások betartása megvédi az Igazgatóságot és a *{I.2.1. Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

Titoktartási kötelezettség terhel minden, az Igazgatóság informatikai rendszereivel kapcsolatba kerülő természetes és jogi személyt, tekintet nélkül arra, hogy a kapcsolat milyen jogviszonyból ered. A titoktartási kötelezettség a szerződéses partnerek alvállalkozóira teljes körűen vonatkozik.

A titoktartási kötelezettség kiterjed a rendszerben kezelt adatokra, valamint a rendszer felépítésére, működési rendjére vonatkozó adatokra, a biztonsági rendszabályokra egyaránt. A titoktartási kötelezettség időkorlát nélkül áll fenn és az érintett személy a mindenkor érvényes jogszabályok alapján tartozik ezen kötelezettségéért felelősséggel.

Minden munkatárs (beleértve az ideiglenes, ill. megbízási szerződés alapján munkát végző munkatársakat is) csak Titoktartási nyilatkozat aláírása után kezdheti meg az érdemi munkát, kaphat hozzáférést információkhoz, erőforrásokhoz.

A munkatársak informatikai biztonsághoz kapcsolódó felelősségi és hatásköreit a „Munkaköri leírások” és az „Álláshelyen ellátandó feladatok” tartalmazzák, ennek hiányában az egyes álláshelyeken történő szabályozások vagy a FIBH előírásai érvényesek.

A felhasználók részére a FIBH tartalmaz egy kivonatot, melynek megismeréséről és betartásáról írásban nyilatkozniuk kell.

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

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

Az Igazgatóság elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

II. Adminisztratív védelmi intézkedések

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

II.1. INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az Igazgatóság Informatikai Biztonsági Szabályzatát a jelen dokumentum tartalmazza.

II.2. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁÉRT FELELŐS SZEMÉLY

Az Igazgatóságnak ki kell jelölnie vagy meg kell bíznia az elektronikus információs rendszer biztonságáért felelős személyt, aki ellátja az Ibtv. 13. §-ában meghatározott feladatokat. Az IBF feladatait, felelősségét és jogait a jelen IBSZ *{II.10.4. Az IBF}* fejezete tartalmazza.

II.3. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

Az IBF-nek a jelen IBSZ kiadását követően 90 napon belül intézkedési tervet kell készítenie a következő biztonsági szint, illetve a következő biztonsági osztály elérésére vonatkozóan.

Az intézkedési tervet az Igazgató hagyja jóvá. Az intézkedési tervet az IBF-nek évente felül kell vizsgálnia.

II.4. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK NYILVÁNTARTÁSA

Nyilvántartást kell vezetni az igazgatóság által működtetett valamennyi elektronikus információs rendszerről. A nyilvántartásnak minden elektronikus információs rendszerre nézve a következőket kell tartalmaznia:

a) az EIR nevét;

b) annak alapfeladatait;

c) biztonsági osztályba sorolását;

d) a rendszerek által biztosítandó szolgáltatásokat;

e) az érintett rendszerekhez tartozó licenc számot;

f) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatait;

g) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatait, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek személyazonosító és elérhetőségi adatait.

A nyilvántartást a rendszergazdának kell vezetnie és évente felülvizsgálnia.

II.5. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS ENGEDÉLYEZÉSI ELJÁRÁS

Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárásoknak ki kell terjedniük minden, az Igazgatóság hatókörébe tartozó:

a) emberi, fizikai és logikai erőforrásra;

b) eljárási és védelmi követelményszintre és folyamatra.

II.6. KOCKÁZATELEMZÉS

II.6.1. Kockázatelemzési és kockázatkezelési eljárásrend

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

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

Az Igazgatóság kockázatelemzési és kezelési eljárásrendjét az *{4. számú melléklet – Kockázatelemzési és kezelési módszertan}* tartalmazza.

II.6.2. Biztonsági osztályba sorolás

Az Igazgatóságnak az Ibtv. 7. § (3) bekezdésében meghatározottak figyelembevételével, a technológiai vhr 1. számú melléklete alapján biztonsági osztályba kell sorolnia az elektronikus információs rendszereit, illetve biztonsági szintbe kell sorolnia a szervezetét.

II.6.2.1. Biztonsági osztályba sorolás követelménye

Az Igazgatóság elektronikus információs rendszereit a technológiai vhr által előírt módon, külön-külön a bizalmasság, a sértetlenség és a rendelkezésre állás vonatkozásában egy 5 fokozatú skálán biztonsági osztályba kell sorolni.

A biztonsági osztályba sorolást az elektronikus információs rendszerben kezelt adat bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer sértetlenségének és rendelkezésre állásának sérülése esetén bekövetkező kár mértéke alapján kell elvégezni a technológiai vhr 1. mellékletében megadott szempontrendszer alapján.

A biztonsági osztályba sorolást kockázatelemzéssel kell alátámasztani.

A biztonsági osztályba sorolást újra el kell végezni, hogy ha

a) jelentős változás következik be az Igazgatóság szervezeti felépítésében;

b) az elektronikus információs rendszerben kezelt adatok bővülnek vagy az adatok köre változik;

c) változnak a hatályos információbiztonságra vonatkozó jogszabályok.

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

A biztonsági osztályba sorolást az IBF készíti elő az adatgazdákkal együttműködve és az Igazgató hagyja jóvá.

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

II.6.2.2. Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása

Az Igazgatóság a technológiai vhr alapján elvégezte az elektronikus információs rendszerek biztonsági osztályba sorolását.

A biztonsági osztályba sorolás eredményét a jelen IBSZ *{2. számú melléklet – Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása}* melléklete tartalmazza.

II.6.3. Biztonsági szintbe sorolás

Az Ibtv. 9. §-ának (1) és (2) bekezdései alapján a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet, valamint az elektronikus információs rendszer

a) fejlesztését végző,

b) üzemeltetését végző,

c) üzemeltetéséért felelős vagy

d) információbiztonságáért felelős

szervezeti egységeket az elektronikus információs rendszerek védelmére való felkészültségük alapján a szervezettől elvárt, eltérő biztonsági szintekbe kell sorolni jogszabályban meghatározott szempontok szerint.

II.6.3.1. Az Igazgatóság biztonsági szintbe sorolása

Az Ibtv. 9. §-ának (4) bekezdése alapján a szervezet vagy szervezeti egységek biztonsági szintjének meghatározását az elektronikus információs rendszer felhasználásának módja határozza meg, jogszabályban meghatározott szempontok szerint.

A technológiai vhr alapján

az Igazgatóság elvárt biztonsági szintje 4-es,

mivel

a) szakfeladatait támogató elektronikus információs rendszert használ (3-as szint)

b) személyes adatok formájában kritikus adatokat[1] kezel (3-as szint)

c) elektronikus információs rendszert üzemeltet (4-es szint).

II.6.3.2. Szervezeti egységek biztonsági szintbe sorolása

Az Igazgatóság hatályban lévő Szervezeti és Működési Szabályzata alapján az Igazgatóságnál az Üzemeltetési Osztály Informatikai Csoportja látja el az elektronikus információs rendszerek üzemeltetését az általános igazgatóhelyettes felügyelete mellett.

A technológiai vhr alapján

az Üzemeltetési Osztály Informatikai Csoport elvárt biztonsági szintje 4-es,

a) szakfeladatait támogató elektronikus információs rendszert használ (3-as szint)

b) személyes adatok formájában kritikus adatokat kezel (3-as szint)

c) elektronikus információs rendszert üzemeltet (4-es szint).

II.6.4. Kockázatelemzés

A kockázatelemzést a jelen IBSZ *{4. számú melléklet – Kockázatelemzési és kezelési módszertan}* mellékletében leírt módszertan alapján az IBF végzi el.

A kockázatelemzést évente el kell végezni, melynek során felül kell vizsgálni az előző évi kockázatelemzés eredményét. A kockázatelemzést soron kívül el kell végezni, hogy ha

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

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

A kockázatelemzés eredményét IBF-nek dokumentálnia kell, majd meg kell ismertetnie az Igazgatóval.

[1] *Ibtv. 1. §. 32.a kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat;*

A nem tolerálható kockázatok kezelésére intézkedési tervet kell készíteni, melynek tartalmaznia kell a kockázat kezelésére javasolt intézkedéseket, felelős, határidő és költségvonzat megjelölésével.

A kockázatkezelési tervet az IBF-nek kell előkészítenie és az Igazgató hagyja jóvá.

A kockázatelemzéssel és kezeléssel kapcsolatos dokumentumok bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, az Igazgató, valamint az Igazgató által írásban kijelölt személyek jogosultak.

II.7. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS – BESZERZÉSI ELJÁRÁSREND

Az Igazgatóságnak a jelen fejezetben foglalt követelmények alapján kell az elektronikus információs rendszereire vonatkozó beszerzéseit elvégeznie.

II.7.1. Erőforrás igény felmérés

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

A biztonsági beruházások tervezését az informatikai biztonsági stratégiai célok, valamint a cselekvési tervekben megfogalmazottak alapján kell elkészíteni.

A tervezési dokumentumot az információbiztonsági felelős készíti el az informatikai területért felelős vezetővel együttműködve.

A tervezési dokumentumban legalább a következőket kell feltüntetni:

a) beruházás megnevezése;

b) beruházás indoka, célja, kezelt kockázat;

c) költség-hasznon elemzés;

d) a beruházás elhagyásának következményei (jogi, információbiztonsági kockázat).

Az információbiztonsági beruházások tervezését tartalmazó előterjesztést az információbiztonsági felelős terjeszti be az Igazgatónak jóváhagyás céljából. A dokumentumot előzetesen ellen kell jegyeztetni az informatikai területért felelős vezetővel.

II.7.2. Beszerzések

II.7.2.1. Funkcionális biztonsági követelmények

A kockázatokkal arányos védelem kialakítása érdekében az IBF-et még a tervezés (ajánlatkérés) fázis elejétől kezdve be kell vonni a projektbe.

Az IBF bevonása a szerződést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.

A tervezés fázisában az adatgazdának az IBF-el együttműködve biztonsági osztályba kell sorolni az alkalmazni kívánt EIR-t.

Az IBF-nek a megállapított biztonsági osztály alapján meg kell határoznia a szállító felé a vonatkozó adminisztratív, fizikai és logikai védelmi intézkedéseket.

Webes alkalmazás fejlesztés esetén elő kell írni, hogy a fejlesztés feleljen meg az *{Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója}* –ban rögzített, IBF által meghatározott követelményeknek.

Mobil alkalmazás fejlesztése során elő kell írni, hogy a fejlesztés feleljen meg *{Open Web Application Security Project Mobile Application Security Verification Standard aktuális verziója}*-ban rögzített, IBF által meghatározott követelményeknek.

A szállító által teljesítendő védelmi intézkedéseket a szerződés mellékletévé kell tenni. A szállítónak dokumentált módon el kell készítenie a fentiekben meghatározott védelmi intézkedések alapján a szállítandó termék funkcionális biztonsági követelményeit, azaz ki kell fejtenie, hogy az adott követelményt konkrétan hogyan, milyen módon fogja teljesíteni az általa szállítandó rendszer vonatkozásában.

Az IBF-fel a tervezés fázisában el kell fogadtatni a funkcionális biztonsági követelményeket, anélkül az EIR fejlesztése nem kezdhető meg.

II.7.2.2. Garanciális biztonsági követelmények

A biztonsági intézkedések fejtsék ki hatásukat, és teljesítsék a bennük közvetlenül megfogalmazott funkcionális követelményeket. A szállítóknak el kell készíteniük az intézkedések funkcionális leírását és tervét olyan részletességgel, amely lehetővé teszi az intézkedések elemzését és tesztelését (ideértve az intézkedést megvalósító összetevők közötti funkcionális interfészeket is). A szállítók az intézkedések szerves részeként szerepeltessék a kiosztott felelősségeket és speciális tevékenységeket annak érdekében, hogy amikor az intézkedéseket megvalósítják, azok folyamatosan és következetesen (azaz az informatikai célrendszer egészében) teljesítsék megkívánt feladatukat vagy céljukat, továbbá segítsék az intézkedések hatékonyságának javítását.

Az intézkedéseket oly módon dolgozzák ki, hogy nagy biztonsággal támogatni tudják azt, hogy az intézkedések összessége teljes, konzisztens és helyes.

II.7.2.3. Biztonsággal kapcsolatos dokumentációs követelmények

A szállítónak - szükség szerint az IBF-el és a rendszergazdákkal együttműködve - a következő dokumentumokat kell elkészítenie az átadás-átvétel előtt:

a) rendszerbiztonsági terv, mely tartalmazza a szállítandó termék/fejlesztés biztonsági intézkedéseinek funkcionális biztonsági leírását;

b) adminisztrátori dokumentáció;

c) felhasználói dokumentáció.

Egyedi fejlesztések esetében a következő, további dokumentumokat kell a szállítónak elkészítenie és átadnia:

a) követelményspecifikáció;

b) rendszerterv;

c) teszteseteket tartalmazó tesztelési forgatókönyv.

II.7.2.4. Dokumentálás formai követelményei

Az EIR dokumentálása során az alábbi pontokban részletezett formai elemeket minden dokumentumban értelemszerűen kell szerepeltetni.

a) Dokumentum adatlap:
    a. a Dokumentum címe,
    b. tárgya,
    c. fájl neve és verziója,
    d. Dokumentum típusa,
    e. Dokumentum verziószáma,
    f. Dokumentum státusza,
    g. Dátum,
    h. Készítő, Ellenőr,
    i. Verziószám,
    j. Státusz,
    k. Minősítés.
b) lapszámozás,
c) tartalomjegyzék,
d) tárgymutató.

II.7.2.5. Dokumentumok rendelkezésre állása

Az EIR dokumentációjának egy eredeti nyomtatott példányban és szerkeszthető Open Document Format (ODF) vagy Microsoft Word formátumban és nyomtatható PDF formátumban elektronikus formában kell rendelkezésre állnia.

II.7.2.6. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelmények

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

A biztonsággal kapcsolatos dokumentumokat a következő szerepkörök ismerhetik meg:

a) fejlesztő;
b) rendszergazda;
c) IBF;
d) Igazgató.

II.7.2.6.1. Az elektronikus információs rendszer fejlesztési környezetére vonatkozó előírások

A szerződésekben elő kell írni, hogy a leszállított szoftver megfelelően biztonságos környezetben, auditálható körülmények között készüljön. A leszállított szoftver nem tartalmazhat a dokumentációkban nem rögzített szükségtelen funkcionalitást, nem tartalmazhat hátsó kaput, illetve egyéb kártékony kódot. Amennyiben mégis tartalmazna, és ebből adódóan az Igazgatóságnak bármilyen kára keletkezne, akkor azért a Szállító felelősséggel tartozik.

Az Igazgatóság részére történő fejlesztések során csak olyan szoftverkomponensek használhatóak fel, melyek nemzetközileg széles körben elfogadottak, rendelkeznek megfelelő gyártói támogatással a felfedezett biztonsági rések javítására és a gyártói támogatásuk még legalább 3 évig érvényes.

II.7.2.6.2. Az elektronikus információs rendszer tervezett üzemeltetési környezetére vonatkozó előírások

Amennyiben az elektronikus információs rendszert az Igazgatóság fogja üzemeltetni, a tervezés fázisában egyeztetni kell a rendszergazdákkal az általuk támogatható futtatókörnyezetet és annak erőforrásigényét (hardverigény, licencek száma stb.). A rendszerdokumentációkban rögzíteni kell a tervezett futtatókörnyezet leírását.

II.7.2.7. Fejlesztési szerződések biztonsági követelményei

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

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

Elő kell írni a jelen IBSZ *{II.7.3. Az elektronikus információs rendszerre vonatkozó dokumentáció}* fejezetében megkövetelt biztonsági dokumentációk elkészítését.

A szerződésben meg kell követelni, hogy a fejlesztő, szállító hozza létre és bocsássa rendelkezésére jelen IBSZ *{II.7.2.1. Funkcionális biztonsági követelmények}* fejezetében megkövetelt, az alkalmazandó védelmi intézkedések funkcionális tulajdonságainak a leírását.

A szerződésben elő kell írni, hogy minden egyes új verzióra kiterjedően a szoftver forráskódját és fordítási paramétereit át kell adni az Igazgatóság részére, vagy azokat letétbe kell helyezni arra kijelölt harmadik személynél olyan formában, hogy a támogató cég megszűnése esetén a kód az Igazgatóság számára hozzáférhető legyen. A szerződésben rögzíteni kell az érintett EIR továbbhasználhatóságának a feltételeit abban az esetben, hogy ha a támogató cég szerződése megszűnik az Igazgatósággal.

II.7.2.8. Támogatási szerződések

Az elektronikus információs rendszerek támogatási szerződéseiben a következőket kell előírni:

a) az EIR-ben felmerülő hibák kezelése, javítása,

b) az Igazgatóság fejlesztési igényeinek ellátása,

c) megállapodás alapján az EIR futtató környezetének (operációs rendszer, adatbázis rendszerek, egyéb szoftverkomponensek) frissítése.

A szerződésben rögzíteni kell a támogatás körülményeit (határidők, rendelkezésre állás, helyszíni vagy telefonos támogatás) is a megfelelő szolgáltatási szint biztosítására. A paraméterek pontos értékének meghatározása az EIR adatgazdájának a feladata.

II.7.3. Az elektronikus információs rendszerre vonatkozó dokumentáció

Az elektronikus információs rendszerre vonatkozó dokumentációk tartalmi követelményei a következők:

II.7.3.1. Követelményspecifikáció

A követelményspecifikációnak tartalmaznia kell mindazokat az elvárásokat, amelyeket az Igazgatóság megfogalmaz a bevezetendő EIR-rel/szolgáltatással szemben.

A követelményspecifikációnak a következőket kell tartalmaznia:

a) Az Igazgatóság által meghatározott igények/feladatok részletes leírása;

b) A funkcionális megoldás összefoglalása;

c) Technológiai követelmények;

d) Oktatási követelmények.

A követelményspecifikációval szemben támasztott követelmények a következők:

a) A követelményspecifikációnak teljesnek kell lennie, azaz biztosítani kell, hogy tartalmazza az Igazgatóság valamennyi elvárását;

b) Ne tartalmazzon a megoldás módjára vonatkozó szükségtelen megszorítást;

c) Következetes kifejezésekkel, szóhasználattal, világos ábrákkal szemléltesse a folyamatokat;

d) Ki kell terjednie minden támogatni kívánt folyamatra;

e) Nem szabad egymásnak ellentmondó követelményeket megfogalmazni.

II.7.3.2. Rendszerterv

A szállítónak egyedi fejlesztés esetén a következő tartalommal rendszertervet kell készítenie:

a) követelmény lista;

b) feldolgozási folyamatok részletes leírása;

c) ellenőrzési rendszer leírása;

d) hibakezelési eljárások;

e) rendszer-felügyeleti kapcsolatok;

f) kapcsolódó rendszerelemek hivatkozása;

g) kapacitástervezési leírás;

h) logikai adatmodell;

i) I/O adatszerkezetek;

j) képernyő tervek;

k) lista tervek;

l) infokommunikációs rendszer logikai architektúra ábrája;

m) elemek funkcionális leírása;

n) technikai környezet leírása;

o) biztonsági kontrollok ismertetése.

II.7.3.3. Rendszerbiztonsági terv

A rendszerbiztonsági terv követelményeit a jelen IBSZ *{IV.2.1. Rendszerbiztonsági terv}* fejezete tartalmazza.

II.7.3.4. Adminisztrátori dokumentáció

Az adminisztrátori dokumentációnak tartalmaznia kell:

a) a technikai környezet ismertetését,
b) a kapacitástervezési leírást,
c) az alkalmazott portok, szolgáltatások, és protokollok részletes ismertetését,
d) a kommunikációs környezet ismertetését,
e) a szerepköröket és hozzájuk tartozó feladatok ismertetését,
f) a jogosultsági rendszer részletes ismertetését,
g) a feldolgozási folyamatok részletes ismertetését üzemeltetési szempontból,
h) a mentés, archiválás, monitorozás ismertetését,
i) az időszaki teendők ismertetését,
j) a hibaüzenetek, hibaelhárítással kapcsolatos feladatok ismertetését,
k) rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,
l) a biztonsági funkciók hatékony alkalmazását és fenntartását,
m) naplózási lehetőségek ismertetését,
n) a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket.

II.7.3.5. Felhasználói dokumentáció

A felhasználói dokumentációnak tartalmaznia kell:

a) szerepkörönként elkülönítve a funkciók leírását képekkel illusztrálva,
b) a kezelési felületek, menürendszer ismertetését,
c) az interfész leírásokat,
d) a kapcsolódó rendszerelemek pontos hivatkozását,
e) az ellenőrzési és hibakezelési eljárásokat / hibajegyzéket,
f) logikai kontrollok ismertetését.

II.7.3.6. Felhasználói tesztelési forgatókönyv

A felhasználói tesztelési dokumentációnak tartalmaznia kell a következő elemeket:

a) Tesztek dokumentálási követelményei;
b) Elfogadási kritériumok meghatározása;
c) Tesztelési környezet meghatározása;

Tesztesetek a követelményspecifikációban rögzített főbb funkcionalitások tesztelésére.

II.7.4. A védelem szempontjainak érvényesítése a beszerzés során

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

A sikeres átadás-átvétel feltétele

a) a jelen IBSZ-ben meghatározott dokumentációk Igazgatóság általi elfogadása;

b) a funkcionális biztonsági követelmények IBF általi, tesztrendszerben történő ellenőrzése;

c) a felhasználók részéről sikeres tesztek elvégzése a tesztforgatókönyvek alapján;

d) szükség szerint a Nemzeti Kibervédelmi Intézet Eseménykezelő Központ részéről sikeres sérülékenységvizsgálat elvégzése.

II.7.5. Külső elektronikus információs rendszerek szolgáltatásai

Külső elektronikus információs rendszerek igénybevétele esetén a jelen IBSZ *{II.7.2.7. Fejlesztési szerződések biztonsági követelményei}* pontjában foglaltakon kívül szerződésben kell rögzíteni az érintett EIR biztonsági osztályát, a szolgáltató és az Igazgatóság által külön-külön, illetve együttesen teljesítendő, az érintett EIR biztonsági osztályából fakadó adminisztratív, fizikai és logikai védelmi intézkedéseket.

A szerződésben ki kell térni az Igazgatóság felhasználóinak feladataira az igénybe vett külső elektronikus információs rendszerek szolgáltatásával kapcsolatban.

A szerződésben ki kell kötni a jogot arra, hogy az Igazgatóság az IBF útján auditálhassa a szolgáltatónál kialakított, szerződésben meghatározott védelmi intézkedéseket.

II.7.6. Folyamatos ellenőrzés

Az IBF az elektronikus információs rendszerek folyamatos ellenőrzése céljából folyamatba épített ellenőrzési tervet hajt végre. A folyamatos ellenőrzés követelményeit a jelen IBSZ *{IV.4.1. Biztonsági értékelések}* fejezete tartalmazza.

II.8. ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK ÜGYMENET FOLYTONOSSÁGÁNAK TERVEZÉSE

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

II.8.1. Ügymenet folytonosságra vonatkozó eljárásrend

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

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

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

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

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

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

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

II.8.1.1. Az ÜFT felülvizsgálata

Az Ügymenet-folytonossági tervet évente felül kell vizsgálni.

Az Ügymenet-folytonossági tervet soron kívül felül kell vizsgálni

a) az elektronikus információs rendszer vagy a működtetési környezet jelentős változása,

b) az ügymenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémák esetén.

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

II.8.1.2. Az ÜFT kezelése

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

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

II.8.2. Folyamatos működésre felkészítő képzés

Évente folyamatos működésre felkészítő képzést kell tartani, melynek során képezni kell a felhasználókat az ÜFT-ben foglaltakról. A képzést az IBF-nek kell megtartania. A képzésen a részvétel kötelező.

II.8.3. Az elektronikus információs rendszer mentései

Az elektronikus információs rendszerek és az azokban kezelt adatok az adatgazdák és a jogszabályok által elvárt, megfelelő rendelkezésre állásának biztosítása érdekében mentési eljárásrendet kell kidolgozni a következők figyelembevételével:

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

a) felhasználói szintű adatok (ügyviteli adatok)

b) rendszerszintű információk

c) naplóinformációk

d) a rendszerrel kapcsolatos dokumentációk.

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

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

Az EIR-ek fizikai védelme érdekében, gondoskodni kell arról, hogy a telepítő állományok ne károsodjanak, ezért az eredeti példányukról biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag elkülönítve, biztonságos helyen elzárva kell tárolni. Az eredeti hordozókról készített másolatokat kell a napi tevékenység során használni. Az olvasási biztonság fenntartása érdekében az eredeti adathordozókról kétévente frissítő mentést kell készíteni.

Az ügymenet folytonosság fenntartása érdekében a mentéseket tartalmazó adathordozókat szerverhelyiségtől elkülönítve, páncélszekrényben kell tárolni.

II.8.4. Az elektronikus információs rendszer helyreállítása és újraindítása

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

a) katasztrófát követő helyreállítandó célállapot;

b) a katasztrófa események definíciója;

c) a katasztrófa tényét eldöntő, a folyamat inicializálásáért felelős személyt, személyeket;

d) a helyreállítási terv hatóköre;

e) a megelőzés érdekében végzett tevékenységeket;

f) felkészülés a katasztrófa elhárítására;

g) katasztrófa esetén végrehajtandó tevékenységek;

h) elektronikus információs rendszerek vészleállításának és újraindításának folyamatát leíró dokumentumot;

i) a helyreállítási terv tesztelése, karbantartása.

Az elektronikus információs rendszerekre vonatkozó helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról a rendszergazda gondoskodik. A terv készítési tevékenységeket az IBF-nek információbiztonsági szempontból támogatnia és évente ellenőriznie kell.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs infrastruktúra (pl.: új elektronikus információs rendszer bevezetése, új nagyteljesítményű hardverelemek változása).

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

II.9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – BIZTONSÁGI ESEMÉNYKEZELÉSI TERV

II.9.1. Biztonsági események figyelése

Az Igazgatóság az elektronikus információs rendszerek biztonsági eseményeinek kezelésekor (nyomon követés, dokumentálás) a következők szerint jár el.

II.9.2. Biztonsági események meghatározása

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

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;
b) a rendszer hibás működése vagy túlterhelések (Dos-támadás);
c) emberi hibák;
d) a szabályzatoknak vagy irányelveknek való nem megfelelés;
e) a fizikai biztonsági rendelkezések megsértése;
f) nem ellenőrzött rendszerbeli változások;
g) a szoftver vagy hardver hibás működése;
h) hozzáférési előírások megsértése;
i) kártékony kód általi fertőzés;
j) a nem teljes vagy nem pontos működési adatokból eredő hibák;
k) a bizalmasság és sértetlenség megsértése;
l) az elektronikus információs rendszerrel való visszaélés.

II.9.3. Biztonsági események kategorizálása

Az Igazgatóság az elektronikus információs rendszereit érintő biztonsági eseményeket két kategóriába sorolja:

a) Súlyos biztonsági esemény;
b) Enyhébb fokozatú biztonsági esemény.

II.9.3.1. Súlyos biztonsági esemény

Az Igazgatóságnál a következők számítanak súlyos biztonsági eseménynek:

a) Egynél több vagy az Igazgatóság összes elektronikus információs rendszerét érintő biztonsági esemény;
b) A bekövetkezett kár mértéke alapján a társadalmi-politikai hatás jelentős;

c) Személyes adatok illetéktelen kézbe kerülése feltételezhető;

d) Jogszabály által védett adatok illetéktelen kézbe kerülése feltételezhető.

II.9.3.2. Enyhébb fokozatú biztonsági esemény

Az Igazgatóságnál a következők számítanak enyhébb fokozatú biztonsági eseménynek:

a) Nem kritikus elektronikus információs rendszer vagy adat bizalmassága sértetlensége vagy rendelkezésre állása sérül;

b) Az ügymenetet jelentősen nem befolyásoló elektronikus információs rendszer rendelkezésre állása sérül.

II.9.4. Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát.

A biztonságot érintő eseményekről szóló jelentések elkészítésére a jelen IBSZ *{3. számú melléklet – Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

Amennyiben a rendszergazda úgy ítéli meg, hogy a bejelentett probléma biztonsági eseményre utal, úgy jelentenie kell az IBF-nek.

Biztonsági esemény esetén az IBF látja el a biztonságiesemény-kezelési megbízott feladatait.

Az IBF-nek a saját Ügyfélkapuján keresztül haladéktalanul jelentenie kell a biztonsági eseményt az Eseménykezelő Központ (továbbiakban: GovCert) részére.

Az IBF-nek csatolnia kell a bejelentéshez a biztonsági eseményhez kapcsolódó valamennyi bizonyítékot.

Az IBF-nek és az Igazgatóságnak együtt kell működnie a GovCert-tel a biztonsági esemény kezelésében és a GovCert által javasolt intézkedéseket végre kell hajtania.

Az IBF-nek kivizsgálást kell kezdeményeznie a beérkezett jelentés alapján és javaslatot kell tennie az Igazgató részére az esemény előfordulási esélyének csökkentése, illetve az okozott kár mérséklése érdekében.

Amennyiben a biztonsági esemény igazoltan a szabályok megsértéséből adódik, úgy az Igazgatónak le kell folytatnia a szükséges fegyelmi eljárást az Igazgatóság vonatkozó előírásai alapján.

II.9.5. Jelentés a biztonság gyenge oldalairól

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

A biztonságot érintő gyenge pontokról szóló jelentések elkészítésére a jelen IBSZ *{3. számú melléklet – Biztonsági események jelentése}* mellékletében található űrlapot kell használni.

II.9.6. Jelentés a szoftverzavarokról

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

a) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet is,

b) be kell szüntetni az adott számítógép használatát.

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

Abban az esetben, hogy ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazda jelenti az IBF-nek, aki a jelen *IBSZ {II.9.4. Jelentés a biztonsági eseményekről}* pontjának megfelelően kivizsgálja az eseményt.

II.9.7. Tanulságok levonása a biztonsági eseményekből

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

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

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

II.9.8. Képzés a biztonsági események kezelésére

Az általános biztonságtudatossági képzés részévé kell tenni a biztonsági események kezelésével összefüggő ismereteket, így különösen

a) a biztonsági esemény fogalma;

b) biztonsági események fajtái;

c) teendők biztonsági esemény esetén;

d) biztonsági események dokumentálása;

e) tájékoztatás közreműködési kötelezettségről a biztonsági események kivizsgálása során;

f) eljáró szervek biztonsági eseménye esetén eljáró szervek, hatóságok feladatainak ismertetése;

g) szükséges javító intézkedések megtétele biztonsági események kivizsgálása után.

II.10. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ – SZEMÉLY – BIZTONSÁG

II.10.1. Információbiztonsági tevékenységek

Az Igazgatóságnál a következő információbiztonsági tevékenységeket kell ellátni:

a) informatikai kockázatelemzés és kezelés,

b) elektronikus információs rendszerek biztonsági felügyelete,

c) új elektronikus információs rendszerek információbiztonsági véleményezése és elfogadása,

d) szervezetek közötti információbiztonsági együttműködés,

e) az információbiztonság független felülvizsgálata.

II.10.2. Az információbiztonsági felelősségi rend meghatározása

Az információbiztonság megteremtése és fenntartása olyan alapvető felelősség, amely szerint nem tartozhat egyszemélyi felelősségi és hatáskörbe az elektronikus információs rendszerek tervezése, fejlesztése, üzemeltetése és felügyelete.

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

II.10.3. Az Igazgató

Az Igazgató az Ibtv. alapján gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

II.10.3.1. Az Igazgató feladatai

Az Igazgató

a) Meghozza az Igazgatóság informatikai rendszerével kapcsolatos döntéseket.

b) Megteszi a külső szervezetek számára a szakmai nyilatkozatokat és tájékoztatást.

c) Gondoskodik az Igazgatóság informatikai stratégiájának megalkotásáról.

d) Tájékoztatja az informatika üzemelésért felelős vezetőt a kilépő, vagy belépő dolgozó, illetve munkakör változás esetén a dolgozók és informatikai rendszerrel kapcsolatos jogosultságainak változásáról.

e) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

f) biztosítja az Igazgatóságra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

g) az elektronikus információs rendszer biztonsági osztálya és az Igazgatóság biztonsági szintje alapján előírt követelményeknek megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki vagy bíz meg,

h) meghatározza az Igazgatóság elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

i) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és az Igazgatóság munkatársai információbiztonsági ismereteinek szinten tartásáról,

j) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy az Igazgatóság elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

k) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

l) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről,

m) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

n) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a jelen IBSZ-ben foglaltak szerződéses kötelemként teljesüljenek,

o) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

p) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

Az Igazgató köteles együttműködni a jogszabályban meghatározott hatóságokkal. Ennek során

a) az Igazgatóság alapadatairól és az IBF személyéről tájékoztatást nyújt,

b) az IBF útján az Igazgatóság informatikai biztonsági szabályzatát tájékoztatás céljából megküldi,

c) a Hatóság által közzétett formában nyilatkozik a Hatóság részére az elektronikus információs rendszerek biztonsági osztályba sorolásáról és az Igazgatóság, illetve az Igazgatóság szervezeti egységeinek biztonsági szintbe sorolásáról,

d) az IBF útján megküldi az Igazgatóság elvárt biztonsági szintjének és az elektronikus információs rendszereinek elvárt biztonsági osztályának elérésére készített cselekvési tervet,

e) biztosítja a jogszabályokban meghatározott hatóságok részére az ellenőrzés lefolytatásához és a biztonsági incidensek kivizsgálásához szükséges feltételeket.

A fentieket a HR, vezetővel, a gazdasági vezetővel valamint az általános igazgatóhelyettessel egyetértésben teszi.

II.10.3.2. Az Igazgató felelőssége

Az Igazgató felelős az Igazgatóságnál az Ibtv. által előírt biztonsági szintnek és biztonsági osztályoknak megfelelő információbiztonsági intézkedések megvalósulásáért, illetve az ezek végrehajtásához szükséges erőforrások biztosításáért.

II.10.4. Az IBF

Az Igazgató által megbízott IBF-nek a következők a feladatai, jogai és felelőssége:

II.10.4.1. Az IBF feladatai

Az informatikai biztonsággal összefüggő tevékenység koordinálását az informatikai biztonságért felelős szervezi az üzemeltetési osztályvezetővel összhangban. Így részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására.

Az Igazgatóság informatikai biztonságért felelőse a jogszabályi követelményeknek eleget tevő, jelenleg külső megbízású személy, aki munkája során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

Az IBF az Igazgatóság információbiztonsági irányítási rendszerének működtetése és ellenőrzésével kapcsolatos feladatai a következők:

a) gondoskodik az Igazgatóság elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi vagy irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) előkészíti az Igazgatóság elektronikus információs rendszereire informatikai biztonsági szabályzatot,

d) cselekvési tervet készít az elektronikus információs rendszerek biztonsági osztályba sorolásából és az Igazgatóság, illetve az Igazgatóság szervezeti egységeinek biztonsági szintbe sorolásából fakadó védelmi intézkedések végrehajtásához, ebben mérföldköveket határoz meg, azokat meghatározott időközönként felülvizsgálja, valamint karbantartja az intézkedési tervet,

e) előkészíti az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolását és az Igazgatóság biztonsági szintbe történő besorolását,

f) véleményezi az elektronikus információs rendszerek biztonsága szempontjából az Igazgatóság e tárgykört érintő szabályzatait és szerződéseit,

g) kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal.

Az IBF biztosítja a jogszabályokban meghatározott követelmények teljesülését

a) az Igazgatóság valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők,

b) ha az Igazgatóság adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, a közreműködők,

az IBSZ hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

Ezek alapján:

a) Gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről.

b) Összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében.

c) Az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz a szervezet vezetőjének a további intézkedésekre, a felelősségre vonásra.

d) Új informatikai központ tervezése és kialakítása során ellenőrzi az IBSZ-ben megfogalmazott, a helyiségek fizikai paramétereire vonatkozó követelmények kielégítését és a meglevő helyiségek paramétereinek értékét. Ellenőrzi az informatikai központba való beléptetési eljárást és a belépő személyek körének jogosultságát.

e) Az SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét.

f) Ellenőrzi a fejlesztő rendszerek elkülönítésének megfelelősségét az éles rendszertől.

g) Felügyeli a beruházásokat, a fejlesztéseket és az üzemvitelt informatikai biztonsági szempontból, illetve azokra javaslatot tesz.

h) Az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad.

i) Szúrópróbaszerűen ellenőrzi:

    a. az egyes felhasználói gépek hardverkonfigurációját, és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverek listájával;

    b. hogy a javításra kiszállított eszközökön adat ne kerüljön ki;

    c. az adathordozók selejtezését.

j) Az IBSZ-t évente felülvizsgálja, és javaslatot tesz a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások miatt szükségessé váló módosításokra.

II.10.4.2. Az IBF jogai

Az IBF az Igazgatóság információbiztonságának fenntartása érdekében, illetve információbiztonsági incidens esetében jogosult:

a) külön engedély nélkül az Igazgatóság bármely helyiségébe belépni, amennyiben ott az információbiztonságot érintő munkavégzés folyik,

b) bármelyik számítógép, adathordozó vagy számítógépes lista tartalmába betekinteni, függetlenül annak minősítésétől (a vonatkozó jogszabályok betartásával), amennyiben az adott ügyben, illetve témában vizsgálat folyik,

c) minden értekezleten részt venni, észrevételeit és javaslatait megtenni, amelynek számítástechnikai, illetve információbiztonsági vonatkozása van, és ez az értekezlet összehívásakor ismert.

II.10.4.3. Az IBF felelőssége

Az IBF felelős az Igazgatóság elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.

II.10.5. Üzemeltetési Osztály vezetője

Az IT rendszer üzemeltetését az **Üzemeltetési Osztály az Informatikai Csoport útján** látja el. Az IT rendszer üzemeltetésért felelős vezető a mindenkori szervezeti egység osztályvezetője.

II.10.5.1. Az Üzemeltetési Osztály vezetőjének feladata

Az Üzemeltetési Osztály vezetőjének feladata:

a) Évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,

b) Rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,

c) Közreműködik a biztonsági incidensek kivizsgálásában,

d) Együttműködik az informatikai biztonsággal összefüggő tevékenység végzésében az informatikai biztonságért felelőssel.

e) Irányítja és felügyeli az IT üzemeltetői részleg munkáját,

f) Meghatározza az informatikai oktatási irányokat és gondoskodik megvalósításukról.

g) Javaslatot tesz az informatikai biztonságot erősítő továbbképzésre.

h) Az adott szakterületek vezetőivel egyeztetve meghatározza az egyes feladatkörökhöz tartozóan az informatikai biztonsággal kapcsolatosan elsajátítandó ismeretek körét, és ellenőrzi az elsajátítás tényét.

i) Amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését.

j) Ellenőrzi a víruskereső programok használatát.

k) az IBF-fel közösen meghatározza az információbiztonsági követelmények megvalósításához szükséges informatikai eszközöket;

l) kidolgozza a hatáskörébe tartozó üzemeltetési eljárásokat.

II.10.6. A rendszergazda

A rendszergazda információbiztonsággal kapcsolatos feladata és kötelessége a következő:

II.10.6.1. A rendszergazda feladata

A rendszergazda feladatai a következők:

a) szerverek hardveres és szoftveres karbantartása;

b) szerverek mentése;

c) rendszerfelügyelet biztosítása;

d) rábízott elektronikus információs rendszerek üzemeltetése;

e) a vírusvédelmi rendszer konfigurálása és üzemeltetése;

f) munkaállomások hardveres és szoftveres karbantartása;

g) a szerverszoba felügyelete;

h) a rendszergazdai teendőkkel összefüggő kimutatások készítése;

i) a felhasználókat érintő rendszerváltozások rögzítése és közzététele;

j) helyszíni segítségnyújtás a felhasználóknak;

k) közreműködik a biztonsági incidensek kivizsgálásában;

l) vezeti és naprakészen tartja az IBSZ-ben előírt nyilvántartásokat.

II.10.6.2. A rendszergazda felelőssége

A rendszergazda felelőssége az általa a jelen IBSZ *{2. számú melléklet – Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása}* mellékletében felsorolt elektronikus információs rendszerek jelen IBSZ-ben foglaltak és az Adminisztrátori dokumentációk szerinti biztonságos üzemeltetése.

II.10.7. Az adatgazda

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

Az elektronikus információs rendszerek adatgazdáit az Igazgató jelöli ki.

II.10.7.1. Az adatgazda feladatai

Az adatgazda információbiztonsággal kapcsolatos feladatai a következők:

a) az IBF-el közreműködve biztonsági osztályba sorolja a hozzá rendelt elektronikus információs rendszereket;

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

c) Az ügymenet folytonosság tervezése során meghatározza az érintett EIR maximális kiesési idejét és az EIR-ben elfogadható maximális adatvesztés mértékét.

II.10.7.2. Az adatgazda felelőssége

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

II.10.8. A szervezeti egység vezetője

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

II.10.9. A felhasználó

Az Igazgatóság felhasználóinak az elektronikus információs rendszerek biztonságával kapcsolatban a következők a jogai, a kötelességei és a felelőssége:

II.10.9.1. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre,

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

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

II.10.9.2. A felhasználó kötelessége

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

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

a) az informatikához kapcsolódó tevékenység fennakadása, megszakadása,

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

c) információbiztonsági esemény.

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

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, az Igazgatóság erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással.

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

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

II.10.9.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a jelen IBSZ *{7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend}* mellékletének megismeréséért és az abban foglalt szabályok betartásáért,

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

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

d) az elektronikus információs rendszerben végzett műveletekért,

e) az Igazgatóság elektronikus információs rendszereinek szakszerű kezeléséért és

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

II.10.10. A munkaköri felelősség és az alkalmazás feltételei

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

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

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

Az Igazgatóság elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

II.10.11. Munkakörök, feladatok biztonsági szempontú besorolása

Az Igazgatóság az információbiztonsági szempontból alap és kiemelt munkaköröket állapított meg.

Az Igazgatóságnál nincsenek nemzetbiztonsági ellenőrzés alá eső munkakörök és feladatok.

II.10.11.1. Alap biztonsági osztály

Az alap biztonsági osztályba a következő munkakörök kerültek besorolásra:

a) Adatgazda,

b) Felhasználó.

Az alap munkakör betöltésének követelményei:

a) Erkölcsi bizonyítvány,

b) Szakirányú végzettség,

c) Informatikai alapismeretek,

II.10.11.2. Kiemelt biztonsági osztály

A kiemelt biztonsági osztályba a következő munkakörök tartoznak:

a) Igazgató,

b) Rendszergazda,

c) Információbiztonsági felelős.

A kiemelt biztonsági munkakör betöltésének követelményei:

a) Erkölcsi bizonyítvány

b) Szakirányú végzettség

c) 2 év szakmai tapasztalat

d) Alapfokú angol nyelvtudás

II.10.12. A személyek ellenőrzése

Az Igazgatóság személyügyi referensének a feladata, hogy az elektronikus információs rendszerekhez való hozzáférési jogosultság megadása előtt ellenőrizze, hogy az érintett személy a *{II.10.11. Munkakörök, feladatok biztonsági szempontú besorolása}* fejezetben meghatározott feltételeknek megfelel-e. A vizsgálat magában foglalja az alábbiakat:

a) referenciák ellenőrzése,

b) a felvételre jelentkező életrajzának ellenőrzése a teljességre és pontosságra vonatkozóan,

c) a legmagasabb iskolai végzettség (szakképzettség) ellenőrzése,

d) nyelvtudást igazoló okiratok ellenőrzése,

e) hatóság által kibocsátott azonosító irat ellenőrzése,

f) erkölcsi bizonyítvány ellenőrzése.

Külső szerződő felek esetében a szerződést kezdeményező feladata a szerződésben előírni a személybiztonsági feltételeket.

II.10.13. Eljárás jogviszony megszűnésekor

A jogviszony megszüntetésekor a következő feladatok végrehajtása szükséges:

a) Jogosultságok dokumentált formában történő megszüntetése.

b) 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.

c) Az így archivált adatokat a törvényi előírásoknak megfelelően tárolni kell, illetve 1 év után törölni kell a rendszerből.

A fentiek végrehajtását a jogviszony megszűnésével egy időben, kockázatot jelentő esetekben a jogviszony megszűnését megelőzőn kell végrehajtani. A végrehajtás elrendeléséért az Igazgató, a végrehajtásért a rendszergazda a felelős.

Kiemelt biztonsági osztályba tartozó munkakörök esetén a jogviszony megszűntetését információbiztonsági szempontból az IBF koordinálja.

II.10.13.1. Vagyontárgyak visszaszolgáltatása

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

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

II.10.13.2. Hozzáférési jogok megszüntetése

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

A fentiektől eltérni az Igazgató írásos engedélyével lehetséges.

A feladatok végrehajtásáért a rendszergazda a felelős.

II.10.13.3. Információbiztonsági kötelmek a jogviszony megszűnése után

A személyügyi referensnek a jelen IBSZ *{9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén}* mellékletében foglaltak szerint tájékoztatnia kell a dolgozót arról, hogy

a) legkésőbb a jogviszony megszűnése napján köteles az Igazgatóság elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni;

b) az Igazgatóságnál működő elektronikus információs rendszereket az Igazgatóság kizárólag hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában az Igazgatóság fenntartja magának a tulajdonjogot;

c) az Igazgatóságnak továbbra is hozzáférési lehetősége van az általa korábban használt, kezelt elektronikus információs rendszerekhez és az azokban kezelt adatokhoz;

d) a titoktartási kötelezettsége a jogviszonya megszűnését követően is fennáll.

A fentiek megsértése jogi következményeket von maga után.

II.10.14. Áthelyezések, átirányítások és kirendelések kezelése

Az áthelyezés során el kell végezni az érintett munkatárs ellenőrzését a jelen IBSZ *{II.10.12. A személyek ellenőrzése}* pontjában foglaltak alapján.

Az érintett munkatárs részére az elektronikus információs rendszerhez történő logikai és fizikai hozzáférések engedélyezését a jelen IBSZ *{IV.10.3. Hozzáférési jogok igénylésének eljárásrendje}* pontjában foglaltaknak megfelelően kell elvégezni.

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

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

II.10.15. Harmadik felekkel kapcsolatos előírások

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

Az Igazgatóság és szerződéses partnerei szerződésben rögzített, a jelen IBSZ-nek megfelelő biztonsági intézkedéseket kötelesek foganatosítani annak érdekében, hogy a kicserélt (átadott/átvett) adatok és dokumentumok véletlen vagy szándékos kompromittálódását megakadályozzák.

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

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

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

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

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

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

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

Harmadik fél az Igazgatóság adatait és az elektronikus információs rendszereit a hozzáférést rögzítő szerződés és a jelen IBSZ *{10. számú melléklet – Titoktartási Nyilatkozat}* mellékletében található titoktartási nyilatkozat aláírása előtt nem ismerheti meg.

II.10.15.1. A harmadik fél hozzáférési kockázatának azonosítása

Az Igazgatóságnak fel kell mérnie, és meg kell határoznia, hogy mekkora a kockázata annak, ha a harmadik félnek hozzáférési joga van az Igazgatóság információs vagyonához.

A kockázatok felmérése a jelen IBSZ *{4. számú melléklet – Kockázatelemzési és kezelési módszertan}* melléklete szerint történik. A kockázatkezeléshez, a megfelelő óvintézkedések kialakításához és a hozzáférések engedélyezéséhez a hozzáférés igénylésben pontosan meg kell határozni a hozzáférések típusát és azt, hogy milyen okból történik a hozzáférés.

A kockázat meghatározásért a harmadik féllel kötött szerződés teljesítésében elsődlegesen érintett szervezeti egység vezetője a felelős, és a szerződés megkötése előtt köteles az informatikai biztonsági felelőst bevonni a szerződéskészítés folyamatába.

II.10.15.2. A harmadik féllel kötött szerződés biztonsági követelményei

A szerződésekben, amennyiben az értelmezhető az alábbiakat kell előírni:

a) a külső szervezetnek meg kell határoznia az Igazgatósággal kapcsolatos, az információbiztonságot érintő szerep- és felelősségi köröket, köztük a biztonsági szerepkörökre és felelősségekre vonatkozó elvárásokat;

b) meg kell követelni, hogy a szerződő fél feleljen meg az Igazgatóság által meghatározott személybiztonsági követelményeknek;

c) meg kell követelni, hogy a szerződő fél dokumentálja a személybiztonsági követelményeket;

d) elő kell írni, hogy ha a szerződő féltől olyan személy lép ki, vagy kerül áthelyezésre, aki rendelkezik az Igazgatóság elektronikus információs rendszeréhez kapcsolódó hitelesítési eszközzel vagy kiemelt jogosultsággal, akkor soron kívül küldjön értesítést az Igazgatóságnak;

e) az informatikai biztonság fő szabályait;

f) az információs vagyon bizalmasságának, sértetlenségének és rendelkezésre állásának meghatározását, illetve a védelem érdekében meghatározott eljárásokat;

g) az információk másolásának és nyilvánosságra hozatalának feltételeit;

h) a szolgáltatás elvárt szintjének és a szolgáltatási időszaknak a meghatározását;

i) a felek felelősségének meghatározását;

j) a szellemi tulajdon védelmére és másolására vonatkozó jogokat és kötelezettségeket;

k) a teljesítések ellenőrizhetőségét, monitorozását és jelentések készítését;

l) a felmerülő problémák kezelését;

m) a hardver- és szoftvertelepítésből és karbantartásokból eredő felelősséget;

n) világos és egyértelmű jelentéskészítési struktúrát és rendszert;

o) a változáskezelések egyértelmű és meghatározott folyamatát;

p) óvintézkedések meghatározását a kártékony kódok ellen;

q) biztonsági események kivizsgálására és jelentésére vonatkozó intézkedések meghatározását;

r) az alvállalkozók bevonására vonatkozó szabályokat.

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

II.10.16. Fegyelmi intézkedések

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

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

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

II.10.17. Belső egyeztetés

Az Igazgatóságnak a cselekvési tervében foglaltaknak megfelelően terveznie és egyeztetnie kell az elektronikus információs rendszerei biztonságát érintő következő tevékenységeit annak érdekében, hogy csökkentse annak a nem érintett szervezeti egységeire gyakorolt hatását:

a) információbiztonsági értékelések;

b) információbiztonsági auditok;

c) hardver vagy szoftverkarbantartások;

d) biztonsági frissítések telepítése;

e) vészhelyzeti tervek tesztelése.

II.10.18. Viselkedési szabályok az interneten

Az Igazgatóság által nyújtott internetkapcsolat és elektronikus levelezési szolgáltatás igénybevételének a következők a szabályai:

II.10.18.1. A web böngészés szabályai

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja! A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

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

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

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

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

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos az Igazgatósággal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

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

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

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

II.10.18.2. E-mail használat

Az Igazgatóság által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos az Igazgatósági e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, online játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni stb.)!

Az Igazgatóság által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az Igazgatóság elektronikus hivatalos kommunikációja elsősorban kormányzati e-mail címek igénybe vétele útján folyhat.

Kormányzati e-mail címnek kell tekinteni:

a) a gov.hu végződésű e-mail címeket,

b) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv által biztosított hivatalos elektronikus levelezési címeket,

c) a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket,

d) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv vagy a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alatt álló gazdasági társaság tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket, valamint

e) a Kormány irányítása vagy felügyelete alá nem tartozó, Alaptörvényben meghatározott szerv hivatalos elektronikus levelezési címeit.

A meghatározott iratok kizárólag kormányzati e-mail címre küldhetők ki.

Kizárólag kormányzati e-mail címre küldhetők ki az alábbi iratok:

a) törvényjavaslatot tartalmazó irat,

b) Kormány részére készült előterjesztés, jelentés,

c) Kormány döntését igénylő előterjesztés,

d) politikai felsővezetői (miniszterelnök, miniszter, államtitkár) döntést igénylő előterjesztés, különösen miniszteri rendelettervezet,

e) politikai felsővezető részére készülő előterjesztés, jelentés,

f) politikai vezető (kormánymegbízott) részére készülő előterjesztés, jelentés,

g) biztosi jogviszonyban álló (kormánybiztos, miniszterelnöki biztos, miniszteri biztos) részére készülő előterjesztés, jelentés,

h) szakmai felsővezető (közigazgatási államtitkár, helyettes államtitkár, központi hivatal vezetője és vezetőjének helyettese, kormányhivatal főigazgatója) részére készülő előterjesztés, jelentés

i) szakmai vezető (kormányhivatal igazgatója, járási hivatal, illetve fővárosi kerületi hivatal vezetője és vezetőjének helyettese, főosztályvezető, osztályvezető) részére készülő előterjesztés, jelentés,

j) minden olyan irat, amely a Kormánynak, a Kormány tagjának, politikai felsővezetőnek vagy vezetőnek, szakmai vezetőnek vagy felsővezetőnek, biztosi jogviszonyban állónak a döntését tartalmazza, mely nem kerül nyilvánosan közzétételre,

k) a fentiekről készült tervezet, másolat vagy kivonat, a fentiekkel kapcsolatos munkaanyag

Ezen irattípusok nem kormányzati e-mail címre történő kiküldése tilos, kivéve, ha azt az Igazgatóság erre kijelölt vezetője kifejezetten, írásban (ez alatt az elektronikus jóváhagyást is érteni kell) engedélyezi.

a) A kizárólag kormányzati e-mail címre küldhető iratoknak nem kormányzati e-mail címre történő továbbításának engedélyezésére kizárólag az erre kijelölt vezető – Dudás György általános igazgatóhelyettes – jogosult, kifejezetten írásban.

b) Amennyiben a fenti irattípusok közé tartozó irat nem-kormányzati e-mail címre történő továbbítására engedély nélkül kerül sor, akkor az minden esetben munkajogi következményekkel jár az intézkedésben részt vevő kollegák irányában.

c) Amennyiben a fentiek szerinti irat nem kormányzati e-mail címre történő megküldése szükséges, akkor az irat továbbítása helyett elsősorban az irat tartalmának kivonatolása útján kell az abban foglaltakat a címzettel közölni. Ennek során lehetőleg kerülni szükséges az utalást arra, hogy a kérdéses tartalom végső soron honnan származik és azt milyen dokumentum tartalmazza, ehelyett elsősorban általános körülírással szükséges utalni a dokumentumban foglaltak keletkeztetőjére.

d) Továbbá haladéktalanul értesíteni kell a Minisztériumot minden esetről, amikor a fentiek szerinti irat nem kormányzati e-mail címre történő továbbítására engedély nélkül került sor (eset leírása, a kiadott irat ismertetése, a címzett e-mail cím megjelölése, az alkalmazott munkáltatói intézkedés bemutatása). Az előbbi tájékoztatókat minden esetben a fentiek szerint kijelölt felelős vezető köteles megküldeni.

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

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

Az Igazgatóság elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására, mivel műszakilag - az elektronikus levelezési szolgáltatás működési elvéből fakadóan – a rendszergazdák nem tudnak garanciát vállalni arra, hogy az elektronikus levél

a) eljut a címzetthez,

b) átküldése közben illetéktelenek annak tartalmát el nem olvassák,

c) átküldése közben illetéktelenek annak tartalmát nem módosítják.

Amennyiben a fentiek biztosítására szükség van (pl.: elektronikus ügyintézés), akkor az állam által nyújtott Központi Elektronikus Ügyintézési Szolgáltatásokat kell igénybe venni vagy egyéb kriptográfiai algoritmusokat kell alkalmazni az elküldött elektronikus levelek bizalmasságának és sértetlenségének biztosítása érdekében.

A fentiekhez hasonlóan a rendszergazdák arra sem tudnak garanciát vállalni, hogy egy hivatali címzettnek szóló levél időben és sértetlenül megérkezik a címzetthez, mivel ehhez más, külső szolgáltatók közreműködése is szükséges, illetve az Igazgatóság a tömeges, kéretlen, valamint kártékony levelek elleni védekezésül spamszűrő rendszert működtet, mely kivételes esetben (fals pozitív) kiszűrhet hasznos levelet is.

Az Igazgatóság elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

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

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán email címére).

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

Ismeretlen helyről származó e-mail-ek, illetve azok csatolmányainak megnyitásakor és az azokban elhelyezett hivatkozásokra kattintással fokozott óvatossággal kell eljárni, mert maga az

email vagy annak csatolmánya, illetve az email-ben elhelyezett hivatkozás kártékony lehet. Ebben az esetben ellenőrizni kell az email feladóját, a tárgyat, a levél szövegezését (magyartalan megfogalmazás), a szükségtelen csatolmányokat és a levélben elhelyezett hivatkozásokat.

II.11. TUDATOSSÁG ÉS KÉPZÉS

II.11.1. Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel

Az Igazgatóság a fenyegetésekre, sebezhetőségekre és biztonsági eseményekre vonatkozó legfrissebb információk megosztása érdekében kapcsolatot alakít ki és tart fenn a következő, elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és e célt szolgáló ágazati szervezetekkel:

A Nemzetbiztonsági Szakszolgálat szervezeti egységeként működő Nemzeti Kibervédelmi Intézettel, valamint az Intézet szervezetén belüli szakmai területekkel:

a) Hatóság (jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó hatósági szakterület),
b) Eseménykezelő Központ (incidenskezelési szakterület),
c) a védelmi képességek fejlesztését és üzemeltetését támogató biztonságirányítási-, és sérülékenység-vizsgálati szakterület.

II.11.2. Biztonság tudatossági képzés

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

II.11.2.1. Alapképzés

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

a) információbiztonságra vonatkozó jogszabályok;
b) információbiztonsági alapfogalmak;
c) alapvető biztonsági követelmények;
d) felhasználók napi munkavégzése során jelentkező fenyegetettségek;
e) a lehetséges fenyegetések felismerése;
f) fenyegetettségekkel szembeni védekezési lehetőségek;
g) Igazgatóság információbiztonsági szabályozó rendszerének ismertetése.

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

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

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

II.11.3. Belső fenyegetés

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

II.11.4. Szerepkör vagy feladat alapú biztonsági képzés

Az Igazgatónak, a rendszergazdának és az IBF-nek a következő, külön jogszabályban előírt továbbképzésen és éves továbbképzésen kell részt venniük:

Szerepkör megnevezése	Képzés megnevezése
Igazgató	elektronikus információs rendszerek védelméért felelős vezető (Nemzeti Közszolgálati Egyetem)
Rendszergazda	elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy (Nemzeti Közszolgálati Egyetem)
IBF	NKE végzettség esetén elektronikus információbiztonsági vezető
	A képzési rendelet 7. § (2) bekezdése szerinti nemzetközi minősítések esetében az adott minősítés fenntartásának biztosítása

II.11.5. A biztonsági képzésre vonatkozó dokumentációk

Az Igazgatóság a biztonságtudatosságra vonatkozó alap-, szerepkör vagy feladat alapú biztonsági képzéseit dokumentálja, a képzésen résztvevők a jelenléti ív aláírásával elismerik a képzés, oktatás megtörténtét és az információbiztonsági előírások megismerését.

III. Fizikai védelmi intézkedések

III.1. ALAPELVEK

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

a) az elektronikus információs rendszereket fizikailag védett, biztonságos helyre kell telepíteni, és a környezetet a berendezések gyártói által megadott fizikai feltételek szerint kell kialakítani, fenntartani;

b) a környezeti fizikai feltételeket (hőmérséklet, páratartalom, áramszolgáltatás stb.) folyamatosan ellenőrizni kell;

c) a megbízható működés biztosítása céljából a körülményeknek megfelelő legfontosabb klímatechnikai, épületgépészeti, áramellátó tartalékberendezésekről gondoskodni kell.

III.2. A TERÜLETEK FIZIKAI BIZTONSÁGI KÖVETELMÉNYEI

III.2.1. Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani.

A jelen IBSZ *{I.2.2. Tárgyi hatály}* pontja alá eső területeket az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;

b) védett terület;

c) érzékeny terület.

További védett terület kategóriákat az IBF határozhat meg.

III.2.2. Belső terület

Belső területnek tekintendők az Igazgatóság bejárata utáni közös használatú helyiségei és folyosói.

A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IBF feladata.

III.2.3. Védett terület

Védett terület valamennyi iroda és tárgyaló helyiség.

A védett területeken a következő védelmi intézkedéseket kell alkalmazni:

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

b) a fénymásoló és nyomtató berendezéseket, a fax készülékeket védett területen belül kell elhelyezni. Gondoskodni kell arról, hogy a belső területen elhelyezett eszköz esetében csak egyedi azonosítás és hitelesítés után lehessen a nyomtatást az eszközön elindítani;

c) a dokumentumok tárolása védett területen történjen;

d) azokban az időszakokban, amikor a helyiségek felügyelet nélkül maradnak, az ajtókat és ablakokat zárva kell tartani;

e) a védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

f) munkaidőn kívül, amikor az épületben senki sem tartózkodik a belső és a védett területeken elektronikus riasztórendszert kell alkalmazni.

g) ügyfelet és más külsős személyt nem szabad felügyelet nélkül hagyni.

III.2.4. Érzékeny terület

Érzékeny terület az Igazgatóság

a) szerverszobája és

b) a strukturált kábelezés rendező központjai.

Az érzékeny területekre vonatkozóan a következő védelmi intézkedéseket kell megvalósítani:

a) Az érzékeny területek elérésére az Igazgató, a rendszergazda és az IBF jogosultak. Minden más személy részére csak az Igazgató engedélyezheti a belépést.

b) Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.

c) Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében be- és kilépési naplót kell vezetni. A belépési naplót a rendszergazdák tárolják.

d) A szerverhelyiséget biztonsági ajtóval kell védeni.

e) Tilos a szerverhelyiség ajtaját nyitva hagyni, illetve tárggyal kiékelni.

f) Az érzékeny területek belépési naplóit, valamint a kiosztott jogosultságokat az IBF-nek évente ellenőriznie kell.

g) Az érzékeny területekre az ideiglenes jellegű munkát végző harmadik fél számára csak korlátozott mértékben és ellenőrzés mellett szabad biztosítani a hozzáférést. A felügyeletet a rendszergazda biztosítja.

h) A szerverszobában munkanapokon 18 órától 06 óráig, munkaszüneti napokon 0-24 óráig, illetve az utolsó rendszergazda távozása után elektronikus riasztórendszert kell alkalmazni.

i) A nyilvános helyen elhelyezett rack szekrényekben nyitásérzékelővel ellátott elektronikus riasztórendszert kell alkalmazni.

III.3. FIZIKAI BELÉPÉSI ENGEDÉLYEK

El kell készíteni és napra készen kell tartani az Igazgatóságra belépésre jogosultak listáját. A listát az Igazgató hagyja jóvá.

Amennyiben valakinek megszűnik a munkavégzésre irányuló jogviszonya, a személyügyi referensnek soron kívül törölnie kell a listáról.

Az Igazgatóságra történő be- és kilépések naplózására papír alapú jelenléti ív szolgál.

A jelenléti íven rögzíteni kell az aktuális dátumot, a munkában töltött időt, az ebédre szánt időt, valamint a további, egyéb távolléteket.

A jelenléti ívet az érintett munkatárs vezeti.

Ügyfélszolgálati időn kívül az Igazgatóság főbejárati ajtaját zárva kell tartani.

III.4. FIZIKAI BELÉPÉS ELLENŐRZÉSE

III.4.1. Fizikai belépések

Az Igazgatóság irodaként (is) funkcionáló, IT biztonsági szempontból releváns épületeibe a belépés kizárólag az alábbi pontokon lehetséges:

a) Igazgatóság egri székhelye: főbejárat

b) Kelet-bükki Tájegység miskolci őrszolgálati irodája: főbejárat

c) Kelet-bükki Tájegység tardi őrszolgálati irodája: főbejárat

d) Nyugat-bükki Tájegység irodája a Bükki Nemzeti Park Nyugati Kapu Látogatóközpont területén: főbejárat

e) Dél-hevesi Tájegység irodája: főbejárat

f) Dél-borsodi Tájegység irodája: főbejárat

g) Mátrai és Tarna-Lázbérci Tájegység irodája a Mátrai Tájvédelmi Körzet Látogatóközpont területén: főbejárat

h) Nógrádi Tájegység irodája a Baglyas-kő Vár Természetvédelmi Látogatóközpont területén: főbejárat

III.4.2. Fizikai belépések naplózása

Az Igazgatóságba történő fizikai be- és kilépések tényét naplózni kell.

Az Igazgatóságba történő be- és kilépések naplózására az Igazgatóság papír alapú jelenléti íve szolgál.

A jelenléti íven rögzíteni kell az aktuális dátumot, a munkában töltött időt, az ebédre szánt időt, valamint a további, egyéb távolléteket.

A jelenléti ívet az érintett munkatárs vezeti.

III.4.3. Vendégek kísérete

Biztosítani kell az Igazgatóságba érkező vendégek, ügyfelek kíséretét és regisztrációját, amennyiben védett munkaterületre lépnek be. A regisztrációt az érintett ügyintéző végzi el. A regisztráció során rögzíteni kell a vendég nevét, lakcímét és személyi igazolvány számát, a látogatás célját, az ügyintéző nevét, valamint a ki-és belépés időtartamát. A kíséretet annak a munkatársnak kell biztosítani, akihez a vendég érkezik.

A látogatói naplókat 1 évig meg kell őrizni.

III.4.4. Kulcsok megóvása

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

III.4.5. Rendellenességek jelentése

Valamennyi hivatali dolgozó kötelessége, hogy jelentse a jelen fejezetben leírt szabályokkal ellentétes viselkedést az Igazgatónak, aki kivizsgálja az eseményt és dönt a szükséges további intézkedésekről.

III.5. AZ INFOKOMMUNIKÁCIÓS ESZKÖZÖK BIZTONSÁGA

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

III.5.1. Az infokommunikációs eszközök elhelyezése és védelme

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

A védelmi intézkedések biztosítsák, hogy a különböző környezeti hatás miatt keletkező meghibásodások csökkenjenek. Ezért:

a) be kell tartani a tűzvédelmi előírásokat;

b) az Igazgatóság területére a normál háztartási vegyi anyagokon, tisztítószereken túl vegyi anyagot, robbanóanyagot behozni tilos;

c) a monitorokat úgy kell elhelyezni, hogy ki lehessen zárni azok illetéktelen leolvasását;

III.5.2. „Üres asztal - üres képernyő" szabály

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

a) a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc inaktivitást követően zárolja a számítógépet;

d) a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a munkaállomást;

e) a felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) ügyfelet vagy más külsős személyt irodában felügyelet nélkül hagyni tilos.

III.6. FELÜGYELET ALÓL KIKERÜLŐ ESZKÖZÖK

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

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

A munkatársak részére hosszú távú használatra kiadott nagy értékű eszközökről (pl.: laptop) az Igazgatóságnak nyilvántartást kell vezetnie. Ezen eszközöket a munkatársak korlátozás nélkül ki- és beszállíthatják a jelen IBSZ *{IV.10.14. Titkosítás}* fejezetében leírt követelmények betartásával.

Minden más esetben eszközt kiszállítani csak az Igazgató írásos engedélyével lehet.

A ki- és beszállítások ellenőrzése a rendszergazda feladata. Infokommunikációs eszközök és berendezések írásos engedély nélküli ki- és beszállításának kísérlete esetét jelenteni kell az IBF-nek a szabálysértést elkövető személy felettes vezetőjének egyidejű értesítése mellett.

Az információbiztonsági tudatosság fokozását célzó oktatások keretében a felhasználókat tájékoztatni kell az ezzel kapcsolatos ellenőrzési feladatokról és jogokról.

III.7. ÁRAMELLÁTÓ BERENDEZÉSEK ÉS KÁBELEZÉS

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

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

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

III.8. VÉSZVILÁGÍTÁS

A szerverhelyiségben automatikus vészvilágítási rendszert kell alkalmazni és karbantartani, amely áramszünet esetén aktiválódik, és amely biztosítja a szerverhelyiség biztonságos elhagyásának lehetőségét.

III.9. TŰZVÉDELEM

A szerverhelyiségben független áramellátással ellátott tűzjelző készüléket, valamint elektromos tüzek oltására alkalmas tűzoltó készüléket kell alkalmazni.

A tűzvédelem részletszabályait a Bükki Nemzeti Park Igazgatóság Tűzvédelmi Szabályzata tartalmazza.

III.10. VÍZ-, ÉS MÁS, CSŐVEZETÉKEN SZÁLLÍTOTT ANYAG OKOZTA KÁR ELLENI VÉDELEM

Biztosítani kell, hogy víz- és más csővezetéken szállított anyag esetében az Igazgató által kijelölt személyek részére hozzáférhetőek legyenek a főelzáró szelepek.

Az Igazgató felelőssége gondoskodni a főelzáró szelepek működőképességének fenntartásáról.

A szerverhelyiségben gondoskodni kell a víz és más csővezetékek kiváltásáról vagy vízbetörésérzékelő szonda felszereléséről.

III.11. HŐMÉRSÉKLET ÉS PÁRATARTALOM ELLENŐRZÉS

A szerverhelyiségben elhelyezett központi kiszolgáló egységek biztonságos működése érdekében a hőmérsékletet 20-21 Celsius fok között kell tartani.

A hőmérsékletet az elhelyezett eszközök hő leadását figyelembevevő teljesítménnyel rendelkező klímaberendezéssel kell biztosítani.

A klímaberendezés által termelt kondenzvizet erre rendszeresített zárt csatornán ki kell vezetni a szerverhelyiségből.

A relatív páratartalom szintjét 40-60% között kell tartani.

A hőmérsékletet és a relatív páratartalom szintjét arra alkalmas eszközzel folyamatosan mérni kell. Az eszköznek riasztást kell adnia (pl.: SMS, email) a rendszergazdának, hogy ha a hőmérséklet 10 Celsius fok alá csökken vagy meghaladja a 28 Celsius fokot, illetve ha a relatív páratartalom szintje eléri a fent megadott határértéket.

III.12. KARBANTARTÓK

A rendszergazdáknak nyilvántartást kell vezetni a helyszíni karbantartást végző szervezetekről vagy személyekről.

A karbantartás megkezdése előtt a rendszergazdáknak ellenőriznie kell a karbantartók személyazonosságát.

A karbantartók munkavégzésének folyamatos felügyelete biztosítása a rendszergazdák feladata és felelőssége.

IV. Logikai védelmi intézkedések

IV.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK

IV.1.1. Engedélyezés

Az Igazgatóságnak úgy kell kialakítania az általános védelmi intézkedéseit, hogy biztosított legyen

a) az elektronikus információs rendszer és annak környezete biztonsági állapotának felügyelete,

b) meghatározásra kerüljenek az információbiztonsággal összefüggő szerepkörök és felelősségi körök,

c) kijelölésre kerüljenek az ezeket betöltő személyek,

d) az elektronikus információbiztonsági engedélyezési folyamatok kerüljenek integrálásra az Igazgatósági szintű kockázatkezelési eljárásba, összhangban az informatikai biztonsági szabályzattal.

e) az elektronikus információbiztonsággal kapcsolatos engedélyezés terjedjen ki minden, az Igazgatóság hatókörébe tartozó:

f) emberi, fizikai és logikai erőforrásra;

g) eljárási és védelmi szintre és folyamatra.

IV.1.2. Elektronikus információs rendszer kapcsolódásai

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

Az összekapcsolást mind az Igazgatónak, mind a rendszergazdának, mind pedig az IBF-nek is jóvá kell hagynia.

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

Más kapcsolódó szervezet csak az Igazgatóság által nyújtott interfészen keresztül csatlakozhat az Igazgatóság EIR-jeihez.

Szerződésben vállalnia kell a kapcsolódó szervnek, hogy biztosítja a saját elektronikus információs rendszerében a cél elektronikus információs rendszer biztonsági osztályának megfelelő, a technológiai vhr által előírt követelmények teljesülését.

Információbiztonsági incidens esetén az Igazgatóság jogosult a kapcsolatot felfüggeszteni.

Szabványos, sérülékenységektől mentes kriptográfiai eszközökkel gondoskodni kell az átvitt adatok bizalmasságának és sértetlenségének biztosításáról.

IP szinten korlátozni kell a kapcsolódást.

Az összekapcsolás feltételeinek fennállását legalább évente ellenőrizni kell.

Az engedélynek tartalmaznia kell az összeköttetés pontos paramétereit, interfész-leírását (cél, technikai megvalósítás, átvitt információk, biztonsági követelmények).

IV.1.3. Belső rendszerkapcsolatok

Az Igazgatóság elektronikus információs rendszere több elemből épül fel, melyek bizonyos interfészeken kapcsolódhatnak egymáshoz. Valamennyi interfészt dokumentálni kell, és előzetesen jóvá kell hagyatni az IBF-fel.

IV.1.4. Külső kapcsolódásokra vonatkozó korlátozások

Az Igazgatóság határvédelmének működtetése során alapértelmezés szerint minden kapcsolatot tiltani kell, csak a működéshez szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Amennyiben az értelmezhető, úgy az érintett kapcsolatnál IP alapú korlátozást

kell bevezetni és gondoskodni kell a megfelelő azonosításról és hitelesítésről, valamint az átvitt adatok sértetlenségéről és bizalmasságáról.

Minden kapcsolatot előzetesen jóvá kell hagyatni az IBF-fel.

IV.2. TERVEZÉS - BIZTONSÁGTERVEZÉSI ELJÁRÁSREND

IV.2.1. Rendszerbiztonsági terv

El kell készíteni az elektronikus információs rendszerek rendszerbiztonsági tervét, mely a következőket tartalmazza:

a) az elektronikus információs rendszer hatóköre, alap feladatai (biztosítandó szolgáltatásait), biztonságkritikus elemei és alap funkciói,

b) az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztálya,

c) az elektronikus információs rendszer működési körülményei és más elektronikus információs rendszerrel való kapcsolatai.

Az elektronikus információs rendszer biztonsági követelményeit a vonatkozó rendszerdokumentációban kell rögzíteni.

Meg kell határozni a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedésbővítéseket, illetve végre kell hajtani a jogszabály szerinti biztonsági feladatokat.

Az elektronikus információs rendszerek rendszerbiztonsági tervét kétévente felül kell vizsgálni.

Soron kívül felül kell vizsgálni a rendszerbiztonsági terveket az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások, illetve a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.

Az elektronikus információs rendszerek rendszerbiztonsági tervét az érintettek bevonásával a szállító készíti el.

A rendszerbiztonsági tervek bizalmasnak minősülnek, ezért azok megismerésére az IBF, a rendszergazda, az Igazgató, valamint az Igazgató által írásban kijelölt személyek jogosultak.

IV.2.2. Cselekvési terv

A cselekvési tervre vonatkozó követelményeket a jelen IBSZ {I.5Az IBSZ általános követelményei} fejezete tartalmazza.

A cselekvési tervet a biztonsági osztályba sorolással párhuzamosan háromévente az IBF vizsgálja felül és az Igazgató hagyja jóvá.

IV.2.3. Személybiztonság

A személybiztonságra vonatkozó követelményeket a jelen IBSZ *{I.5. Az IBSZ általános követelményei}* pontja tartalmazza.

IV.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS

IV.3.1. A rendszer fejlesztési életciklusa

Az elektronikus információs rendszerek életciklusait a következő fejezetben leírtak szerint kell meghatározni:

IV.3.1.1. Követelmény meghatározás

A beszerzés előtt dokumentált formában, részletesen meg kell határozni a felhasználói és az információbiztonsági követelményeket a jelen IBSZ *{II.7. Rendszer és szolgáltatás beszerzés – Beszerzési eljárásrend}* fejezetében meghatározottak alapján.

A felhasználói követelményeket az adatgazdának, az információbiztonsági követelményeket az IBF-nek kell meghatároznia.

IV.3.1.2. Fejlesztés/beszerzés

A fejlesztés/beszerzés fázisában az IBF-nek folyamatosan képviselni kell az IBSZ-ben, illetve az információbiztonsági követelményekben foglaltak teljesülését a jelen IBSZ *{II.7. Rendszer és szolgáltatás beszerzés – Beszerzési eljárásrend}* fejezetében meghatározottak alapján.

IV.3.1.3. Megvalósítás/értékelés

Az éles bevezetés előtt tesztkörnyezetben funkcionális, biztonsági és üzemeltetési teszteket kell folytatni. A tesztek a rendszerdokumentációkban megfogalmazott elvárások bizonyítására szolgálnak.

A bevezetésről az Igazgató dönt az adatgazda, az Üzemeltetési Osztály vezetője és az IBF javaslatára.

A jelen fejezetben foglaltakra a jelen IBSZ *{II.7. Rendszer és szolgáltatás beszerzés – Beszerzési eljárásrend}* fejezetében meghatározottak az irányadók.

IV.3.1.4. Üzemeltetés és fenntartás

Az üzemeltetés és fenntartás során valamennyi érintett félnek be kell tartania az IBSZ-ben foglalt követelményeket.

IV.3.1.5. Kivonás (archiválás, megsemmisítés).

Elektronikus információs rendszer kivonása esetén értesíteni kell a Hatóságot az érintett EIR kivonásáról, valamint felül kell vizsgálni az IBSZ-t és annak *{2. számú melléklet – Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása}* mellékletét.

Kivonáskor az EIR-ben tárolt adatok archiválása után (figyelemmel az adatvédelmi előírásokra) az adathordozók újrafelhasználása vagy selejtezése esetében a jelen IBSZ *{IV.8.3. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése}* pontjában leírtak, illetve az Igazgatóság Selejtezési Szabályzata az irányadó.

IV.3.2. Funkciók, portok, protokollok, szolgáltatások

Az Igazgatóságnak meg kell követelnie a szolgáltató/fejlesztő felé, hogy az adminisztrátori dokumentációban vagy a rendszertervben határozza meg a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

IV.4. BIZTONSÁGI ELEMZÉS – BIZTONSÁGELEMZÉSI ELJÁRÁSREND

Az Igazgatóság biztonsági elemzés segítségével értékeli az elektronikus információs rendszerei és annak működési környezete védelmi intézkedéseit. A biztonságelemzés célja az, hogy az Igazgatóság meggyőződhessen arról, hogy a szükséges védelmi intézkedések megvalósítása megfelelően megtörtént, működésük a tervezettnek megfelelő. A biztonsági elemzés eredményei alapján megállapíthatók az eltérések az Igazgatóság biztonsági szabályzatai, eljárásrendjei és a gyakorlatban megvalósított megoldások között.

IV.4.1. Biztonsági értékelések

Az Igazgatóság által végzett biztonsági elemzés alapját az elektronikus információs rendszerek biztonsági osztályba sorolásából fakadó, a technológiai vhr. által előírt védelmi intézkedések alkotják.

A biztonsági elemzés az Igazgatóság Informatikai Biztonsági Szabályzatában előírt adminisztratív, fizikai és logikai védelmi intézkedések vizsgálatára kiterjed. A biztonsági elemzés tervezéséért és végrehajtásáért az IBF a felelős.

A biztonsági elemzés végrehajtásának támogatásához az IBF minden év február 28-ig biztonságelemzési tervet készít, amely a következőket tartalmazza:

a) vonatkozó védelmi intézkedések;

b) biztonsági elemzés környezete;

c) a terv végrehajtásához szükséges személyi és technikai erőforrások;

d) a terv végrehajtása során alkalmazott technikák;

e) a terv végrehajtásához kapcsolódó szerepkörök és ezek feladatai;

f) a terv végrehajtásának ütemezése.

A biztonságelemzési tervet végrehajtás előtt az Igazgatónak jóvá kell hagynia. A biztonsági elemzés végrehajtásának eredményéről biztonságelemzési jelentés készül. A biztonságelemzési jelentés tartalmazza a következőket:

g) az elvégzett tevékenység;

h) feltárt hiányosságok, sérülékenységek;

i) javasolt intézkedések.

A biztonságelemzési jelentés jóváhagyója az Igazgató. A biztonságelemzési jelentés eredményeit az Igazgatóság a kockázatelemzési folyamatában felhasználja.

IV.4.2. A biztonsági teljesítmény mérése

Az Igazgatóság a *{NIST Special Publication 800-55 –Performance Measurement Guide for Information Security}* dokumentumban található mérőszámok alapján az elektronikus információs rendszerei biztonsági teljesítményének a mérését következők szerint végzi.

A méréseket az IBF-nek kell elvégeznie a biztonságértékelési terv végrehajtásával párhuzamosan. A mérések eredményéről az IBF tájékoztatja az Igazgatót, a szükséges beavatkozásokat (eljárásrendek módosítása, felhasználói tesztek javítása) az IBF végzi el.

IV.4.2.1. Szabálysértések száma

Mérni kell, hogy hányszor és milyen okból kellett eltérni az információbiztonságra vonatkozó szabályzatokban, eljárásrendekben foglaltaktól.

a) Mérőszám neve: Szabálysértések száma

b) Mérés célja: Megbizonyosodni arról, hogy hányszor és milyen okból kellett eltérni az információbiztonságra vonatkozó szabályzatokban, eljárásrendekben foglaltaktól, illetve hányszor sérült a szabályokban foglaltak végrehajtása.

c) Mérőszám leírása: Az adott évben a szabálytól való eltérések száma.

d) Sikerkritérium: évente 5-nél kevesebb

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Biztonsági incidensek jegyzőkönyvei

IV.4.2.2. Biztonsági incidensek száma

Mérni kell, hogy egy adott időszakra vonatkozóan hány biztonsági esemény történt az elektronikus információs rendszerek működése során.

a) Mérőszám neve: Biztonsági incidensek száma

b) Mérés célja: Megbizonyosodni a biztonsági incidensek számáról.

c) Mérőszám leírása: Az adott évben a biztonsági incidensek száma.

d) Sikerkritérium: 2 db

e) Mérés gyakorisága: Évente

f) Mérési adat forrása: Biztonsági incidensek jegyzőkönyvei

IV.4.2.3. SLA

Mérni kell, hogy az elektronikus információs rendszerek nyilvánosan elérhető elemei (partnerek, ügyfelek részére biztosított) hány alkalommal nem voltak elérhetőek és össze kell vetni az ÜFT-kben vállalt rendelkezésre állási mutatókkal.

a) Mérőszám neve: SLA

b) Mérés célja: Megbizonyosodni arról, hogy a vállalt SLA érték teljesült-e.

c) Mérőszám leírása: X=(vállalt szolgáltatási időszak-kiesési idő órában)/szolgáltatási időszak*100

d) Sikerkritérium: <99,9%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Internetszolgáltatótól beszerzett statisztika, Web szerver és a tűzfal naplói

IV.4.2.4. Alkalmazás hibáinak a száma

Mérni kell, hogy az elektronikus információs rendszerek működése során hány hibát nem sikerült elhárítani.

a) Mérőszám neve: Alkalmazás hibák

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal kezelik-e a felhasználók által bejelentett hibákat.

c) Mérőszám leírása: X=(összes hiba-kezeletlen hiba)/összes hiba*100

d) Sikerkritérium: 99%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Hibajegyek

IV.4.2.5. Biztonságtudatossági képzés

Mérni kell a biztonságtudatossági képzésen részt vevő felhasználók számát, illetve a kitöltött teszt sikerességét.

a) Mérőszám neve: Biztonságtudatossági képzés

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal sajátítják el a képzési anyagot a felhasználók.

c) Mérőszám leírása: (összes felhasználó szám-tesztet nem teljesítők)/összes felhasználó száma*100

d) Sikerkritérium: 99,5%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Felhasználói tesztek

IV.4.2.6. Szerepkör alapú képzés

Mérni kell a szerepkör alapú biztonságtudatossági képzésen részt vevő felhasználók számát, illetve a kitöltött teszt sikerességét.

a) Mérőszám neve: Szerepkör alapú képzés

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal sajátítják el a képzési anyagot a felhasználók.

c) Mérőszám leírása: (Szerepkör alapú képzéseken részt vevők – sikertelen vizsgázók száma)/ Szerepkör alapú képzéseken részt vevők *100

d) Sikerkritérium: 99,5%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Szerepkör alapú tesztek

IV.4.2.7. ÜFT tesztelése

Mérni kell az ÜFT-k tesztelését.

a) Mérőszám neve: ÜFT teszt

b) Mérés célja: Megbizonyosodni arról, hogy kellő hatékonysággal tesztelik-e a kidolgozott ÜFT-ket.

c) Mérőszám leírása: (végrehajtott tesztek száma - sikertelen tesztek száma)/végrehajtott tesztek száma*100

d) Sikerkritérium: 99,5%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Szerepkör alapú tesztek

IV.4.2.8. Előírt dokumentációk elérhetősége

Meg kell vizsgálni, hogy az egyes EIR-ek megfelelően dokumentáltak-e.

a) Mérőszám neve: EIR dokumentációk

b) Mérés célja: Megbizonyosodni arról, hogy az EIR-ek rendelkeznek-e az előírt dokumentációkkal

c) Mérőszám leírása: (Megfelelő dokumentációval rendelkező EIR-ek száma/összes EIR száma*100

d) Sikerkritérium: 100%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Üzemeltetési Osztály által szolgáltatott információk

IV.4.2.9. Sérülékenységek száma

Mérni kell az egyes EIR-ekben felfedezett és nem kezelt magas vagy kritikus sérülékenységek számát. A mérést EIR-enként kell elvégezni.

a) Mérőszám neve: EIR sérülékenységek

b) Mérés célja: Megbizonyosodni arról, hogy az EIR-ek rendelkeznek-e publikus magas vagy kritikus sérülékenységgel.

c) Mérőszám leírása: (Adott időszakban az EIR-ben felfedezett magas vagy kritikus sérülékenységek száma/Adott időszakban kezelt magas vagy kritikus sérülékenységek száma)*100

d) Sikerkritérium: 100%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Sérülékenység vizsgálatok jegyzőkönyvei

IV.4.2.10. Mobil eszközök biztonsága

Meg kell bizonyosodni arról, hogy az Igazgatóság adatokat kezelő mobil eszközök közül hány eszközön alkalmaznak megfelelő tároló titkosítást.

a) Mérőszám neve: Mobil eszközök biztonsága

b) Mérés célja: Megbizonyosodni arról, hogy Igazgatóság adatokat kezelő mobil eszközök közül hány eszközön alkalmaznak megfelelő tároló titkosítást.

c) Mérőszám leírása: (tároló titkosítást alkalmazó Igazgatóság adatot kezelő mobil eszköz/összes Igazgatóság adatot kezelő mobil eszköz)*100

d) Sikerkritérium: 100%

e) Mérés gyakorisága: évente

f) Mérési adat forrása: Vagyonleltár

IV.5. TESZTELÉS, KÉPZÉS, FELÜGYELET

IV.5.1. Tesztelési, képzési és felügyeleti eljárások

Az Igazgatóság a jelen fejezetben foglaltak alapján valósítja meg az elektronikus információs rendszerei tesztelésével, képzésével és felügyeletével kapcsolatos eljárásokat, amelyek támogatják a tesztelési, képzési és felügyeleti tevékenységek:

a) fejlesztését és fenntartását;

b) folyamatos időbeni végrehajtását.

Az Igazgatóságnak felül kell vizsgálnia a tesztelési, képzési és ellenőrzési terveket a kockázatkezelési stratégia és a lehetséges, vagy bekövetkezett biztonsági események súlya alapján.

IV.5.2. Sérülékenység teszt

Az Igazgatóság elektronikus információs rendszerei sérülékenység tesztjét a jogszabály által kijelölt Nemzeti Kibervédelmi Intézet Eseménykezelő Központ végezheti.

A sérülékenység tesztet az érintett elektronikus információs rendszeren az olyan újonnan ismerté vált sérülékenységek esetén - amelyek érinthetik a rendszert, illetve alkalmazást - mielőbb, de minimum évente megismételni szükséges.

Az elvégzett vizsgálatról jelentést kell készíteni, amelyben a hibák, nem megfelelően konfigurált elemek kerüljenek kimutatásra, illetve az ezekre tett hibaelhárítási javaslatok jelennek meg.

A vizsgálat során feltárt sérülékenységek hatásait ki kell értékelni, be kell építeni a kockázatértékelési folyamatba. Gondoskodni kell arról, hogy a kritikus és a magas sérülékenységek soron kívül kerüljenek megszűntetésre, csillapításra.

A sérülékenységi vizsgálatok koordinálásáért és kiértékeléséért az IBF felelős.

IV.5.3. Frissítési képesség

Az Igazgatóságnál végzett sérülékenységi teszt csak olyan eszközzel végezhető, amely megfelel az iparági sztenderdeknek, így képes a szoftverkomponenseit, szignatúráit frissíteni, hogy képes legyen az újonnan feltárt sérülékenységeket is felismerni.

IV.5.4. Frissítés időközönként, új vizsgálat előtt vagy új sérülékenység feltárását követően

Az Igazgatóságnál sérülékenység-teszt céljából használt eszköz szignatúra adatbázisát új vizsgálat megkezdése előtt frissíteni szükséges, így biztosítva, hogy az eszköz képes legyen a legutóbb megismert sérülékenységek felismerésére az elektronikus információs rendszerben.

IV.5.5. Privilegizált hozzáférés

Az érintett elektronikus információs rendszerhez az IBF által ellenőrzött és dokumentált körülmények közt az Igazgatóság privilegizált hozzáférést is biztosít az Eseménykezelő Központ részére.

IV.5.6. Felfedhető információk

A sérülékenységi teszt után az IBF-nek fel kell mérnie, hogy egy támadó milyen érzékeny adatokhoz lehet képes hozzáférni az Igazgatóság információvagyonából. A vizsgálatot követően kockázatelemzés alapján intézkedéseket kell foganatosítani az érzékeny adatok megismerésének elhárítására.

IV.6. KONFIGURÁCIÓKEZELÉSI ELJÁRÁSREND

IV.6.1. Alapkonfiguráció

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

A dokumentációnak minimálisan a következő elemeket kell magában foglalnia: a munkaállomásokra, kiszolgálókra, a hálózati eszközökre és egyéb mobil eszközök telepített operációs rendszerek és egyéb szoftverek verzióit, patch szintjét, továbbá az egyes szoftverkomponensek biztonságosnak ítélt konfigurációs beállításait.

Vázolni kell az érintett EIR elhelyezkedését a logikai topológiában.

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

IV.6.2. A konfigurációváltozások felügyelete (változáskezelés)

A változáskezelés szabályozásának célja a produktív elektronikus információs rendszer biztonságos módosítási lehetőségeinek és folyamatának meghatározása, és ezzel a naprakész rendszerállapot-információk elérhetőségének biztosítása.

Jelen eljárásrend azt szabályozza, hogy a változtatásban érintett szervezeti egységek jóváhagyása (javaslata) és az érintettek tájékoztatása hogyan zajlik, és ez alapján milyen módon történhet meg egy változtatás.

Minden változást megfelelően és visszakereshetően dokumentálni kell, amely alapján a változások egyértelműen megállapíthatóak.

Minden egyes változást az Igazgatóság megfelelően tesztel és dokumentál, mielőtt azt az éles rendszeren alkalmazná.

A vizsgált rendszer esetében a következő tevékenységek tartoznak a változáskezelés hatálya alá:

a) fejlesztések, verzióváltás,

b) a rendszerelemek cseréje (hardver, szoftver),

c) a rendszerműködés, konfiguráció módosítása,

d) a gyártó által kiadott frissítések telepítése.

IV.6.2.1. Változáskezelési előírások

A változáskezeléssel kapcsolatosan az alábbi előírásokat kell figyelembe venni:

a) A rendszer bármely funkcióját megváltoztató művelethez - beleértve a verzióváltást és egyéb, jelentős beavatkozást igénylő hangolást is - az informatikai terület és az adatgazdai terület vezetőjének engedélye szükséges.

b) A változtatást az kezdeményezi, akinél az igényként felmerül.

c) Minden változtatással kapcsolatos bejelentés, véleményezés, döntés, a kivitelezés dokumentálása egy változáskezelési űrlap/kérelem és egy változáskezelési nyilvántartási táblázat kitöltésével jár együtt.

d) A változtatási kérelemre vonatkozó valamennyi dokumentációt az informatikai területnek nyilvántartásba kell venni és visszakereshető formában kell tárolnia.

e) A tervezett változtatást véleményezés céljából meg kell küldeni az IBF-nek is, aki kockázatelemzéssel megállapítja a tervezett változtatás rendszerre gyakorolt hatását.

f) Az IBF-nek a fentiek elvégzése után ellen kell jegyeznie a változtatási kérelmet.

g) Az éles üzembe állítást csak a változással érintett adatok, rendszerek teljes mentését követően lehet elvégezni.

h) Amennyiben a változtatáshoz a rendszer leállítása szükséges, akkor arról az informatikai terület a felhasználókat legalább 1 héttel a leállítást megelőzően tájékoztatni köteles.

A változáskezelési előírások betartását és a változáskezelési folyamatot az elektronikus információs rendszerek biztonságáért felelős személy az éves ellenőrzési tervében foglaltak szerint ellenőrzi.

IV.6.3. Előzetes tesztelés és megerősítés

A változtatásokat először tesztelni szükséges. A tesztkörnyezet nem tartalmazhat éles adatokat, illetve személyes adatokat. A tesztkörnyezetben a személyes adatokat algoritmus felhasználásával anonimizálni kell.

A tesztkörnyezet jogosultsági beállításai, jogosultságkezelési folyamatai és adatbiztonsága az éles rendszerrel megegyező elvárásokat kell, hogy teljesítse. A teszt adatbázist teljes mértékben az eredetivel megegyező módon kell kezelni, a hozzáférés szabályozást is beleértve.

Az üzemeltetői teszteket az informatikai terület, a felhasználói teszteket a szakterület munkatársai, a biztonsági teszteket az IBF végzi el.

A tesztelést dokumentált formában kell végezni, a tesztek eredményeit dokumentálni kell, amely alapul szolgál a változtatás éles környezetben történő átvezethetőségére.

Az éles rendszerben történő változtatás előtt frissíteni kell a rendszer valamennyi érintett dokumentációját, úgy, hogy az konzisztens legyen a véghezvitt változtatásokkal.

IV.6.4. Biztonsági hatásvizsgálat

A változtatás megkezdése előtt az IBF-nek egy előzetes kockázatelemzéssel és a biztonsági funkciók tesztelésével kell biztosítania a változtatás éles környezetre ható kockázatainak minimalizálását. A kockázatelemzésnek ki kell terjedni minden olyan lényeges elemre, amely rávilágíthat a változtatás következtében bekövetkező biztonsági problémákra.

IV.6.5. Konfigurációs beállítások

A vizsgált rendszer működtetése során csak jóváhagyott hardver és szoftver elemek használhatók, melyek a rendszer rendszerdokumentációjában szerepelnek. A rendszer minden egyes eleméhez a konfigurációs beállítások elvégzését, annak dokumentálását végre kell hajtani. Minden egyes módosítást, amely a konfiguráció beállításokhoz köthetőek, megfelelően dokumentálni kell.

A fentiektől eltérő hardver/szoftver alkalmazása változtatásnak minősül, ezért annak végrehajtása során a *{IV.6.2. A konfigurációváltozások felügyelete (változáskezelés)}* fejezetben leírtakat kell alkalmazni.

A kötelező, jóváhagyott konfigurációs beállításokat az IBF az éves ellenőrzési tervében foglaltak szerint, a rendszerdokumentációban foglaltak alapján ellenőrzi.

IV.6.6. Legszűkebb funkcionalitás

Az Igazgatóság elektronikus információs rendszereiben csak a szükséges portokat, protokollokat és szolgáltatásokat szabad engedélyezni. Az engedélyezett portokat, protokollokat és szolgáltatásokat dokumentálni kell a rendszer alapkonfigurációjában.

A munkaállomások és a kiszolgálók alapkonfigurációjának a kialakításakor figyelembe kell venni a nemzetközi „Center for Internet Security” szervezet ajánlásait. Ennek érdekében hardening guide-okat kell kidolgozni és beállítani az EIR-eket alkotó szoftverkomponensek esetében.

A hardening guide-okat az IBF állítja össze az Üzemeltetési Osztály vezetőjével. A beállításokat az Üzemeltetési Osztály hajtja végre előzetes tesztelést követően.

A hardening guide-okat évente felül kell vizsgálni.

IV.6.7. Elektronikus információs rendszerelem leltár

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

IV.6.8. A szoftver használat korlátozásai

Az Igazgatóságnál kizárólag az Igazgató által engedélyezett, jogtiszta, a megfelelő licence-el rendelkező szoftvereket lehet használni.

Az alkalmazott szoftverekről leltárt kell vezetni.

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

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

A szerzői jogokkal védett szellemi termékek felhasználását nyomon kell követni.

IV.6.9. A felhasználó által telepített szoftverek

A felhasználók semmilyen alkalmazást (beleértve a csupán másolással telepíthető alkalmazásokat is) nem telepíthetnek a munkaállomásaikra. A rendszerprogramok, illetve a felhasználói alkalmazások telepítését a kiszolgálókra és munkaállomásokra csak a rendszergazda végezheti el.

A felhasználók munkaállomásain telepített alkalmazások megfelelőségét az IBF szúrópróbaszerűen ellenőrzi.

IV.7. RENDSZER KARBANTARTÁSI ELJÁRÁSREND

Az elektronikus információs rendszerek karbantartására vonatkozóan a jelen fejezetben leírtak az irányadók:

IV.7.1. Rendszeres karbantartás

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

IV.7.2. A karbantartások engedélyezése

A tervezett karbantartásokat dokumentált formában az Igazgató engedélyezi. Amennyiben ez az elektronikus információs rendszerek leállításával jár, akkor a felhasználókat a karbantartás megkezdése előtt legalább 1 héttel értesíteni szükséges.

IV.7.3. A karbantartások dokumentálása, nyilvántartása

Az elvégzett munkákat jegyzőkönyvezni kell, valamint a karbantartás tényét karbantartási nyilvántartásban kell dokumentálni, illetve nyilvántartani. A nyilvántartásba a következő adatokat kell minimálisan rögzíteni:

a) az elvégzett karbantartás megnevezése,

b) az érintett eszközök, szoftverek, elektronikus információs rendszerek,

c) a karbantartás engedélyezője,

d) a karbantartás elvégzője,

e) a karbantartás dátuma,

f) leállási idő (ha volt ilyen).

A jegyzőkönyveket csatolni kell a karbantartási nyilvántartáshoz.

IV.7.4. A karbantartások ütemezése

Éves karbantartási tervet kell készíteni, melyben meg kell tervezni a karbantartások ütemezését. A terv elkészítése a rendszergazda, a terv jóváhagyása az Igazgató feladata.

IV.7.5. Kiszállítás

Amennyiben az adatot tartalmazó adathordozó kiszállítása válik szükségessé, akkor a jelen IBSZ *{IV.8.3Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése}* fejezetben leírtak szerint kell eljárni. A kiszállítást a rendszergazda engedélyezi.

IV.7.6. A karbantartás ellenőrzése

Az elvégzett karbantartás után az eszköz fajtájától függően funkcionális és biztonsági teszteket kell végezni, melynek eredményét rögzíteni kell a karbantartási nyilvántartásban. Sikertelen teszt esetén az eszköz nem helyezhető újra éles üzembe.

IV.7.7. Karbantartók

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

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

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

a) szervezet megnevezése,

b) szerződésszám,

c) szerződés időtartama,

d) szerződéses kapcsolattartó neve, elérhetősége,

e) karbantartást végzők neve, elérhetősége,

f) szerződés tárgya, hatálya (mely rendszerelemre terjed ki).

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

A külső féllel kötött szerződébe kell foglalni, hogy a karbantartást felügyelők jogosultak kérni a karbantartást végző személy személyazonosságának igazolását, illetve hogy a karbantartást végző személynek kötelessége a felszólításra a szükséges iratokat bemutatni.

IV.8. ADATHORDOZÓK VÉDELMÉRE VONATKOZÓ ELJÁRÁSREND

Az adathordozók védelmére a következő előírások vonatkoznak.

IV.8.1. Hozzáférés az adathordozókhoz, adathordozók használata

Az Igazgatóságnál csak az Igazgatóság tulajdonában lévő, regisztrált adathordozót lehet használni. Adathordozó igénylését a rendszergazdához kell benyújtania a szervezeti egység vezetőjének.

Az eszközhasználatot, az Igazgatóság elektronikus információs rendszereihez történő csatlakoztatása után, az Igazgatóság minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot floppyn, CD-n, elektronikus levélben vagy egyéb más módon (Pl.: Pen drive) az Igazgatóság informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának vagy a szervezeti egység vezetőjének kell engedélyeznie, minden esetben írásos formában.

Az Igazgatóság az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

IV.8.2. Adathordozók tárolása

Az Igazgatóság elektronikus információs rendszereinek kiszolgáló oldali adathordozóit a szerverhelyiségben kell tárolni. A szerverhelyiség fizikai védelmét a jelen IBSZ *{III. Fizikai védelmi intézkedések}* fejezetében foglaltaknak megfelelően kell kialakítani.

A felhasználók részére kiosztott mobil adathordozókat használaton kívül zárható irodabútorban kell tárolni.

IV.8.3. Az infokommunikációs eszközök biztonságos újrahasznosítása, mások rendelkezésére bocsátása, selejtezése

IV.8.3.1. Újrahasznosítás

Infokommunikációs eszközök újrahasznosítása előtt a következők végrehajtása szükséges:

a) a rajtuk tárolt adatokat helyreállíthatatlanságot garantáló logikai törléssel (pl.: Eraser) törölni kell;

b) a törlést az adattárolón lévő adatok gazdájának jóvá kell hagynia;

c) garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az IBF dönt az eszköz cserére történő kiadhatóságáról, vagy megsemmisítéséről.

Az Igazgatósági adatokat tartalmazó infokommunikációs eszközök harmadik fél részére történő átadása újrafelhasználás céljából - a fentiek végrehajtásától függetlenül információbiztonsági szempontból - nem engedélyezett, egyedi esetekről az Igazgató az IBF bevonásával dönt.

IV.8.3.2. Selejtezés

Infokommunikációs eszközök selejtezése előtt az Igazgatóság Selejtezési Szabályzatában foglaltakon túl még működőképes eszköz esetén a rajtuk tárolt adatokat helyreállíthatatlanságot garantáló logikai törléssel (pl.: Eraser) a rendszergazda útján törölni kell, valamint függetlenül az eszköz működőképességétől megfelelő tanúsítvánnyal rendelkező adatmegsemmisítéssel foglalkozó szakértő bevonásával fizikai rongálással vagy megsemmisítéssel kell gondoskodni az eszközökön tárolt adatok visszaállíthatatlanságáról.

Az adatok megfelelő módon történő eltávolításáért a rendszergazda a felelős. Az adatok eltávolítását jegyzőkönyvezni kell.

IV.8.4. A hordozható infokommunikációs eszközök védelme

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

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek, emiatt nem szabad őrizetlenül hagyni autóban, szállodai szobában;

IV.8.5. Mobil infokommunikációs eszközök ellopása esetén

Mobil infokommunikációs eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az IBF-nek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha az eszközt a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és az Igazgató részére át kell adni.

IV.8.6. Infokommunikációs eszköz elvesztése

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

IV.9. AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁSREND

IV.9.1. Azonosítás és hitelesítés (szervezeten belüli felhasználók)

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

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

IV.9.2. Hálózati hozzáférés privilegizált fiókokhoz

A privilegizált felhasználói fiókok hálózati hozzáférésekor többtényezős azonosítást és hitelesítést kell alkalmazni, oly módon, hogy a hálózati bejelentkezés során Active Directory címtár szintjén a tudás (hálózati azonosító és jelszó) mellett birtoklás (hard vagy soft token) alapú azonosítást és hitelesítést is alkalmaz az Igazgatóság.

A többtényezős hitelesítést távoli hozzáférések során is alkalmazni kell.

IV.9.3. Azonosító kezelés

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

90 nap inaktivitás után az azonosítókat a rendszergazdának le kell tiltania.

A fentiek háromhavi rendszerességgel történő végrehajtása az rendszergazdák feladata.

IV.9.4. A hitelesítésre szolgáló eszközök kezelése

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 Igazgatóság jelszókezelő rendszere:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását;

b) kényszerítse ki az ideiglenes jelszavak megváltoztatását az első bejelentkezéskor;

c) kényszerítse ki a megfelelő minőségű jelszavak használatát;

d) kényszerítse ki a jelszóváltoztatást;

e) tiltsa meg a korábban használt jelszavak ismételt felhasználását;

f) beíráskor ne jelenítse meg a jelszavakat a képernyőn;

g) a jelszó állományokat egyirányú lenyomatképző algoritmussal védje, biztosítsa a jelszavak visszaállíthatatlanságát a tárolt adatokból;

h) változtassa meg a szállító alapértelmezett jelszavát a szoftver installálása után.

Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni, úgy, hogy:

a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavaik titokban tartását;

b) biztosítani, hogy a kezdeti jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) a jelszó legalább nyolc karakter hosszú legyen, és - ahol műszakilag az megvalósítható - törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 90 naponta meg kell változtatni;

c) a jelszavakat két napon belül nem szabad megváltoztatni;

d) az előző jelszavak újra használatát 24 alkalomig kerülni kell;

e) 5 sikertelen bejelentkezési kísérlet esetére 30 percre zárolja a fiókot és a számlálót 30 perc után nullázza.

IV.9.4.1. Technikai azonosítók kezelése

A technikai azonosítók elkülönített úton történő kezelését a jelen fejezetben foglaltak szerint kell megvalósítani:

A technikai azonosítókat a rendszergazda hozza létre. A technikai azonosítóknak nem adható automatikusan rendszergazda jog, törekedni kell a „szükséges, minimális jogok elve” alapján a minimális jog biztosítására.

Az azonosítók létrehozásánál biztosítani kell a nevükben futó alkalmazások, szolgáltatások egyedi azonosítását és hitelesítését a következő névkonvenció alapján: _svc_”futó szolgáltatás rövid neve”.

A technikai azonosítók jelszavait jelszógenerátorral véletlenszerűen kell képezni, úgy hogy a jelszó hossza minimum 20 karakter legyen és feleljen meg a bonyolultsági kritériumnak.

Gondoskodni kell a technikai azonosítók jelszavainak évente történő megváltoztatásáról.

A jelszavakat vagy lezárt borítékban és páncélszekrényben vagy szabványos, kriptográfiai algoritmussal őrzött jelszókonténerben kell tárolni. A jelszókonténer mesterjelszavát lezárt borítékban, páncélszekrényben kell őrizni.

IV.9.5. A felhasználó felelősségi köre a jelszó használat során

Az Igazgatóság elektronikus információs rendszereiben a jelszavak használatának és képzésének részletes szabályai a következők:

a) a felhasználó a jelszavát köteles titokban tartani;

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben;

c) a felhasználói jelszót TILOS leírni;

d) ha bármilyen jel mutat arra, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell az IBF-et;

e) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:

f) könnyen megjegyezhető, és nehezen kitalálható legyen;

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

h) ne legyen a gépnévre vagy a felhasználói névre utaló;

i) ne legyen sorozat.

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

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

IV.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az illetéktelen hozzáférések elkerülése érdekében olyan hitelesítési módszereket kell alkalmazni, amely a beütött jelszavak karaktereit valamilyen helyettesítő karakterrel ábrázolja (pl.: csillag karakter).

IV.9.7. Hitelesítés kriptográfiai modul esetén

Az Igazgatóság nem alkalmaz kriptográfiai modult az azonosítási és hitelesítési folyamatai során.

IV.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

Az elektronikus információs rendszernek egyedileg kell azonosítania és hitelesítenie az érintett szervezeten kívüli felhasználókat, illetve a tevékenységüket.

IV.9.9. Hitelesítés szolgáltatók tanúsítványának elfogadása

Az Igazgatóság EIR-jeihez történő külső felhasználó általi hozzáférés esetén, amennyiben az azonosítás és hitelesítés kriptográfiai tanúsítvány felhasználásával történik, csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő bizalmi szolgáltatók által kibocsátott tanúsítványokat lehet felhasználni.

IV.10. HOZZÁFÉRÉS ELLENŐRZÉSI ELJÁRÁSREND

A hozzáférési jogok kezelését jelen eljárásrendben foglaltak szerint kell megvalósítani a következő alapelvek alkalmazásával:

a) Minden felhasználó csak a feladatellátásához szükséges, minimális jogosultságot kapja meg.

b) A felhasználók a munkaállomásukon nem rendelkezhetnek rendszergazda jogokkal.

c) A rendszergazda a rendszerek adminisztrálásához használt adminisztrátori azonosítóját a napi munkavégzése során nem használhatja. A napi munkavégzéshez normál felhasználói jogú azonosítót kell használnia.

IV.10.1. Felhasználói fiókok kezelése

Elektronikus információs rendszerenként meg kell határozni, hogy milyen típusú fiókok engedélyezettek (pl.: általános, megosztott, csoport, gyártói/fejlesztői/szállítói, ideiglenes, vendég, technikai).

Meg kell határozni azokat az alapfunkciókat (alapjogosultságokat) melyeket munkakörökhöz lehet rendelni és ezeket a jogosultságokat a felhasználók automatikusan megkaphatják a munkakör betöltésekor.

Elektronikus információs rendszerenként dokumentálni kell az érintett EIR-ben létrehozott szerepköröket és a szerepkörökhöz rendelt jogosultságokat (szerepkör-jogosultsági mátrix).

Az Igazgatóság EIR-jeihez hozzáférési jogosultságokat vagy az Igazgatóság Szervezeti és Működési Szabályzata alapján meghatározott alapfunkciók alapján vagy egyedi igénylések alapján lehet biztosítani.

A beépített adminisztrátori és vendég fiókokat valamennyi eszközön tiltani kell.

A felhasználók csak jóváhagyott hozzáférés-védelmi megoldásokat alkalmazhatnak.

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

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

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

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

d) Az összeférhetetlenségi szabályokat figyelembe kell venni.

e) Az elektronikus információs rendszerben alkalmazott hozzáférési jogosultságokat adminisztrálni kell.

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

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

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

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

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

b) A csoportos felhasználó azonosítók használatát tiltani kell.

c) A felhasználói hozzáférési jogosultságokat a szervezeti egység vezetője határozza meg. A jogosultság meghatározása során figyelembe kell venni:

   i. a felhasználó munkakörét és az azzal kapcsolatos feladatait;

   ii. a munkaköri feladatok végrehajtásához minimálisan szükséges jogosultságok elvét;

   iii. a felhasználó jogviszonyát;

   iv. a felhasználó munkahelyét.

d) A jogosultság igénylését tartalmazó dokumentumnak tartalmaznia kell:

   i. a felhasználó nevét, munkakörét, szervezeti egységét és munkahelyét;

   ii. annak megjelölését, hogy milyen szolgáltatásokhoz történik a jogosultságigénylés;

   iii. azt, hogy az érintett szolgáltatások tekintetében milyen szerepkör, vagy hozzáférési jogok (olvasás, bevitel/bővítés, törlés, módosítás, teljes) igénylése történik;

   iv. annak megjelölését, hogy az érintett szolgáltatások és jogosultságok igénylése milyen adatkörre vonatkozóan történik;

   v. a munkahelyi vezető aláírását.

A jogosultságigénylési lapot az igényelt és a beállított jogosultságok egyeztetése céljából a rendszergazda tárolja.

IV.10.2. Kiemelt jogosultságok kezelése

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

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

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

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

c) az adminisztrátori jogot kizárólag az Igazgató engedélyezheti írásban;

d) technikai azonosító részére adminisztrátori jogot az IBF engedélyezi írásban.

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

A rendszergazda nem küldhet levelet más felhasználó nevében.

IV.10.3. Hozzáférési jogok igénylésének eljárásrendje

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

IV.10.3.1. Új hozzáférési jog igénylése

Az igénylő a hozzáférési jogok igénylését a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlap kitöltésével kezdeményezi. Hozzáférési jogot az igényelhet, akinek a feladatellátásához az szükséges.

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

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

Az űrlapot ezután meg kell küldeni az adatgazda részére, aki jóváhagyja a jogosultságigénylést.

A jóváhagyott jogosultságigénylési űrlapot ezután el kell küldeni rendszergazda részére, aki intézkedik a jogosultság kiadásáról.

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ *{6. számú melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda az igényelt beállításokkal létrehozott felhasználói fiókról telefonon vagy személyesen értesíti az igénylőt, és megadja a belépéshez használatos felhasználói nevet, és az első belépést lehetővé tevő kezdeti jelszót és szükség esetén egyéb fontos adatokat. Telefonos kapcsolat esetén az igénylőlapon rögzített információk alapján azonosítani kell az igénylőt.

A feldolgozás harmadik lépése: a kért feladatok elvégzésének bizonylatolása érdekében a rendszergazda aláírja a kitöltött jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}* mellékletét, valamint e-mail-en tájékoztatja az igénylőt és a jóváhagyót a jogosultságok megadásáról és a felhasználói névről.

Az aláírt űrlapokat a rendszergazda tárolja visszakereshető formában.

Az IBF az említett adatlapok meglétét és a tényleges jogosultság kiadását bármikor ellenőrizheti, és véleményét írásba foglalhatja, amelyet az Igazgatóság a jogosultsági rendjének folyamatos javítására használ fel.

IV.10.3.2. Hozzáférési jog módosítása

A munkahelyi vezető a dolgozó megváltozott feladatkörének, illetve munkakörének ellátásához szükséges jogosultság módosításához kitölti a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapot.

Az eljárásrend megegyezik az *{IV.10.3.1 Új hozzáférési jog igénylése}* fejezetben leírtakkal annyi kiegészítéssel, hogy amennyiben szervezeti egység váltás történik, akkor a rendszergazda gondoskodik a már nem szükséges jogosultságok visszavonásáról.

IV.10.3.3. Hozzáférési jog visszavonása

A munkahelyi vezetőnek haladéktalanul intézkednie kell a már nem szükséges jogosultságok visszavonása iránt. A hozzáférési jogosultság visszavonását a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található űrlapon kell kezdeményezni.

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

A feldolgozás első lépése: A rendszergazda rögzíti az igényt a jelen IBSZ *{6. számú melléklet – Hozzáférések nyilvántartása űrlap}* mellékletében található űrlapon.

A feldolgozás második lépése: a rendszergazda visszavonja a jogosultságot.

A feldolgozás harmadik lépése: a rendszergazda aláírja a jelen IBSZ *{5. számú melléklet – Jogosultságigénylési űrlap}* mellékletében található, kitöltött űrlapot, valamint e-mail-en tájékoztatja a munkahelyi vezetőt a visszavonás tényéről.

IV.10.3.4. A felhasználói hozzáférési jogok felülvizsgálata

Ellenőrizni kell, hogy a kiadott hozzáférési jogosultságok szintje alkalmas-e a kívánt célra (biztosítja-e az elvárt logikai védelmet). Ennek érdekében a kiosztott hozzáférési jogokat az IBF évente felülvizsgálja.

IV.10.4. Hozzáférés ellenőrzés érvényre juttatása

Az elektronikus információs rendszereknek az IBSZ-szel összhangban érvényre kell juttatnia a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

IV.10.5. Sikertelen bejelentkezési kísérletek

Az Active Directory (továbbiakban: AD) alapú hálózatba történő bejelentkezések során 5 sikertelen bejelentkezési kísérlet során 30 percre zárolni kell az érintett fiókot. A számlálót 30 perc után lehet nullázni vagy a fiókot csak a rendszergazda engedélyezheti újra.

Nem AD alapú hitelesítés esetén az érintett elektronikus információs rendszerben egyedileg kell a fentieket kikényszeríteni.

IV.10.6. A rendszerhasználat jelzése

Az elektronikus információs rendszerekbe történő bejelentkezés előtt ki kell jelezni a felhasználó számára, hogy a felhasználó az Igazgatóság adott éles rendszerét használja és a bejelentkezéssel egyidejűleg a beleegyezését adja, hogy az Igazgatóság

a) a rendszer használatát figyelheti, rögzítheti, naplózhatja;

b) a rendszer jogosulatlan használata tilos, és büntetőjogi vagy polgárjogi felelősségre vonással jár.

IV.10.7. A munkaszakasz zárolása

Az Igazgatóság munkaállomásain 10 perc inaktivitás után automatikusan életbe lépő képernyőzárolást kell alkalmazni, melyet csak a hálózathoz vagy a munkaállomáshoz tartozó jelszó megadását követően lehet inaktiválni.

IV.10.8. Képernyőtakarás

A munkaszakasz zárolását oly módon kell megvalósítani, hogy a zárolási képernyőn vagy a felhasználó által beállított háttérkép vagy egy üres képernyő látszódjon.

IV.10.9. A munkaszakasz lezárása

A felhasználó a munkaidő végeztével köteles a munkaállomását kikapcsolni.

IV.10.10. Távoli hozzáférés

Az Igazgatóság elektronikus információs rendszereihez VPN-en keresztül lehet hozzáférni. Az elektronikus levelezési szolgáltatás Roundcube webmail szolgáltatáson keresztül is elérhető.

A távoli hozzáféréshez csak olyan munkaállomás vagy laptop használható

a) mely naprakész (az operációs rendszer és az alkalmazások biztonsági frissítései telepítésre kerültek);

b) helyi, bekapcsolt tűzfallal rendelkezik;

c) naprakész, memóriában rezidens vírusvédelemmel rendelkezik.

A fentiek biztosítása az eszköz felhasználójának a felelőssége.

IV.10.11. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

Az Igazgatóságnál nincsenek azonosítás és hitelesítés nélkül engedélyezett tevékenységek, kivéve az elektronikus információs rendszerek azonosításához és hitelesítéséhez szolgáló felületek elérése.

IV.10.12. Vezeték nélküli hozzáférés

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

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

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

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

Az Igazgatóság belső hálózatához történő hozzáférés esetén csak olyan Wi-Fi hozzáférési pont létesíthető, amely AD integrált felhasználói hitelesítést (802.1x) alkalmaz.

Csak internet kapcsolatot biztosító (vendég, képviselői) Wi-Fi hozzáférések esetén minimum WPA2 titkosítást kell alkalmazni. Kockázat elemzéssel kell meghatározni a szükséges védelmet és a megfelelő hitelesítési módszert.

A kiosztott kulcsok létrehozására vonatkozóan a következőket kell követni:

a) A kulcs hossza minimum 12 karakter.

b) A kulcs tartalmazzon kisbetűt, nagybetűt, számot vagy speciális karaktert.

A kulcsot háromhavonta meg kell változtatni.

Az Igazgatóság belső hálózatából a munkaállomásokról és laptopokról tilos mobil internet megosztással internetelérést kezdeményezni.

IV.10.13. Mobil eszközök hozzáférése

Mobil eszközzel csak az Igazgatóság által biztosított elektronikus levelezéshez lehet hozzáférni. Az Igazgatóság által biztosított elektronikus levelezéshez alapvetően az Igazgatóság által biztosított mobil eszköz használható.

Saját tulajdonú mobil eszköz akkor használható, hogy ha azon

a) a tároló titkosítás bekapcsolásra került;

b) legalább pin kódos azonosítást alkalmaznak;

c) kártékony kód elleni védelem telepítésre került.

Tilos továbbá ezen eszközöket rootolni vagy jailbreak-elni (a gyártó által nem engedélyezett módón többlet jogosultságot szerezni).

IV.10.14. Titkosítás

Az Igazgatóság által biztosított mobil eszközökön be kell kapcsolni a teljes eszköz vagy tároló titkosítást. A titkosításhoz szabványos, sérülékenységektől mentes kriptográfiai algoritmusokat kell alkalmazni.

IV.10.15. Külső elektronikus információs rendszerek használata

Az Igazgatóság belső elektronikus információs rendszereinek külső hozzáférése során ismert sérülékenységektől mentes, szabványos titkosítású algoritmust alkalmazó VPN kapcsolatot kell használni, melynek során egyedileg kell azonosítani és hitelesíteni a felhasználót. A munka befejeztével bontani kell a VPN kapcsolatot.

Az Igazgatóság belső elektronikus információs rendszereinek külső hozzáféréséhez csak olyan biztonságos eszköz használható, amely megfelel a következő követelményeknek:

a) Az eszközökön a felhasználóknak rendszergazdai jog nem adható.

b) Az eszközökön naprakész kártékony kód elleni védelmet kell megvalósítani.

c) Az eszközökön az operációs rendszer és a felhasználói programok naprakészségét biztosítani kell.

d) Az eszközökön bekapcsolt tűzfalat kell alkalmazni.

e) A kapcsolat idejére a helyi eszköz háttértárolóinak a felcsatolása és a vágólap használata nem engedélyezett.

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

IV.10.16. Nyilvánosan elérhető tartalom

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

A nyilvános tartalmak kezelésével kapcsolatban a következők szerint kell eljárni:

a) Ki kell jelölni azokat a személyeket, akik jogosultak az Igazgatóság honlapján az Igazgatóság és az Igazgatóság működésével kapcsolatos bármely információ közzétételére;

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

c) gondoskodni kell arról, hogy közzététel előtt átvizsgálásra kerüljenek a publikálandó tartalmak;

d) Időszakosan át kell vizsgálni az Igazgatóság honlapját a nem nyilvános információk tekintetében, és gondoskodni kell azok eltávolításáról.

IV.11. RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉGRE VONATKOZÓ ELJÁRÁSREND

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

IV.11.1. Hibajavítás

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

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

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

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

Új hardverek üzembe állításakor a fentieket kell értelemszerűen alkalmazni.

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

Gyártói támogatással nem rendelkező operációs rendszerek és egyéb alkalmazások használata tilos.

A rendszergazdának gondoskodnia kell az általa felügyelt elektronikus információs rendszerek rendszerkomponensei sérülékenységeinek figyeléséről.

IV.11.1.1. Microsoft termékek biztonsági frissítéseinek telepítése

A Microsoft termékek biztonsági frissítéseinek a telepítéséről a megjelenésüktől számított 2 héten belül gondoskodni kell. A biztonsági frissítéseket a rendszergazdának előzetesen tesztelni kell.

IV.11.1.2. Nem Microsoft termékek biztonsági frissítéseinek telepítése

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

IV.11.2. Kártékony kódok elleni védelem

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

A kártékony kódok elleni védekezés során a következőkről kell gondoskodni:

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

b) Hetente egyszer egy teljes körű, ütemezett átvizsgálást kell elvégezni.

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

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

e) A kártékony kód elleni alkalmazások adatbázisát automatikusan frissíteni kell.

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

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

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

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

j) A kártékony kód felfedezésekor teendő intézkedéseket és a jelentési rendszert szabályozni kell. A rendszergazdának értesítenie kell az IBF-et. A további teendőket az IBF határozza meg.

k) Kártékony kód általi fertőzéskor a munkaállomást haladéktalanul le kell választani az Igazgatósági hálózatról és így kell megtenni a szükséges vírusirtást vagy a rendszer újratelepítését.

l) A vírusfertőzésekkel és elhárításukkal kapcsolatban tett intézkedéseket dokumentálni kell.

IV.11.2.1. Vírusriadó

A vírusriadót az IBF javaslatára az Igazgató rendelheti el.

Abban az esetben, ha egyértelműen megállapítható, hogy a tapasztalt jelenségeket vírusfertőzés okozza, és a vírus egy-két gépet fertőzött csak meg, akkor vírusriadót nem szükséges elrendelni. A fertőzött gépeket azonnal le kell kapcsolni a hálózatról, meg kell kísérelni a vírusok kiirtását. Ha ez nem sikerül, akkor vírusriadót kell elrendelni.

Feltétlenül vírusriadót kell elrendelni a következő esetek bármelyikénél:

a) ha a szokásosnál sokkal több vírusincidens történt;

b) a vírusfertőzést magas kockázatúnak értékeli a vírusvédelmi szoftver gyártója;

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

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

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

f) szerver oldali vírusfertőzés esetén.

A vírusriadó idején a vírus mentesítés szakmai felügyeletét az IBF és a rendszergazda közösen látják el.

IV.11.2.2. Teendők vírusfertőzés, vírusriadó esetén

Az IBF feladata a vírus fertőzés kivizsgálásának irányítása, a felelősség megállapítása.

A rendszergazda feladatai:

a) a vírusvédelmi rendszer támogatójának értesítése;

b) a vírus fertőzés következtében szükséges intézkedések koordinálása;

c) a fertőzés tényének és a foganatosított intézkedéseknek a rögzítése;

d) a vírusos számítógép leválasztása a hálózatról;

e) a felhasználók értesítése a vírusról;

f) az e-mail rendszer leállítása, ha email-ben terjedő vírusról van szó;

g) a hálózaton terjedő vírus esetén a külső kapcsolat megszakítása;

h) a vírus adatait tartalmazó vírus tudásbázis letöltése és teljes vírusellenőrzés végrehajtása;

i) a fertőzöttség lehetőségeinek feltérképezése, gondolva a hálózaton, cserélhető adathordozók által, vagy e-mail-en történő fertőzésekre;

j) a kliensek frissítése;

k) manuális vírus ellenőrzés végrehajtása azokon a munkaállomásokon, amelyek megfertőződhettek;

l) amennyiben az az Igazgatóságon kívülre is terjedhetett, értesíteni kell az érintett szervezeteket;

m) a vírus fertőzés okának kivizsgálása a vírusvédelmi szoftver támogatójával közösen.

IV.11.3. Az elektronikus információs rendszer felügyelete

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

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

Automatikus eszközökkel monitorozni kell a tűzfalak, a kiszolgálók, a hálózati aktív eszközök erőforrásait és az azokon futó kritikus szolgáltatásokat.

A fenti feladatok végrehajtása a rendszergazda feladata.

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

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

a) az EIR-ek működőképességét;

b) a vírusdefiníciós állományok naprakészségét;

c) a kártékony kód elleni védelem naplóállományait;

d) az EIR-ek mentésének sikeres lefutását;

e) a monitorozó eszközök riasztásait;

f) a központi tűzfal működőképességét és naplóállományait.

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

Az üzemeltetési eljárások megfelelőségét az információbiztonsági felülvizsgálatok alkalmával az IBF felülvizsgálja, a szükséges módosításokat átvezetik, az Igazgató pedig jóváhagyja.

IV.11.4. Biztonsági riasztások és tájékoztatások

Az Igazgatóságnak az IBF útján folyamatosan figyelemmel kell kísérnie az Eseménykezelő Központ által kiadott riasztásokat, valamint a Hatóság által közzétett értesítéseket.

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

IV.11.5. A kimeneti információ kezelése és megőrzése

A kimeneti információk (pl.: nyomtatás) kezelésével és szétosztásával kapcsolatban az Igazgatóság Iratkezelési Szabályzatával összhangban 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 korlátozódik,

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.

IV.12. NAPLÓZÁSI ELJÁRÁSREND

Az elektronikus információs rendszereknél a következő naplózási eljárásrendet kell kialakítani.

IV.12.1. Naplózható események

Biztosítani kell, hogy az alkalmazott elektronikus információs rendszerek a következő eseményeket naplózni tudják:

a) a felhasználók adminisztrációs tevékenysége:

i. bejelentkezés;

ii. kijelentkezés;

iii. jelszómódosítás.

b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;

c) a rendszergazdák a rendszer bármely rétegébe történő be-és kijelentkezése;

d) a rendszergazdák tevékenysége a rendszer bármely rétegében;

e) a felhasználói jogosultságok módosítása;

f) rendszer események, esetleges hibák;

g) konfigurációs beállítások módosítása.

h) Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóba kell rögzíteni.

Az elektronikus információs rendszerek naplózása kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyeket az adatgazdák igényelnek.

IV.12.2. Naplóbejegyzések tartalma

A naplóbejegyzéseknek a következőket kell tartalmaznia:

a) a rendszerelem azonosítóját,

b) az adatazonosítót (fájl / rekord / mező),

c) az esemény ismertetését / a funkcióazonosítót,

d) a felhasználó azonosítóját,

e) az esemény időpontját,

f) az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát.

IV.12.3. Napló tárkapacitás

A naplók tárkapacitását az adott rendszer fejlesztőjének a bevonásával vagy ajánlásai alapján az előzetes kapacitástervezési folyamat során kell kialakítani.

A napló tárkapacitás figyelését a rendszerek felügyeleti tevékenységébe kell beépíteni.

A naplózást úgy kell beállítani, hogy amennyiben a napló betelik, úgy automatikusan kerüljön archiválásra a napló, ezzel biztosítva a naplóbejegyzések felülírásának megakadályozását/automatikus értesítést küldjön a rendszergazdának és további (naplózandó) tevékenység elvégzését ne engedje a tárkapacitás növeléséig.

IV.12.4. Naplózási hiba kezelése

Az Igazgatóság elektronikus információs rendszereiben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak.

IV.12.5. Időbélyegek

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

Az Igazgatóságnak szinkronizálnia kell az EIR-ek belső rendszer óráit a belső hálózatban kijelölt eszközhöz, a kijelölt eszköznek pedig külső, megbízható időszolgáltatóhoz kell szinkronizálnia.

IV.12.6. Szinkronizálás

Az elektronikus információs rendszerek és az azt kiszolgáló infrastruktúra elemek rendszeróráját megbízható, Stratum 1 szintű, egyazon külső időkiszolgálóhoz kell szinkronizálni.

IV.12.7. A napló információk védelme

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

IV.12.8. A naplóbejegyzések megőrzése

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

IV.12.9. Naplógenerálás

Olyan elektronikus információs rendszereket kell alkalmazni, melyek

a) biztosítják a naplóbejegyzések előállítási lehetőségét a *{IV.12.1. Naplózható események}* pontban meghatározott naplózható eseményekre;

b) lehetővé teszik meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

c) naplóbejegyzéseket állít elő a *{IV.12.1. Naplózható események}* pontban meghatározottak szerinti eseményekre az *{IV.12.2. Naplóbejegyzések tartalma}* pontban meghatározott tartalommal.

IV.13. RENDSZER ÉS KOMMUNIKÁCIÓ VÉDELMI ELJÁRÁSREND

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

IV.13.1. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem

Az Igazgatóság elektronikus információs rendszereit hálózati, infrastruktúra és alkalmazás szinten is fel kell készíteni a szolgáltatás megtagadás alapú támadásokkal szemben.

IV.13.1.1. Hálózati szint

Hálózati szinten a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) A *{IV.13.2. A határok védelme}* pontban leírtak alapján kell a határvédelmet konfigurálni;

b) Különös figyelmet kell fordítani a menedzsment portok kommunikációjának titkosítására, elérhetőségének korlátozására (pl.: IP cím szűrés).

c) Biztosítani kell a hálózati eszközöket alkotó szoftverkomponensek naprakészségét a *{IV.11.1. Hibajavítás}* fejezetben leírtak szerint.

d) Az érintett hálózati eszközöket - a *{IV.6.6. Legszűkebb funkcionalitás}* fejezet előírásaira tekintettel - úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

e) Hálózati szinten az Igazgatóság határvédelmi rendszerében és a központi Wi-Fi kontrollerében be kell kapcsolni a túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelmet.

IV.13.1.2. Infrastruktúra szint

Infrastruktúra szintjén a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) Biztosítani kell az érintett rendszert alkotó szoftverkomponensek naprakészségét a *{IV.11.1. Hibajavítás}* fejezetben leírtak szerint;

b) Az érintett rendszert infrastruktúra szinten - a *{IV.6.6. Legszűkebb funkcionalitás}* fejezet előírásaira tekintettel - úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve;

c) Az érintett rendszer kártékony kód elleni védelmét a *{IV.11.2. Kártékony kódok elleni védelem}* fejezetben leírtak szerint kell megvalósítani.

IV.13.1.3. Alkalmazás szint

Alkalmazás szinten a következőket kell végrehajtani a túlterhelés elleni védelem megvalósítása érdekében:

a) Biztosítani kell alkalmazás szinten az érintett rendszert alkotó szoftverkomponensek naprakészségét a *{IV.11.1. Hibajavítás}* fejezetben leírtak szerint.

b) Az érintett rendszert alkalmazás szinten - a *{IV.6.6. Legszűkebb funkcionalitás}* fejezet előírásaira tekintettel - úgy kell konfigurálni, hogy csak a minimálisan szükséges portok, protokollok és szolgáltatások legyenek engedélyezve.

c) Alkalmazás szinten különböző csillapítási technikákat kell alkalmazni (pl.: Captcha kód, meghatározott küszöbszámok elérésre után forrás IP cím korlátozása stb.) a felhasználó felületeket érő szolgáltatás megtagadás alapú támadások, illetve viharszerű lekérdezések elleni védekezésül.

d) A bemeneti információ ellenőrzésének megvalósítása a *{Open Web Application Security Project Application Security Verification Standard (ASVS) aktuális verziója}-ban* leírtak alapján.

IV.13.2. A határok védelme

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

a) **Minden tilos, ami kifejezetten nincs megengedve!** Ez azt jelenti, hogy alaphelyzetben minden forgalmat tiltani kell, majd csak azt megengedni, amelyre valóban szükség van.

b) A belső hálózat irányából az internet irányába kapcsolatot csak azokra a protokollokra/szolgáltatásokra engedélyezünk, amelyre szükség van.

c) Kifejezetten tiltani kell a belső hálózat irányából az internet irányába a levelezési (SMTP) kapcsolatokat. Levelet továbbítani csak a levelező szerveren keresztül szabad.

d) Megfelelő interfészt kell alkalmazni az Igazgatóság és más szervezet tulajdonában lévő, vagy nyilvános hálózat között;

e) Ellenőrizni kell a felhasználók információszolgáltatáshoz való hozzáférését.

f) Az Igazgatóság belső hálózatáról Internet kapcsolat kizárólag jóváhagyott tűzfalakon keresztül létesíthető.

g) Biztosítani kell, hogy az Igazgatóság elektronikus információs rendszerei alapértelmezés szerint ne legyenek elérhetők az Internet felől. Amelyeknél az Internet felöli hozzáférés szükséges igény, ott kizárólag biztonságos és ellenőrzött kapcsolaton keresztül történhet hozzáférés.

h) Minden Internet elérést naplózni kell, annak érdekében, hogy kellő mennyiségű információt lehessen összegyűjteni a szabálytalan internetes tevékenységek detektálása és kiderítése érdekében.

i) Figyelni kell és 1 héten belül telepíteni kell a tűzfal operációs rendszere/firmware-e biztonsági frissítéseit.

j) A tűzfalat úgy kell konfigurálni, hogy az akadályozza és naplózza a port letapogatási próbálkozásokat.

A felhasználóknak tilos az Internet felhasználási szabályait és biztonsági beállításait megváltoztatni, illetve megkerülni.

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

Az IBF köteles ellenőrizni, hogy a felhasználók számára biztosított az Internet elérést lehetővé tevő szoftverek mentesek a komolyabb biztonsági hibáktól.

Az Igazgatóság központi tűzfalát csak a belső hálózatból vagy a konzolról lehet adminisztrálni. A külső hozzáférés nem engedélyezett.

A fentiek végrehajtása érdekében tűzfal biztonsági politikát kell készíteni, mely tartalmazza

a) a tűzfal kialakítására vonatkozó követelményeket,

b) a tűzfalon engedélyezett portokat, protokollokat és szolgáltatásokat,

c) a tűzfal adminisztrálásával kapcsolatos feladatokat és felelősségi köröket

d) a tűzfal biztonsági politikában foglaltak ellenőrzését.

IV.13.2.1. A hálózati szolgáltatások belső használatának szabályozása

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

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

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

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

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

Az Igazgatóság elektronikus információs rendszerében TILOS modemet csatlakoztatni.

IV.13.2.2. Hálózat szegmentálás

Az Igazgatóság hálózatában az infokommunikációs szolgáltatásokat, felhasználókat és elektronikus információs rendszereket szegmentálni kell. A külső felhasználók Internet irányából csak a szükséges elektronikus információs rendszereket érhetik el. A belső hálózatot tűzfal válassza el a többi zónától.

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

IV.13.2.3. A hálózati összeköttetések ellenőrzése

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

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

IV.13.2.4. A hálózati üzenettovábbítás ellenőrzése

A hálózati üzenettovábbítás ellenőrzését a tűzfalaknak, illetve kapcsolódó tartalomszűrő és címfordító megoldásoknak, valamint azok naplóinak kell biztosítaniuk.

IV.13.2.5. Nyilvános elektronikus információs rendszerek védelme

Az Igazgatóság honlapját web hosting szolgáltató működteti, ezért a vele kötött szerződésben elő kell írni a nyilvánosan elérhető tartalmakkal és rendszerekkel kapcsolatos információbiztonsági követelményeket.

IV.13.3. Kriptográfiai kulcs előállítása és kezelése

A kriptográfiai kulcsok védelmének módját a kriptográfiai eszközök biztonságos használatát garantáló szabályozásban kell kidolgozni, az adott elektronikus információs rendszer használatba vételét megelőzően.

A vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kulcsgondozó rendszerek használhatók. A belső előírásokat kriptográfiai utasításban, illetve a megfelelő alkalmazás leírásaiban kell meghatározni.

IV.13.4. Kriptográfiai védelem

Az Igazgatóságnak az elektronikus információs rendszereiben az adatok sértetlenségének és bizalmasságának védelmére a vonatkozó mértékadó dokumentumokban biztonságosnak minősített kriptográfiai műveleteket kell alkalmaznia.

Az Igazgatóságnál a következő kriptográfiai megoldások engedélyezettek:

a) Szimmetrikus kulcsú titkosítás esetén: AES 128, 192, 256,

b) Aszimmetrikus kulcsú titkosítás: RSA 2048 bit,

c) elektronikus aláírás: RSA: 2048 bit vagy ECDSA (pLEN 256 bit),

d) Kulcscsere: Diffie-Helmann 2048 bit,

e) Lenyomatolás: SHA1, SHA2, SHA3 (minimum 256 bit)

f) Jelszótárolás: PBKDF2, scrypt, bcrypt.

IV.13.4.1. A kriptográfiai óvintézkedések használatának szabályzata

Az Igazgatóság elektronikus információs rendszereiben a kriptográfiai eszközök bevezetése esetén ki kell dolgozni az eszközök biztonságos használatát garantáló szabályozást, melynek a következőket kell tartalmaznia:

a) az eszközök védelmét biztosító előírások;

b) az eszközök felhasználására vonatkozó követelmények;

c) a kulcsok generálására, elosztására, tárolására és megsemmisítésére vonatkozó szabályok;

d) a rejtjelzett adatok visszaállításának szabályai és eljárásai azokra az esetekre, amikor a kulcs megsérült vagy elveszett.

IV.13.4.2. Kriptográfiai megoldások alkalmazásának feltételei

Az Igazgatóság elektronikus információs rendszereiben csak olyan kriptográfiai megoldások alkalmazhatók, amelyek:

a) a vonatkozó szabványoknak vagy szabványként elfogadott előírásoknak megfelelő kriptográfiai algoritmusokat és protokollokat használnak;

b) az implementációt külső független szakértő auditálta;

c) alkalmazását az IBF jóváhagyta.

IV.13.5. Együttműködésen alapuló számítástechnikai eszközök

Az Igazgatóság elektronikus információs rendszereiben együttműködésen alapuló számítástechnikai eszközt (pl.: kamera, mikrofon) csak akkor lehet aktiválni/használni, ha azt a felhasználó előzőleg jóváhagyta.

IV.13.6. A folyamatok elkülönítése

Az Igazgatóság elektronikus információs rendszereiben csak olyan modern, gyártó által támogatott operációs rendszerek használhatóak, amelyek biztosítják az elkülönített végrehajtási tartomány fenntartását minden végrehajtó folyamat számára.

V. Mellékletek

1. számú melléklet – Értelmező Rendelkezések

2. számú melléklet – Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása

3. számú melléklet – Biztonsági események jelentése

4. számú melléklet – Kockázatelemzési és kezelési módszertan

5. számú melléklet – Jogosultságigénylési űrlap

6. számú melléklet – Hozzáférések nyilvántartása űrlap

7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend

8. számú melléklet – Felhasználói Nyilatkozat

9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

10. számú melléklet – Titoktartási Nyilatkozat

11. számú melléklet – Titoktartási Nyilatkozat Iratok nem kormányzati e-mail címre történő kiküldésének igénylése űrlap

1. számú melléklet – Értelmező Rendelkezések

Az IBSZ-ben használt, és a gyakorlatban alkalmazott, az információbiztonság tárgykörébe tartozó kifejezések, meghatározások megfelelnek az Ibtv. és az MSZ ISO/IEC 27001:2014 szabvány és jelen IBSZ 4.1 fejezetében meghatározott jogszabályok által használt kifejezéseknek, és értelmezésük is azonos ezekkel.

(1) Adat: Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

(2) Adatállomány: Valamely elektronikus információs rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

(3) Adatbiztonság: Az adatok jogosulatlan megismerése és kezelése (másolás, módosítás, törlés stb.) elleni szervezési és adminisztratív intézkedések, fizikai védelmi eszközök, műszaki és logikai megoldások összehangolt rendszere.

(4) Adatgazda: Felelős azért, hogy az adott adat teljes életciklusa folyamán az adat megvédéséhez a megfelelő biztonság teljesüljön. Az adatgazda joga és kötelessége, hogy a dolgozók részére meghatározza a munkájuk elvégzéséhez minimálisan szükséges hozzáférés szintjét az adatokhoz.

(5) Alapszintű védelem: Egy elektronikus információs rendszer vagy szervezet számára létrehozott minimális védelem.

(6) Auditálás: Az elektronikus információs rendszer biztonsági mechanizmusainak, a számítógépes tevékenységeknek független szakértők által történő átvizsgálása IT biztonsági szempontból, továbbá a rendszer-ellenőrzések megfelelőségének vizsgálata, a kialakított biztonsági stratégia és a működtetési eljárások megfelelőségének megállapítása céljából.

(7) Azonosítás és hitelesítés: Az adott elektronikus információs rendszer biztonsági mechanizmusok segítségével azonosítja és hitelesíti a hozzá fordulókat, mielőtt valamelyik szolgáltatást biztosítaná. Azonosításra és hitelesítésre három dolog alkalmas: amit az egyed ismer (pl. jelszó, PIN-kód), amit az egyed birtokol (pl. intelligens kártya) és ami az egyed sajátossága (pl. biometrikus jellemzők).

(8) Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

(9) Biztonsági audit napló: A biztonsági auditáláshoz gyűjtött, és esetleg fel is használt adatok.

(10) Biztonsági kockázat: A fenyegetettség mértéke, amely megmutatja, hogy valamely fenyegetés milyen mértékű kárt okozhat, ha kihasználja az elektronikus információs rendszer sebezhetőségét.

(11) Biztonsági mechanizmus: Eljárási módszer, eszköz vagy megoldási elv, ami azt a célt szolgálja, hogy egy vagy több biztonsági követelmény teljesüljön.

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

(13) Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bi-

zalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

(14) Elégséges-védelem: A védelem akkor kielégítő erősségű (mértékű), ha a védelemre akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a releváns fenyegetésekből eredő kockázat a szervezet számára még elviselhető szintű vagy annál alacsonyabb.

(15) E-személyi: Olyan hatósági igazolvány, amely a polgár személyazonosságát és a vonatkozó jogszabályban meghatározott adatait közhitelesen igazolja, illetve a polgár törvényben meghatározott esetekben gyakorolhatja vele a külföldre utazás jogát. Az állandó személyazonosító igazolvány emellett – új elemként – alkalmas a polgár elektronikus úton történő közhiteles azonosítására, valamint a vonatkozó jogszabályokban meghatározott kivételekkel – a polgár kérelmére – elektronikus aláírás létrehozására.

(16) Felelősségre vonhatóság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatba kerülő emberek (felhasználók, operátorok, üzemeltetők, külső munkatársak stb.) a biztonsággal kapcsolatos tevékenységükért utólag felelősségre vonhatók.

(17) Felhő-alapú tárhely-szolgáltatás: A szolgáltatásokat nem egy dedikált hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, a szolgáltatás üzemeltetési részleteit a felhasználótól elrejtve. Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy az interneten.

(18) Fenyegetés: Egy fenyegető tényező lehetősége arra, hogy véletlenül vagy szándékosan kiváltson, kihasználjon egy adott sebezhetőséget. Ez gyakorlatilag egy elektronikus információs rendszeren, vagy tevékenységen belüli bármilyen szoftver, információ, hardver, adminisztratív, fizikai, kommunikációs, vagy személyzeti erőforrás megsértésének vagy elvesztésének a lehetőségét jelenti.

(19) Fenyegetettség elemzés: Az a folyamat, amely felsorolja, jellemzi a vizsgált folyamatok és erőforrások fenyegetettségét (azaz a releváns fenyegetéseket, megvalósíthatóságuk nehézségét)

(20) Fenyegető tényező: Olyan körülmény vagy esemény, amely az adat, illetve információ valamely elektronikus információs rendszerben történő feldolgozásának rendelkezésre állását, sértetlenségét, bizalmasságát vagy hitelességét illetve az elektronikus információs rendszernek és az elektronikus információs rendszer elemeinek működőképességét fenyegetheti. A fenyegető tényezők közé soroljuk nemcsak a személyektől eredő támadásokat, amelyek valamely elektronikus információs rendszer ellen irányulnak, hanem valamennyi szélesebb értelemben vett fenyegetést, mint például véletlen eseményeket, külső tényezők általi behatásokat és olyan körülményeket, amelyek általában magának az informatikának a sajátosságaiból adódnak (pl. tűz, áramkimaradás, adatbeviteli hibák, hibás kezelés, hardver tönkremenetele, kártékony kódok, alkalmazáshibák).

(21) Folytonos védelem: Folytonos a védelem, ha az az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.

(22) Helyreállítás: Egy szolgáltatás akkor tekinthető helyreállítottnak, ha a felhasználó újra képes az adott szolgáltatást igénybe venni, azaz az elektronikus információs rendszer és a rendelkezésre álló adatok visszaállítása megtörtént, a szükséges teszteket elvégezték, a felhasználót minderről tájékoztatták.

(23) Hitelesség: A hitelesség az adat olyan biztonsági jellemzője, amely arra vonatkozik, hogy az adat (bizonyíthatóan) egy elvárt forrásból származik. Ehhez szükséges, hogy az informatikai kapcsolatban lévő partnerek kölcsönösen (és egyértelműen) felismerjék egymást, és ez az állapot a kapcsolat teljes ideje alatt fennálljon.

(24) Információs vagyonelemek: Az információs vagyonelemek közé az elektronikus információs rendszer különböző jellegű összetevői tartoznak, például: fizikai infrastruktúra, számítástechnikai eszközök, alkalmazások, adatbázisok és adatállományok, archivált adatok, rendszerdokumentáció, használói és kezelői kézikönyvek, oktatási anyagok, üzemviteli, üzemeltetési és támogató eljárások, tartalékolási elrendezések stb.

(25) Információbiztonság: az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

(26) Kockázat áthárítása: A kockázat kezelés olyan módja, amelynél a kockázatokat (káros hatásokat) megosztjuk egy másik (külső) szervezettel.[2]

(27) Kockázat becslés: Olyan folyamat, amely a releváns fenyegetések szintjét és hatását értékkel jellemzi és megállapítja a fenyegetések szintje, hatásuk, illetve a védelmi igények[3] alapján a kockázatok szintjét.

(28) Kockázat elkerülése: A kockázat kezelés olyan módja, amelynél a felelős vezető úgy dönt, hogy a kockázatos helyzetet eredményező tevékenységet a szervezet nem folytatja tovább.

(29) Kockázat ellenőrzés: Kockázat menedzsment során hozott döntéseket megvalósító tevékenységek tartoznak a kockázat ellenőrzés körébe. Ilyen lehet a kockázatok felülvizsgálata, rendszeres ellenőrzése, illetve a kockázat menedzsment elvárásoknak való megfelelés fenntartása.

(30) Kockázat felmérés: A kockázat elemzést és kockázat kiértékelést átfogó folyamat.

(31) Kockázat felmérési beszámoló: A kockázat felmérés eredmény termékének (dokumentumának) neve, amely a kockázatok ismertetésére szolgál.

(32) Kockázat ismertetés: A döntéshozók és az érintett felek közötti, kockázatokról szóló információ csere vagy tájékoztatás.

(33) Kockázat kezelési terv: A kockázat kezelés eredmény termékének (dokumentumának) neve, amely a kockázat kezelést biztosító intézkedéseket ismerteti[4].

(34) Kockázat kiértékelés: Folyamat, amely során a megbecsült kockázatok összevetésre kerülhetnek a tolerálható szinttel.[5]

---

[2] Törvényi előírások és jogszabályok megtilthatják a kockázat áthárítását. A kockázat áthárítására jó példa a biztosításkötés. Fenyegetett adatok, folyamatok átadása nem kockázat áthárítás (hanem elkerülés).

[3] Olyan súlyozó szempont, amely az érintett felek szemszögéből az érintett adatok és folyamatok érzékenységét, sérülésének közvetlen vagy közvetett kárát fejezi ki.

[4] Tartalmazhatja a kockázat kezelés módját és kiválasztásának indoklását; tevékenységek prioritási rendjét; erőforrás és költségbecslést; mérföldkövek és ütemezés kijelölését; a megvalósítás és ellenőrzés felelőseinek, illetve időpontjainak kijelölését stb..

[5] A kockázatok elviselhetőségének mérlegelését jelenti, melyben segítséget nyújt a jelen dokumentum kockázat kiértékelési fejezetében ismertetett un. tolerancia mátrix.

(35) Kockázat megtartás: A kockázat kezelés olyan módja, amelynél a lehetséges káros hatásokat (tehát a kockázatokat) a szervezet elfogadja bekövetkezésük esetén.[6]

(36) Kockázat optimalizálása: A kockázat kezelés olyan módja, amelynél a kockázatokat csökkentjük a fenyegetések szintjének és / vagy lehetséges hatásuk csökkentésével, amíg az elfogadható szintre nem csökken.

(37) Kockázatcsökkentés: intézkedések, amelyeket egy kockázattal kapcsolatos valószínűség vagy a negatív következmények (vagy mindkettő) enyhítésére hoztak

(38) Kockázatkezelés: Azoknak a biztonsági kockázatoknak az elfogadható költségen történő minimalizálása vagy megszüntetése, amelyek hatással lehetnek elektronikus információs rendszerekre.

(39) Kockázattal arányos védelem: A kockázatokkal arányos a védelem, ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

(40) Kriptográfia: az információ titkos, az illetéktelen hozzáféréssel szemben biztonságos feldolgozásának és továbbításának elmélete és gyakorlata.

(41) Letagadhatatlanság: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy az elektronikus információs rendszerrel kapcsolatos tevékenységek letagadhatatlanok. Ezt a funkciót titkosítási (rejtjelezési) és digitális aláírási technikákra alapozzák.

(42) Maradványkockázat: Az a kockázat, ami a kockázatcsökkentés után megmarad.

(43) Megkerülhetetlenség: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy a védelmet nem lehet kijátszani, azaz az elektronikus információs rendszer egyetlen eleme sem hagyható ki vagy nem kerülhető meg az elektronikus információs rendszer.

(44) Rendelkezésre állás: Az elektronikus információs rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszerelem a szükséges időben és időtartamra használható.

(45) Sértetlenség fenntartása: Biztosítják, hogy az adatot, információt vagy alkalmazás csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak, illetve nem semmisíthetők meg.

(46) Sértetlenség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

(47) Sérülékenység, sebezhetőség: Egy információs vagyon, vagy vagyon csoport gyengesége, hibája vagy hiányossága, amellyel egy fenyegetés vissza tud élni.

(48) Szoftver-vagyontárgyak: A szoftver-vagyontárgyak közé tartoznak: alkalmazási szoftverek, rendszerszoftverek, fejlesztési segédprogramok stb.

(49) Teljes körű védelem: Teljes körű a védelem, ha az az elektronikus információs rendszer összes elemére kiterjed.

(50) Változás-felügyelet: Eljárások, amelyek biztosítják, hogy minden változtatás ellenőrzött legyen, beleértve annak kérelmezését, rögzítését, elemzését, a vonatkozó döntés meghozását, jóváhagyását, kivitelezését és a változtatás megvalósítás utáni áttekintését is.

(51) Zárt felhasználói kör: Az elektronikus információs rendszer biztonsági mechanizmusai mindenkit kizárnak az elektronikus információs rendszer adott szolgáltatásából, kivéve azokat, akik számára az kifejezetten engedélyezett.

[6] A kockázatok kiértékelése során felhasznált szempont rendszer ebben segítséget nyújthat.

(52) Zárt szolgáltatási kör: Az elektronikus információs rendszer biztonsági mechanizmusai biztosítják, hogy minden informatikai szolgáltatás tilos az adott elektronikus információs rendszerben, kivéve az, ami kifejezetten engedélyezett.

(53) Zárt védelem: Zárt a védelem, ha az az összes releváns fenyegetést figyelembe veszi.

2. számú melléklet – Az Igazgatóság elektronikus információs rendszereinek biztonsági osztályba sorolása

Az Igazgatóság elektronikus információs rendszereinek nyilvántartása és biztonsági osztályba sorolása

Alkalmazás megnevezése	Alkalmazás leírása	Adatgazda	Rendszerben kezelt adatok	Biztonsági osztályba sorolás		
				Bizalmas-ság	Sértetlenség	Rendelkezésre állás
Teamup	csoport naptár	Teamup	naptáradatok, időbeosztások	2	2	2
HotelSystem	vendéglátói informatika	BNPI	foglalások, számlázás, szobák	2	2	2
Kulcs-ügyvitel	készletnyilvántartás	BNPI	készletek	2	2	2
ESZIR	erdészeti szakigazgatási információs rendszer	Erdészet	erdészeti adatok	2	2	2
Coriolis iktató	iktatórendszer	BNPI	iktatási adatok, személyes adatok	3	3	3
VIR – könyvtár-nyilvántartó	könyvtár-nyilvántartó	BNPI	könyvek adatai, kölcsönzési adatok	1	1	1
ForrasKVK	pénzügyi program	BNPI	MNV Zrt. tulajdonosi joggyakorlásához tartozó adatok	2	2	2
Forras.Net	ügyviteli rendszer	BNPI	pénzügyi adatok, kötelezettség vállalások, készlet, tárgyi eszköz	3	3	3

Alkalmazás megnevezése	Alkalmazás leírása	Adatgazda	Rendszerben kezelt adatok	Biztonsági osztályba sorolás		
				Bizalmas-ság	Sértetlenség	Rendelkezésre állás
MAK-Elektra	pénzforgalmi megbízások kezelése	Magyar Államkincstár	számlaadatok, megbízások	3	3	3
Revolution	vállalatirányítási rendszer	BNPI	készlet adatok	1	1	1
EIR	erdészeti információs rendszer	BNPI	erdészeti adatok	2	2	2
OKIR	országos környezetvédelmi információs rendszer	Minisztérium	természetvédelmi adatok, szerződések	2	2	2
TIR	természetvédelmi információs rendszer	BNPI	természetvédelmi adatok, szerződések	2	2	2
Kira	központosított illetményszámfejtés	Magyar Államkincstár	személyi adatok, személyi juttatások	3	3	3
Kér	az egységes kormányzati ügyiratkezelő rendszer érkeztető rendszere	NISZ	postai úton érkező küldemények	2	2	2
KGR-K11	költségvetési gazdálkodási rendszer	Magyar Államkincstár	éves pénzügyi beszámoló, elemi költségvetés, költségvetési jelentés, mérlegjelentés,várható bevételek-kiadások	2	2	2
ÁNYR	álláshely nyilvántartó rendszer	Kormányiroda	álláshely adatok	2	2	2

Alkalmazás megnevezése	Alkalmazás leírása	Adatgazda	Rendszerben kezelt adatok	Biztonsági osztályba sorolás		
				Bizalmas-ság	Sértetlenség	Rendelkezésre állás
TÉR	teljesítmény értékelő rendszer	Belügyminiszté-rium	teljesítmény értékelés adatai	2	2	2
Infosys	ügyviteli rendszer	BNPI	2013 előtti pénzügyi adatok, kö-telezettség vállalások, készlet, tárgyi eszköz	3	3	3
bnpi.hu	holnap	BNPI	kötelezően közzéteendő adatok, közérdekű információk	2	2	2
Email	Elektronikus levelezés	BNPI	ügyviteli adatok	2	2	2

3. számú melléklet – Biztonsági események jelentése

A biztonsági esemény megnevezése:

A tapasztalás helye és időpontja:

Az érintett személyek megnevezése:

Az esemény pontos leírása:

Az észlelő neve:

Dátum:_____év___hó___nap …… ……

Észlelő aláírása IBF aláírása

Az esemény kivizsgálásának leírása:

Tett intézkedés leírása:

Az intézkedés életbelépésének időpontja:

Végleges-e az intézkedés:

☐	*Igen*
☐	*Nem*

Igényel-e kockázatelemzést az esemény:

☐	*Igen*
☐	*Nem*

Dátum:_____év___hó___nap …… ……

Információbiztonsági felelős aláírása Igazgató aláírása

4. számú melléklet – Kockázatelemzési és kezelési módszertan

Kockázatelemzési és kezelési módszertan

A jelen dokumentum célja, hogy a jelen IBSZ *{II.6.4. Kockázatelemzés}* fejezetében foglalt követelmények végrehajtásának módját leírja.

A kockázatelemzési módszertan a Közigazgatási Informatikai Bizottság 25. (25/1-3. IBIV) számú ajánlásán alapul.

Vagyonleltár

Az elektronikus információs rendszerekre ható fenyegetettségek különbözőek, attól függően, hogy az elektronikus információs rendszer melyik összetevőjét fenyegetik.

A fenyegetettségek megfelelő azonosítása érdekében létre kell hozni és értelemszerűen fel kell tölteni a következő vagyonelem csoportokat az Igazgatóság vagyonelemeivel:

a) Környezeti infrastruktúra
b) Hardver
c) Szoftver
d) Adatok
e) Dokumentumok
f) Humán erőforrások

Helyzetfelmérés

Az információbiztonsági kockázatelemzés elvégzéséhez fel kell mérni, meg kell ismerni az elektronikus információs rendszereket és azok környezetét, valamint azok jelenlegi információbiztonsági szintjét.

A következő területeket kell a dokumentációk bekérésével, illetve szakmai interjúk lefolytatásával megismerni:

a) Adminisztratív védelmi intézkedések
    i. Az Igazgatóságra vonatkozó jogszabályok, szabályzatok
    ii. Az elektronikus információs rendszerre vonatkozó szabályzatok
    iii. Szerződések, külső felek kezelése
    iv. Alkalmazásfejlesztés, változáskezelés
    v. Jogosultságigénylés
    vi. Biztonsági események kezelése
    vii. Üzemeltetési eljárások
    viii. Szervizelés, eszközcsere, selejtezés
b) Logikai védelmi intézkedések
    i. Mentési megoldások
    ii. Kártékony kód elleni védekezés
    iii. Biztonsági frissítések telepítése
    iv. Hálózat felépítése
    v. Biztonsági rendszerek
    vi. Kriptográfiai megoldások
c) Fizikai biztonság
    i. Beléptetés
    ii. Számítógépterem kialakítása
    iii. Épületben történő közlekedés

iv. Irodák kialakítása, tiszta asztal, üres képernyő politika.

Gyenge pontok meghatározása

A helyzetfelmérés alapján megszerzett információk birtokában meg kell határozni az egyes vagyonelemek gyenge pontjait.

Fenyegetettségek elemzése

Az egyes vagyonelemek gyenge pontjaira bizonyos fenyegetettségek hatnak.

Az informatikai erőforrásokra ható fenyegetettségek vagy fenyegető tényezők (például: üzleti hírszerzés, rosszindulatú hackerek, természeti katasztrófák) mindig a sérülékeny pontokon keresztül fejtik ki hatásukat, így az ellenük való védekezés legfőbb eleme a sérülékenységek azonosítása és megszüntetése.

Az egyes vagyonelemek gyenge pontjait és fenyegetettségeit *{KIB 25. számú ajánlása: 25/1-3. kötet: Az Információbiztonság Irányításának Vizsgálata (IBIV) 1.0 verzió a „gyenge pontok" és a „fenyegetettségek"}* segédletei alapján érdemes azonosítani.

Sérülékenységek elemzése

A sérülékenység egy bizonyos gyenge pont kihasználása a rá ható fenyegetettség által. Meg kell vizsgálni, hogy a beazonosított gyenge pontokon keresztül mely fenyegetettségek tudják kifejteni a káros hatásukat.

Kárérték szintek kialakítása, károk rávetítése a vagyonelemekre

A következő kárérték szintek kerültek meghatározásra:

Kárérték szint	Kár leírása
1	1-es biztonsági osztályba sorolt EIR sérülhet vagy egyéb jelentéktelen kár
2	2-es biztonsági osztályba sorolt rendszer sérül vagy kisebb kár
3	3-as biztonsági osztályba sorolt rendszer sérül vagy közepes kár
4	4-es biztonsági osztályba sorolt rendszer sérül vagy magas kár
5	5-ös biztonsági osztályba sorolt rendszer sérül vagy kiemelkedően magas kár

A kockázatok megállapításához az elektronikus információs rendszerek vagyonelemeire rá kell vetíteni a kárérték szinteket.

A bekövetkezési valószínűségek meghatározása

Következő lépésként meg kell becsülni a sérülékenységek bekövetkezési valószínűségét.
A bekövetkezési valószínűséghez a következő értékeket kell használni:

- „5" - bármikor bekövetkezhet
- „4" - gyakori
- „3" – közepes
- „2" - ritka
- „1" – nagyon ritka

Kockázatok meghatározása

Az információbiztonsági kockázatokat a sérülékenység bekövetkezésének a valószínűsége és az okozott kár szorzata fogja megadni.

A kockázatok minősítéséhez a következő kockázati mátrixot kell definiálni:

		Bekövetkezési valószínűségek				
		1	**2**	**3**	**4**	**5**
Kárértékek	**5**	A	K	M	NM	NM
	4	A	K	M	NM	NM
	3	NA	A	K	M	M
	2	NA	A	A	K	K
	1	NA	NA	NA	A	A

A kockázatok jelölése a következő:

- NA - Nagyon alacsony
- A – Alacsony
- K – Közepes
- M – Magas
- NM - Nagyon magas

Elviselhető kockázatok meghatározása

Az Igazgatóság azt a döntést hozta, hogy minden közepes, illetve közepesnél nagyobb kockázatot kezelni kíván.

Ennek megfelelően a toleranciamátrix a következő:

		Bekövetkezési valószínűségek				
		1	**2**	**3**	**4**	**5**
Kárértékek	**5**	T	NT	NT	NT	NT
	4	T	NT	NT	NT	NT
	3	T	T	NT	NT	NT
	2	T	T	T	NT	NT
	1	T	T	T	T	T

A táblázatban alkalmazott jelölések értelmezése a következő:

- T – Tolerálható
- NT – Nem tolerálható

Kockázatok kezelése

A nem tolerálható kockázatokat kezelni kell. Az Igazgatóság a kockázatokat a következőképpen kezeli:

a) Megfelelő intézkedésekkel csökkenti a fenyegetés bekövetkezési gyakoriságát vagy hatását (Kockázat csökkentés);
b) Tudatosan, a következményeket felmérve elfogadja a kockázatot (Kockázat elfogadás);
c) Elkerüli a kockázatot azáltal, hogy az érintett tevékenységet felfüggeszti (Kockázat elkerülés);

d) Áthárítja a kockázatot például biztosítással, vagy megfelelő beszállítói szerződésekkel. (Kockázat áthárítás).

Kockázatcsökkentő intézkedések

A PreDeCo elv alapján a kockázatcsökkentés három szemszögből közelíthető meg:

a) Megelőző jellegű (preventív kontrollok)

   A hibák, gyengeségek, sérülékenységek, illetve ezek kihasználására való lehetőségek kiküszöbölése.

b) Korlátozó vagy javító (korrektív kontrollok)

   Egy veszély hatását csökkentő, enyhítő óvintézkedések, további tevékenységek szükségessége nélkül.

c) Észlelő és reagáló (detektív kontrollok)

   A sebezhetőségek támadásának észlelése, ártalmas kihatások enyhítésére, illetve válaszreakciók kidolgozása.

Intézkedési terv

Az el nem viselhető kockázatok kezelésére az Igazgatóságnak intézkedési tervet kell készítenie az egyes feladatok mellé rendelt felelős, határidő és esetleg költség feltüntetésével.

Az intézkedései tervet az IBF készíti elő a rendszergazda bevonásával és az Igazgató hagyja jóvá.

5. számú melléklet – Jogosultságigénylési űrlap

Hozzáférési jogok igénylése űrlap

Iktatószám:

JOGOSULTSÁGIGÉNYLŐ ADATAI

Igénylő neve: …….

Szervezeti egység: ……

Telefon: ……

Email: …….....

Igényelt művelet

Elektronikus információs rendszer megnevezése:.....

Jogosultság kezdete: …… Jogosultság vége: ……..

Új jogosultság
Jogosultság törlése
Jogosultság módosítása

Egyéb:……
……
…….

INDOKLÁS

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése:
……
……

……..
Kelt: …… igénylő aláírása

Munkahelyi vezetői jóváhagyás

Vezető: ……..
Beosztása: …….. …..……..
Kelt: …….. vezető aláírása

Adatgazdai jóváhagyás

Adatgazda: …….. …….
Kelt …… adatgazda aláírása

A jogosultságot beállító aláírása

Rendszergazda: …….. …….
Kelt …… rendszergazda aláírása

6. számú melléklet – Hozzáférések nyilvántartása űrlap

Sorszám	Iktatószám	Felhasználó neve	Igényelt jogosultság	Igénylés dátuma	Munkahelyi vezető

7. számú melléklet – Felhasználói Informatikai Biztonsági Házirend

Felhasználói Informatikai Biztonsági Házirend

1. ÁLTALÁNOS RÉSZ

1.1. A Felhasználói Informatikai Biztonsági Házirend célja

A Felhasználói Informatikai Biztonsági Házirend (a továbbiakban: FIBH) célja, hogy a Bükki Nemzeti Park Igazgatóság (továbbiakban: az Igazgatóság) elektronikus információs rendszereinek felhasználói részére előírja az információbiztonsági előírások rájuk vonatkozó részét.

Az Igazgatóság elektronikus információs rendszereinek védelme érdekében az Igazgatóság kidolgozta az Informatikai Biztonsági Szabályzatát.

Az Informatikai Biztonsági Szabályzat (továbbiakban: az IBSZ) tartalmazza valamennyi információbiztonsággal kapcsolatos szabályt, melynek betartásával az érintettek által elvárt szinten tartható az Igazgatóság elektronikus információs rendszereinek és az azokban kezelt adatok biztonsága.

Az IBSZ számos olyan védelmi intézkedést tartalmaz, amely közvetlenül nem kapcsolódik az Igazgatóság felhasználóihoz, ezért a jelen FIBH-nak az is célja, hogy egy kivonatot adjon az IBSZ felhasználókra vonatkozó előírásairól, illetve tovább értelmezze, és érthető módon kommunikálja az IBSZ-ben magasabb szinten meghatározott követelményeket.

1.2. A FIBH általános követelményei

A FIBH előírásainak alkalmazása, betartása, illetve betartatása, a jelen IBSZ *{I.2.1. Szervezeti-személyi hatály}* **pontban megjelöltek számára kötelező. A szabályok be nem tartása jogi, munkaügyi, illetve szerződésben meghatározott következményeket vonhat maga után. A FIBH el nem olvasása vagy nem ismerete nem mentesít a felelősség alól.**

Az információbiztonsági előírások betartása megvédi az Igazgatóságot és a jelen IBSZ *{I.2.1. Szervezeti-személyi hatály}* pontban kifejtett személyi hatály alá eső felhasználóit, ügyfeleit, partnereit, adataik és információik jogosulatlan vagy véletlenszerű nyilvánosságra jutásától, módosításától, megrongálódásától, megsemmisülésétől.

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

Az Igazgatóság elektronikus információs rendszereit csak a jelen IBSZ *{8. számú melléklet – Felhasználói Nyilatkozat}* mellékletében található nyilatkozat aláírása után lehet használatba venni.

Az Igazgatóság a FIBH-t az IBSZ-szel együtt folyamatosan fejleszti és tökéletesíti.

2. BEVEZETÉS

Az Igazgatóság által kezelt információk érzékenysége miatt azok védelme, azaz bizalmas kezelése, sértetlensége, valamint megfelelő szintű rendelkezésre állása kritikus tényező.

Az Igazgatóság elvégezte a jogszabályok által előírt módon az elektronikus információs rendszereinek biztonsági osztályba sorolását, melynek során valamennyi elektronikus információs rendszert besorolta egy 1-5-ig terjedő skálán. Az elektronikus információs rendszer biztonsági osztálya adja meg a védelem elvárt szintjét.

Az Igazgatósági ügyviteli folyamatok működése nagymértékben az elektronikus információs rendszereire épül, így ezek kiesése, vagy megsemmisülése esetén az Igazgatóság egyes funkciói működésképtelenné válhatnak, valamint az Igazgatóság által kezelt érzékeny információk illetéktelen kezekbe kerülhetnek.

Az Igazgatóság elektronikus információs rendszereinek minden felhasználója személyes felelősséggel tartozik a munkájával kapcsolatban a birtokában lévő, illetve a tudomására jutott információk megfelelő kezeléséért, a biztonsági szabályok betartásáért.

3. A FELHASZNÁLÓ JOGAI, KÖTELESSÉGEI ÉS FELELŐSSÉGE

A felhasználóknak az elektronikus információs rendszerek használata során a következők a kötelességeik, jogaik és felelősségeik.

3.1. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre,

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

e) meghibásodás, üzemzavar esetén az elhárítás igénylésére.

3.2. A felhasználó kötelessége

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

Amennyiben a felhasználó olyan adatokhoz fér hozzá, amelyek kezelésében nem illetékes, a hibát jeleznie kell munkahelyi vezetőjének.

Valamennyi alkalmazott köteles azonnal értesíteni a rendszergazdát minden olyan körülményről, ami az informatikához kapcsolódó tevékenység fennakadásához, megszakadásához vezethet. A rendszergazda szükség esetén értesíti az információbiztonsági felelőst, aki megteszi a további, szükséges intézkedéseket.

Valamennyi információbiztonsággal kapcsolatos észrevételt vagy szabályszegésre vonatkozó feltételezést haladéktalanul jelenteni kell az információbiztonsági felelősnek.

Minden felhasználónak bizalmasan kell kezelnie valamennyi felhasználói azonosítót, jelszót, eToken-t, kulcsot, vagy bárminemű egyéb, az Igazgatóság erőforrásaihoz hozzáférést biztosító eszközt.

A személyi azonosító kódokat, jelszavakat szigorúan titokban kell tartani. Még a közeli munkakapcsolatban álló, egymást jól ismerő kollégák sem közölhetik ezeket egymással. A hozzáférési kódok a rendszergazdáknak sem adhatók ki és a rendszergazdáknak nincs is joga ezeket elkérni.

Az információbiztonsági hiányosságok megelőzése céljából a felhasználók kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére, és a tapasztalatokat a további problémák elkerülésében felhasználni.

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

Az Igazgatóság infokommunikációs eszközei és elektronikus információs rendszerei kizárólag hivatali munkavégzés céljából használható, azok magáncélú használata tilos!

Az Igazgatóság a vonatkozó adatvédelmi jogszabályok figyelembevételével jogosult a felhasználó hivatalos elektronikus levelezését és internetforgalmát vizsgálni.

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

Az Igazgatóságnál az alkalmazottak csak az Igazgatóság tulajdonát képező informatikai eszközöket és engedélyezett szoftvereket használhatják. Ettől eltérni csak az Igazgató írásbeli engedélyével lehet.

A rendszergazdát kivéve, tilos az Igazgatóság számítógépeire szoftvereket telepíteni, és azokat futtatni.

Kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

A nyomtatásra, lapolvasásra, fénymásolásra, faxolásra alkalmas készülékek, multifunkcionális eszközök használatánál ügyelni kell arra, hogy:

a) az érzékeny információt tartalmazó nyomtatványok ne maradjanak a készülékben;

b) illetéktelenek ne férhessenek hozzá, mert belső tárolóikban tárolódott üzenetek visszahívhatók, így illetéktelenek kezébe kerülhetnek;

c) véletlen vagy szándékos átprogramozás során az üzenetek egy nem megfelelő számra kerülhetnek;

d) félretárcsázás vagy hibásan tárolt szám miatt az üzenetek illetéktelen személyhez kerülnek.

3.3. A felhasználó felelőssége

A felhasználó felelősséggel tartozik:

a) a szabályok betartásáért;

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

c) a személyére szóló és védett területre belépést biztosító kártyájának/kártyáinak védelméért és át nem ruházásáért;

d) az elektronikus információs rendszerben végzett műveletekért;

e) az Igazgatóság infokommunikációs eszközeinek (számítógép, nyomtató, scanner, stb.) szakszerű kezeléséért;

f) a személyi használatra átvett eszközök megfelelő fizikai védelméért.

3.4. A felhasználó jogai

A felhasználó jogosult:

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

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

c) információbiztonsági képzésre;

d) a működtetéshez szükséges támogatás igénylésére, a munkavégzéshez szükséges általa nem ismert szoftver eszközökhöz támogatást, képzést kérni;

e) meghibásodás, üzemzavar esetén a lehető legrövidebb időn belüli elhárítás igénylésére.

4. AZ INFORMÁCIÓ KEZELÉSÉNEK SZABÁLYAI

4.1. Munkaállomások hozzáférés védelme

A felhasználó munkaállomást csak saját azonosítójával és jelszavával belépve használhat. Harmadik fél csak a munkaállomás nevesített felhasználója vezetőjének előzetes írásbeli engedélyével használhat munkaállomást, ebben az esetben is a személyesen hozzárendelt azonosító használatával. Hibaelhárítás vagy támogatás esetén a rendszergazda saját azonosítójával a felhasználó engedélyével a felhasználó munkaállomására beléphet.

A felhasználónak sem helyi, sem hálózati rendszergazdai jog nem adható!

4.2. A hozzáférés kiosztás folyamata

Az informatikai rendszerekbe belépést lehetővé tevő azonosítót a vezető igényli a felhasználóknak, az IBSZ *{IV.10.3. Hozzáférési jogok igénylésének eljárásrendje}* fejezetében leírt folyamat szerint.

A hálózati belépést lehetővé tevő azonosítót és a kezdeti jelszót a rendszergazda személyesen vagy telefonon adja át az új felhasználónak. Az átadás során a rendszergazda az azonosító használatáról, a kezdeti jelszó megváltoztatásáról és az egyéb testre szabási lépésekről oktatásban részesíti a felhasználót.

4.3. Hálózati hozzáférés, hozzáférés az egyes alkalmazói programokhoz

Az Igazgatóság vezetése felügyeli az elektronikus információs rendszerek használatát a visszaélések megakadályozására és jogosult az elektronikus információs rendszer használatát ellenőrizni.

Az Igazgatóság infokommunikációs eszközein működtetett szoftvereket és alkalmazói rendszereket a felhasználó a számára beállított jogosultságnak megfelelően használhatja az alábbiak szerint:

a) A felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz.

b) Az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) A jelszó legalább nyolc karakter hosszú legyen, és tartalmaznia kell kisbetűkön kívül nagybetűt és számot vagy speciális karaktert is;

b) a jelszavakat 90 naponta meg kell változtatni,

c) az előző jelszavak újra használatát 24 alkalommal kerülni kell.

A felhasználói jelszavak alkalmazásakor az alábbi szabályokat kell betartani:

a) a felhasználó a jelszavát köteles titokban tartani,

b) a jelszószabályok betartása minden felhasználónak jól felfogott érdeke. A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben,

c) a felhasználói jelszót TILOS leírni,

d) ha bármilyen jel mutat arra, hogy a jelszó kompromittálódhatott, azonnal meg kell változtatni és értesíteni kell az információbiztonsági felelőst,

e) a jelszó minél komplexebb, annál kisebb a valószínűsége, hogy nevünkben visszaélést követnek el.

A felhasználói jelszavak képzésénél az alábbi szempontokat kell betartani:

a) könnyen megjegyezhető, és nehezen kitalálható legyen;

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

c) ne legyen a gépnévre vagy a felhasználói névre utaló;

d) ne legyen sorozat.

4.4. Hozzáférés védelem mobil infokommunikációs eszköz esetén

A mobilitás miatt sokkal nagyobb veszélynek kitett mobil infokommunikációs eszközök esetében is jelszót kell használni a rendszerbe történő belépéshez. Bár ez a védelem megnehezíti a hozzáférést, a háttértárolót eltávolítva az ott nyíltan tárolt adatok így is megszerezhetők. Ezek miatt az Igazgatóság titkosítja a mobil infokommunikációs eszközeinek háttértárolóit.

A fentiek miatt fokozottan kell törekedni ezen eszközök fizikai védelmére is az elvesztés, illetve ellopás ellen.

Külső munkahelyen történő feladat elvégzése után a keletkezett adatokat a hálózati meghajtóra kell menteni.

A mobil infokommunikációs eszközökről a feleslegessé vált adatokat le kell törölni.

Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát, az eszközhöz illetéktelenek ne férhessenek hozzá.

Mobil infokommunikációs eszközök esetén rendszergazda jog felhasználónak nem adható.

4.5. Adatmentések, az adathordozók nyilvántartása és tárolása

Az adatokat nem a helyi munkaállomáson, hanem a „központi fájlszerver” megfelelő könyvtáraiban kell tárolni, ahol biztosított azok rendszeres mentése és biztonságos tárolása. Minden

felhasználó számára rendelkezésre áll a „Saját” könyvtár a saját adatok tárolására, illetve minden iroda rendelkezik külön könyvtárral a szervezeti egységen belül keletkező és közösen kezelendő adatok tárolására. A nem megfelelő könyvtárba mentés a felhasználó felelőssége.

Az Igazgatóság nem vállal felelősséget a helyi gépen tárolt adatokért.

A rendszergazda a „központi fájlszerver”-en tárolt ügyviteli adatokról meghatározott módon és gyakorisággal mentést készít. Ebből adódóan lehetőség van az állományok, adattáblák statikus visszaállítására a mentés időpontjának megfelelő tartalommal. Folyamatok előre-, illetve visszagörgetésére a rendszer nincs felkészítve. Speciális mentési igényekről a rendszergazdát írásban értesíteni kell, és egyeztetni kell a kivitelezés lehetőségéről.

Az adat visszaállítást az adatgazda írásbeli (e-mail) igénye alapján a rendszergazda végzi el.

A feljegyzésnek tartalmaznia kell a visszaállítani kívánt adat:

a) utoljára ismert pontos helyét;

b) megnevezését, és a

c) visszaállítandó időpontot.

A felhasználónak a jogviszonyának megszűnésekor a munkaállomásán, a központi tárhelyen, valamint az elektronikus információs rendszerekben kezelt és tárolt adatok törlése tilos!

4.6. Adathordozók kezelése

Az eszközhasználatot, az Igazgatóság elektronikus információs rendszereihez történő csatlakoztatása után, az Igazgatóság minden előzetes értesítés nélkül figyelheti, monitorozhatja.

Az Igazgatóság informatikai infrastruktúrájából kivitt adatok biztonságát ebben az esetben is biztosítani kell a következő védelmi intézkedésekkel:

a) Otthoni számítógép esetén gondoskodni kell az operációs rendszer és az egyéb irodai alkalmazások naprakészségéről;

b) Az operációs rendszerbe épített helyi tűzfalat be kell kapcsolni;

c) Kémprogram elleni védekezéssel ellátott, naprakész vírusvédelemmel kell rendelkezni.

d) A napi munkavégzéshez használt felhasználói azonosítónak rendszergazda jog nem adható.

Az Igazgatóság az informatikai rendszerében használt adathordozókat információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

5. FELHASZNÁLÓK SZÁMÍTÓGÉPES KÖRNYEZETE

5.1. Számítógépek és a hálózat kezelési előírásai

A felhasználó felelős az infokommunikációs eszközön általa végzett, nyilvánvalóan szakszerűtlen beavatkozásának következményeiért.

A felhasználó semmilyen infokommunikációs eszközt nem telepíthet az Igazgatóság elektronikus információs rendszerébe.

Az Igazgatóság által biztosított infokommunikációs eszközök elhelyezését, telepítési módját nem változtathatja meg, azok borítását nem bonthatja meg, a konfigurációját nem

módosíthatja. Az Igazgatóság által biztosított infokommunikációs eszközökre szoftvert (ideértve a csak másolással telepíthető szoftvereket is) nem telepíthet, nem törölhet, és nem módosíthat.

A felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie. Az igénylést a munkahelyi vezetővel egyeztetve az Igazgató hagyja jóvá.

A rendszergazda bizonyos szoftver elemek telepítését központi szétosztással, automatikusan végzi. Az ilyen távolról történő frissítéskor meg kell várni a frissítés befejeződését, a folyamatot leállítani tilos. El kell fogadni, hogy ez alatt az idő alatt a számítógép valamivel lassabban működik.

Az Igazgatóság belső hálózatához idegen infokommunikációs eszköz nem csatlakoztatható.

5.2. Internethasználat, web böngészés

Az Internet és a web böngészés használatának főbb szabályai:

Az Internethez való kapcsolódás csak és kizárólag a munkavégzést szolgálja!

A felhasználók kizárólag jóváhagyott szoftvereket használhatnak az Internet elérésére.

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

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

Tilos az IBF engedélye nélkül külső féllel nem web alapú hálózati kapcsolat kialakítása (pl.: FTP).

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

Tilos nem a munkavégzést szolgáló közösségi oldalak látogatása.

Tilos az Igazgatósággal kapcsolatos információk nyilvános internetes oldalakon való illegális közzététele.

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

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

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

5.3. E-mail használat

Az Igazgatóság által biztosított elektronikus levél cím és az elektronikus levelezési szolgáltatás kizárólag hivatali munkavégzés céljára biztosított, ezért a felhasználóknak tilos az Igazgatósági e-mail címüket nem hivatali minőségben használni (pl.: regisztráció letöltési weboldalakra, on-line játék oldalakra, közösségi oldalakra, az Interneten elérhető nyilvános chat-és fórum oldalakon hivatali email címmel hozzászólni stb.)!

Az Igazgatóság által nem támogatott levelezőrendszer (pl.: Gmail, Freemail) használata munkavégzésre nem engedélyezett.

Az Igazgatóság elektronikus hivatalos kommunikációja elsősorban kormányzati e-mail címek igénybe vétele útján folyhat.

Kormányzati e-mail címnek kell tekinteni:

a) a gov.hu végződésű e-mail címeket,

b) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv által biztosított hivatalos elektronikus levelezési címeket,

c) a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket,

d) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv vagy a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alatt álló gazdasági társaság tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket, valamint

e) a Kormány irányítása vagy felügyelete alá nem tartozó, Alaptörvényben meghatározott szerv hivatalos elektronikus levelezési címeit.

A meghatározott iratok kizárólag kormányzati e-mail címre küldhetők ki.

Kizárólag kormányzati e-mail címre küldhetők ki az alábbi iratok:

a) törvényjavaslatot tartalmazó irat,

b) Kormány részére készült előterjesztés, jelentés,

c) Kormány döntését igénylő előterjesztés,

d) politikai felsővezetői (miniszterelnök, miniszter, államtitkár) döntést igénylő előterjesztés, különösen miniszteri rendelettervezet,

e) politikai felsővezető részére készülő előterjesztés, jelentés,

f) politikai vezető (kormánymegbízott) részére készülő előterjesztés, jelentés,

g) biztosi jogviszonyban álló (kormánybiztos, miniszterelnöki biztos, miniszteri biztos) részére készülő előterjesztés, jelentés,

h) szakmai felsővezető (közigazgatási államtitkár, helyettes államtitkár, központi hivatal vezetője és vezetőjének helyettese, kormányhivatal főigazgatója) részére készülő előterjesztés, jelentés

i) szakmai vezető (kormányhivatal igazgatója, járási hivatal, illetve fővárosi kerületi hivatal vezetője és vezetőjének helyettese, főosztályvezető, osztályvezető) részére készülő előterjesztés, jelentés,

j) minden olyan irat, amely a Kormánynak, a Kormány tagjának, politikai felsővezetőnek vagy vezetőnek, szakmai vezetőnek vagy felsővezetőnek, biztosi jogviszonyban állónak a döntését tartalmazza, mely nem kerül nyilvánosan közzétételre,

k) a fentiekről készült tervezet, másolat vagy kivonat, a fentiekkel kapcsolatos munkaanyag

Ezen irattípusok nem kormányzati e-mail címre történő kiküldése tilos, kivéve, ha azt az Igazgatóság erre kijelölt vezetője kifejezetten, írásban (ez alatt az elektronikus jóváhagyást is érteni kell) engedélyezi.

a) A kizárólag kormányzati e-mail címre küldhető iratoknak nem kormányzati e-mail címre történő továbbításának engedélyezésére kizárólag az erre kijelölt vezető – Dudás György általános igazgatóhelyettes – jogosult, kifejezetten írásban.

b) Amennyiben a fenti irattípusok közé tartozó irat nem-kormányzati e-mail címre történő továbbítására engedély nélkül kerül sor, akkor az minden esetben munkajogi következményekkel jár az intézkedésben részt vevő kollegák irányában.

c) Amennyiben a fentiek szerinti irat nem kormányzati e-mail címre történő megküldése szükséges, akkor az irat továbbítása helyett elsősorban az irat tartalmának kivonatolása útján kell az abban foglaltakat a címzettel közölni. Ennek során lehetőleg kerülni szükséges az utalást arra, hogy a kérdéses tartalom végső soron honnan származik és azt milyen dokumentum tartalmazza, ehelyett elsősorban általános körülírással szükséges utalni a dokumentumban foglaltak keletkeztetőjére.

d) Továbbá haladéktalanul értesíteni kell a Minisztériumot minden esetről, amikor a fentiek szerinti irat nem kormányzati e-mail címre történő továbbítására engedély nélkül került sor (eset leírása, a kiadott irat ismertetése, a címzett e-mail cím megjelölése, az alkalmazott munkáltatói intézkedés bemutatása). Az előbbi tájékoztatókat minden esetben a fentiek szerint kijelölt felelős vezető köteles megküldeni.

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

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

Az Igazgatóság elektronikus levelező rendszeréből elküldött elektronikus levél önmagában nem használható kötelezettség vállalására, illetve annak visszaigazolására, mivel műszakilag - az elektronikus levelezési szolgáltatás működési elvéből fakadóan – a rendszergazdák nem tudnak garanciát vállalni arra, hogy az elektronikus levél

a) eljut a címzetthez,

b) átküldése közben illetéktelenek annak tartalmát el nem olvassák,

c) átküldése közben illetéktelenek annak tartalmát nem módosítják.

Amennyiben a fentiek biztosítására szükség van (pl.: elektronikus ügyintézés), akkor az állam által nyújtott Központi Elektronikus Ügyintézési Szolgáltatásokat kell igénybe venni vagy egyéb kriptográfiai algoritmusokat kell alkalmazni az elküldött elektronikus levelek bizalmasságának és sértetlenségének biztosítása érdekében.

A fentiekhez hasonlóan a rendszergazdák arra sem tudnak garanciát vállalni, hogy egy hivatali címzettnek szóló levél időben és sértetlenül megérkezik a címzetthez, mivel ehhez más, külső szolgáltatók közreműködése is szükséges, illetve az Igazgatóság a tömeges, kéretlen, valamint

kártékony levelek elleni védekezésül spamszűrő rendszert működtet, mely kivételes esetben (fals pozitív) kiszűrhet hasznos levelet is.

Az Igazgatóság elektronikus levelező rendszeréből csak akkor lehet bizalmas, jogszabály által védett adatot, titkot (személyes adatok, különleges adatok, adótitok stb.) elküldeni, hogy ha szabványos, sérülékenységektől mentes kriptográfiai algoritmussal az adat titkosításra került.

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

A felhasználónak tilos a postafiókjában kezelt elektronikus levelek automatikus vagy manuális továbbítása más, külső elektronikus levelező rendszerbe (pl.: a saját magán email címére).

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

Ismeretlen helyről származó e-mail-ek, illetve azok csatolmányainak megnyitásakor és az azokban elhelyezett hivatkozásokra kattintással fokozott óvatossággal kell eljárni, mert maga az email vagy annak csatolmánya, illetve az email-ben elhelyezett hivatkozás kártékony lehet. Ebben az esetben ellenőrizni kell az email feladóját, a tárgyat, a levél szövegezését (magyartalan megfogalmazás), a szükségtelen csatolmányokat és a levélben elhelyezett hivatkozásokat.

6. VÍRUSVÉDELEM

6.1. A vírusvédelem alkalmazásának előírásai

A rendszergazda a számítógépek vírusok elleni védelmére rendszeresen frissített vírusvédelmi rendszert, és anti-spyware programot üzemeltet. Ez a védelem kiterjed a kiszolgálók, munkaállomások valamint a teljes Internet és elektronikus levélforgalom folyamatos ellenőrzésére. Új vírus megjelenése esetén még így is előfordulhat fertőzés, valamint csatolmányok, CD és DVD lemezek, cserélhető adathordozók, illetve internetről letöltött fájlok használata esetében.

Vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.

Dokumentumok esetében lehetőség szerint kerülni kell a makrók megnyitását, külső forrásból érkező dokumentumok esetében pedig nem szabad engedélyezni.

Ha a vírus helye nem lokalizálható, a rendszergazda jogosult a hálózat egyes funkcióit, vagy a teljes hálózat felhasználói szolgáltatásait a vírusveszély elhárításáig felfüggeszteni.

6.2. Teendők vírusgyanú esetén

Vírusgyanú esetén a felhasználó köteles azonnal felhívni a rendszergazdát, aki ellátja utasítással, vagy intézkednek a jelzés továbbításáról az információbiztonsági felelős felé.

7. AZ INFORMATIKAI ESZKÖZÖK FIZIKAI VÉDELME

7.1. Számítógép használatának előírásai

A munkaállomást és a perifériákat a napi munkavégzés befejezésekor ki kell kapcsolni. Ez alól kivételek azok az eszközök, amelyek automatikusan kikapcsolnak (hálózati nyomtatók vagy a modern monitorok többsége stb.). Az infokommunikációs eszközöket üzem közben letakarni, a szellőző nyílásokat eltakarni tilos!

7.2. „Üres asztal - tiszta képernyő" politika

Az „üres asztal - tiszta képernyő" politika megvalósítása az alábbiakat jelenti:

a) A monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);

b) A felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;

c) A munkavégzés befejeztével a munkaállomásból ki kell jelentkezni, illetve ki kell azt kapcsolni;

d) Elfelejtés esetére jelszóvédett, automatikus zárolás kerül beállításra, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;

e) A felhasználóknak az infokommunikációs eszközök elhelyezésére szolgáló helyiséget be kell zárniuk, ha a helyiségben senki nem tartózkodik;

f) A kinyomtatott, faxolt vagy másolt iratokat nem szabad őrizetlenül a nyomtatókban, multifunkcionális eszközökben, fax-okban hagyni.

g) Ügyfelet és más külső felet nem szabad felügyelet nélkül az irodában hagyni.

7.3. Mobil infokommunikációs eszközök védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi védelmi szabályokat kell betartani:

a) mechanikai és használati sérülések elkerülése érdekében követni kell a géphez kapott használati útmutatót;

b) cserélhető kártyák behelyezésénél, és eltávolításánál szintén a használati utasítást kell követni;

c) a mobilitás és a kis méret miatt a mobil infokommunikációs eszközök fokozottan vannak kitéve lopásveszélynek. Gondoljunk erre, és ne hagyjuk őrizetlenül autóban, szállodai szobában stb. (zárjuk el fizikailag, használjuk, ha lehet az értékmegőrzőt, ha nincsenek érzékeny adatok a gépen);

7.3.1. Mobil infokommunikációs eszközök ellopása

A mobil infokommunikációs eszközök ellopása esetén:

a) az ellopás tényét a lehető leggyorsabban jelenteni kell az információbiztonsági felelősnek és a munkahelyi vezetőnek;

b) értesíteni kell a rendőrséget;

c) értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából vagy a szálloda területén álló kocsiból lopták el;

d) valamennyi rendőrségi jelentést meg kell őrizni és az Igazgatóság részére át kell adni.

7.3.2. Infokommunikációs eszköz elvesztése

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

8. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE

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

a) a szolgáltatás, a berendezés vagy az eszközök elvesztése;

b) a rendszer hibás működése vagy túlterhelések (Dos-támadás);

c) emberi hibák;

d) a szabályzatoknak vagy irányelveknek való nem megfelelés;

e) a fizikai biztonsági rendelkezések megsértése;

f) nem ellenőrzött rendszerbeli változások;

g) a szoftver vagy hardver hibás működése;

h) hozzáférési előírások megsértése;

i) kártékony kód általi fertőzés;

j) a nem teljes vagy nem pontos működési adatokból eredő hibák;

k) a bizalmasság és sértetlenség megsértése;

l) az elektronikus információs rendszerrel való visszaélés.

8.1. Jelentés a biztonsági eseményekről

A biztonságot érintő eseményekről a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét és a rendszergazdát. A rendszergazda értesíti az információbiztonsági felelőst, aki jogosult az esemény kivizsgálására.

A biztonságot érintő eseményekről szóló jelentések elkészítésére az IBSZ *{3 számú melléklet – Biztonsági események jelentése}* mellékletét kell használni.

8.2. Jelentés a szoftverzavarokról

Az elektronikus információs rendszerekben tapasztalt szoftverzavarokat jelenteni kell a rendszergazdának. Szoftverzavarra utaló jelek lehetnek, amikor az alkalmazás nem a várt eredményt adja vagy nem a megszokott képernyőképek jelennek meg.

A jelentéshez az IBSZ *{3 számú melléklet – Biztonsági események jelentése}* mellékletét kell használni. Szoftverzavarok esetén legalább a következő feladatokat végre kell hajtani:

a) fel kell jegyezni a zavaró jelenséget és a képernyőn megjelenő minden üzenetet és

b) be kell szüntetni az adott számítógép használatát.

A felhasználóknak tilos a hibásnak feltételezett szoftvert eltávolítaniuk az elektronikus információs rendszerből, illetve kísérletet tenni a hiba elhárítására.

A hibaelhárítást és helyreállítást a rendszergazda hajthatja végre.

Abban az esetben, ha feltételezhető az információbiztonság sérülése, akkor az eseményt a rendszergazdának jelentenie kell az információbiztonsági felelősnek, aki kivizsgálja az eseményt.

8. számú melléklet – Felhasználói Nyilatkozat

Nyilatkozat

Alulírott (név: ,..... beosztás:..... szervezeti egység: .....), kijelentem, hogy a Bükki Nemzeti Park Igazgatóság Informatikai Biztonsági Szabályzatának és/vagy Felhasználói Informatikai Biztonsági Házirendjének tartalmát megismertem és elfogadom, hogy azt munkám során betartom, illetve betartatom (vezetők esetén).

……., 2020. .....

.....
Aláírás

9. számú melléklet – Információbiztonsági tájékoztató jogviszony megszűnése esetén

Információbiztonsági tájékoztatás

1. Tájékoztatom, hogy a Bükki Nemzeti Park Igazgatósággal (továbbiakban: az Igazgatóság) fennálló jogviszonya megszűnésének napjától, 201… . ……..-től az Igazgatóság elektronikus információs rendszereihez való hozzáférési jogosultsága megszűnt. Legkésőbb ezen a napon köteles a használatában lévő, az Igazgatóság elektronikus információs rendszerével kapcsolatos valamennyi eszközt hiánytalanul, sértetlenül munkáltatója részére visszaszolgáltatni.

2. Az Igazgatóságnál működő elektronikus információs rendszereket az Igazgatóság kizárólag hivatali munkavégzés céljából biztosítja a munkatársak részére, az elektronikus információs rendszerekben keletkező és ott tárolt, kezelt adatok, információk vonatkozásában az Igazgatóság fenntartja magának a tulajdonjogot.

3. Az Igazgatóságnak továbbra is hozzáférési lehetősége van az Ön által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

4. Jogviszonyának megszűnését követően nem jogosult az Igazgatóság elektronikus információs rendszereiben tárolt, jogviszonya folytán készített, illetve megismert adatokat felhasználni, azokat további személyek tudomására hozni, valamint a megismert és használt elektronikus információs rendszerek összetételéről, felépítéséről, működéséről további személyek számára bárminemű információt közölni.

5. A 4-es pontban megfogalmazott jogellenes magatartásnak polgári- és büntetőjogi következményei lehetnek.

6. Jelen tájékoztatás célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló 41/2013. (VII.15.) BM rendelet 3. § (1) bekezdésében foglaltak szerint, az e rendelet 3. számú mellékletében meghatározott követelményeknek a 4. számú melléklet 3.1.6.4.1.3. pontjában meghatározott módon való megvalósítása.

Eger, 201 … .

……
Igazgató

A fenti tájékoztatást tudomásul vettem:

Eger, 201.....

……
munkavállaló neve

…….
aláírása

10. számú melléklet – Titoktartási Nyilatkozat

TITOKTARTÁSI NYILATKOZAT

Alulírott

Név: .....

Anyja neve: .....

Lakcím: .....

Sz. ig. szám: .....

a ..... munkatársa kijelentem, hogy

a **Bükki Nemzeti Park Igazgatóság,** mint **Megrendelő**,

valamint .....

mint **Vállalkozó**

között

.....tárgyú,

..... **-én megkötött vállalkozási/megbízási/szállítási szerződés**

keretében elvégzett feladatok során tudomásomra jutott információkat és adatokat bizalmasan kezelem és megtartom. A tudomásomra jutott információkat, adatokat az érdekkörön kívüli személlyel nem közlöm. Ezen felelősségem fennáll azt követően is, ha a

..... -vel való szerződéses jogviszonyom bármely okból megszűnik.

Eger, 201 .....

……

Nyilatkozó

	Tanú 1	**Tanú 2**
Aláírás:	.....	.....
Neve:	.....	.....
Anyja neve:	.....	.....
Lakcím:	.....	.....
Sz. ig. szám:	.....	.....

11. számú melléklet – Iratok nem kormányzati e-mail címre történő kiküldésének igénylése űrlap

Iratok nem kormányzati e-mail címre történő kiküldésének igénylése űrlap a II.10.18.2. fejezet alapján

Iktatószám:

IGÉNYLŐ ADATAI

Igénylő neve: …….

Szervezeti egység: ……

Telefon: ……

Email: …….....

E-mail cím, melyre az irat kiküldhető

Címzett megnevezése:.....
……..

Jogosultság kezdete: …… Jogosultság vége: ……..

Új jogosultság
Jogosultság törlése
Jogosultság módosítása

Egyéb:……
……
…….

INDOKLÁS

A jogosultságigényléshez kapcsolódó feladatellátás megnevezése indoklással:
……
……

……..
Kelt: …… igénylő aláírása

Munkahelyi vezetői jóváhagyás

Vezető: ……..
Beosztása: …….. …..……..
Kelt: …….. vezető aláírása