BÜNTETÉS-VÉGREHAJTÁS ORSZÁGOS PARANCSNOKSÁGA

Jóváhagyom:

Farsang Tamás bv. ezredes
az országos parancsnok
gazdasági és informatikai helyettese

Budapest, *„az elektronikus dátumbélyegző szerint”*

INFORMATIKAI BIZTONSÁGI KÉZIKÖNYV

Módszertani útmutató az Informatikai Biztonsági Szabályzat (IBSZ) gyakorlati végrehajtásához

2020.

Tartalomjegyzék

I. BEVEZETŐ RENDELKEZÉSEK

1. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai és biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó közvéleményekről szóló 41/2015.(VII.15.) BM rendelet, valamint a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzata (a továbbiakban: IBSz) alapján módszertani útmutatóként az alábbi Informatikai Biztonsági Kézikönyvet (a továbbiakban: IBK) adom ki.

2. Az IBK célja az IBSz-ben foglalt szabályok végrehajtásának elősegítése.

3. Az IBK hatálya a Büntetés-végrehajtás Országos Parancsnokságára (a továbbiakban: BVOP), a büntetés-végrehajtási intézetekre és intézményekre, valamint a fogvatartottak kötelező foglalkoztatására létrehozott gazdasági társaságokra (a továbbiakban együtt: bv. szervek), valamint ezek személyi állományára terjed ki.

Értelmező rendelkezések

4. alapjogosultságok jegyzéke: azon jogosultságok összessége, amelyek a felhasználó által a BV informatikai rendszereiben alapértelmezetten, igénylést követően használhatóak (1. melléklet);
5. elemi jog: az elektronikus információs rendszerben (a továbbiakban: rendszerben) tárolt adattal, informatikai objektummal kapcsolatban végezhető műveletekre vonatkozó lehetőség, engedély, amely lehet:
   a) olvasási jog,
   b) írási jog,
   c) módosítási jog,
   d) végrehajtási jog,
   e) logikai törlési jog,
6. extra jogosultság: az a jogosultság, amelyet a rendszer működtetéséért felelős (adatgazda) szervezeti egység vezetője szakmai indokok alapján ilyenként definiál, kiosztása korlátozott;
7. hálózati tárhely: a bv. szervezet hálózatában működő szervereken létrehozott, többszintű hierarchiába szervezett elektronikus tárolókból álló háttérkapacitás;
8. jogosultság: elemi jogok olyan – legalább egyelemű – halmaza, mely a rendszerben meghatározott adatokon (adatkörökön) meghatározott tevékenységek végrehajtását lehetővé teszi;
9. jogosultságcsoport: jogosultságok – legalább egyelemű – halmaza – amely valamely feladat ellátásához kötődik és annak ellátását a bv. szervezet rendszerében lehetővé teszi;
10. jogosultság ellenjegyzése: az arra jogosult vezető hozzájárulása az igényelt extra jogosultság beállításához;
11. jogosultság engedélyezése: az arra jogosult vezető hozzájárulása az igényelt jogosultság beállításához;
12. jogosultság igénylése: a jogosultság szükségességének jelzése, amelyet az arra jogosult vezető kezdeményez közvetlenül vagy felhasználói jelzés megerősítésével;
13. jogosultság kezelése: a szervezeti egység jogosultságainak, illetve a munkatárs jogosultságainak

a) vezető általi igénylése, engedélyezése és visszavonása, valamint felülvizsgálata, kiadása és visszavétele
b) a rendszer működtetéséért felelős (adatgazda) által történő ellenőrzése, ellenjegyzése,
c) a jogosultság-adminisztrátor általi technikai kialakítása, beállítása, illetve nyilvántartása;

14. jogosultságkezelő alkalmazás: önálló informatikai rendszer, amely lehetővé teszi a felhasználók jogosultságainak megfelelő módon történő, hiteles naplózott nyilvántartását és kezelését a jogosultságkezelésre feljogosított felhasználók számára;
15. külső rendszer: azok a bv. szervezeten kívüli, belföldi, idegen tulajdonú és idegen szervezet által felügyelt nyilvántartások, adatbázisok, melyek használata jogszabályi kötelezettséghez, szerződéshez, illetve együttműködési megállapodáshoz kötött;
16. külső rendszer elérését biztosító jogosultság: a bv. szervezet igénylése alapján a külső rendszer felügyelő szervezet által biztosított jogosultság;
17. az IBK alkalmazásában
    a) közvetlen vezető: szervezeti egység vezetője,
    b) engedélyező vezető: a munkáltatói jogkört gyakorló vezető, BVOP vonatkozásában Informatikai Főosztályvezető (továbbiakban IFO),
    c) ellenjegyző vezető: a rendszer működtetéséért felelős (adatgazda) szervezeti egység vezetője;
18. Az előző pont b) és c) pontjai tekintetében az elektronikus jogosultságkezelést megvalósító alkalmazásokban az engedélyezésre, illetve ellenjegyzésre jogosult vezető helyett az általa kijelölt, irányítása alá tartozó vezető is elláthatja e feladatokat.
19. Az IBK alkalmazásában külső szervezethez tartozó felhasználó közvetlen vezetője alatt a külső munkavállalót fogadó szervezeti egység vezetőjét kell érteni.

II. FIZIKAI ÉS LOGIKAI VÉDELEM

Gépterem, szerverszoba fizikai védelmi eljárásrend

20. A rendszerek központi elemeinek helyt adó helyiségeket (gépterem, szerverszoba) a biztonságtechnikai rendszer részét képező beléptető rendszerrel, nyitásérzékelővel, mozgásérzékelővel, valamint a belépő személyek azonosíthatóságát biztosító kamerával kell ellátni. A rendszer elemeit lehetőség szerint úgy kell elhelyezni, hogy a legkisebb mértékre csökkentse a fizikai és környezeti veszélyekből adódó lehetséges kárt és a jogosulatlan hozzáférés lehetőségét.

21. A fizikai hozzáférést biztosító kulcsokat az informatikai szakterület vezetőjénél elhelyezett páncélszekrényben kell elzártan tárolni. A kulcsok kiadásáról, visszavételéről naprakész nyilvántartást kell vezetni, a nyilvántartás vezetéséért a páncélszekrény kezelője felelős.

22. A bv. szervezet géptermeinek és szerverszobáinak jegyzékét a 2. melléklet tartalmazza.

23. Az egyes géptermekbe és szerverszobákba történő belépést az informatikai szakterület vezetője engedélyezi.

24. A helyiségekbe történő belépés kizárólag mágneskártyával, különösen indokolt esetben kulccsal lehet.

25. Nem a bv. szervezet személyi állományába tartozó személy kizárólag az informatikai szakterület vezetőjének az engedélye alapján belépési engedéllyel rendelkező személy kíséretében léphet be a gépterembe vagy a szerverszobába. A belépésekről az informatikai szakterület elektronikus nyilvántartást vezet (3. melléklet). A nyilvántartásban fel kell tüntetni a belépő személy nevét, benntartózkodás idejét és a kísérő személy nevét.

26. Az informatikai szakterület vezetője gondoskodik a belépési naplók ellenőrzési céllal történő átvizsgálásáról.

27. Azonnal át kell vizsgálni a belépési naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak.

28. A rendszereknek helyt adó létesítmények fizikai követelményeit a 4. melléklet tartalmazza.

29. A BVOP által üzemeltetett központi gépterem esetében a 4. biztonsági osztályba sorolt rendszerek esetében meghatározott biztonsági követelményeket kell teljesíteni. A bv. intézetek által üzemeltetett szerverszobák esetében a 2. biztonsági osztályba sorolt rendszerekre meghatározott biztonsági követelményeket kell teljesíteni.

30. Az információs rendszerelemek, eszközök bv. szervezet létesítményeibe történő be- és kivitelét a BVOP esetében az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője írásban engedélyezi. Az engedélyek őrzéséről az informatikai szakterület gondoskodik.

Biztonsági esemény fogalma

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

32. A biztonsági esemény kiterjedése szerint lehet helyi vagy országos szintű. Helyi szintű biztonsági esemény, melynek hatása csak az adott bv. szervre terjed ki, országos szintű esemény, mely egy adott intézetben történik ugyan, de kihatással van az országos rendszer működésének biztonságára is.

Biztonsági esemény kezelése

33. A rendszerben bekövetkezett biztonsági eseményeket dokumentálni kell, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében. Ennek megfelelően az az informatikai szakterület, illetve a BVOP vonatkozásában az IFO vezetője megfogalmazza, dokumentálja a konkrét biztonsági eseményre vonatkozó eseménykezelési eljárást, amely tartalmazza az előkészületet, az észlelést, a vizsgálatot, az elszigetelést, a megszüntetést és a helyreállítást.

34. Az IFO vezetője:
    a) összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével,

b) egyezteti az eseménykezelési eljárásokat az ügymenet-folytonossági tervéhez tartozó tevékenységekkel,
c) az eseménykezelési tevékenységekből levont tanulságokat beépíti az eseménykezelési eljárásokba, továbbképzésekbe és tesztelésbe.

35. Az informatikai szakterület nyomon követi és dokumentálja a rendszer biztonsági események típusát, terjedelmét, az általuk okozott károkat, a helyreállítás lehetőségeit és költségeit, a helyreállítás időtartamát.

36. A folyamat működtetése és fejlesztése, a kapcsolódó szabályrendszer naprakészen tartása (személyi változások, infrastruktúra-változások, gyakorlati események tapasztalatai stb. miatt), valamint azok kommunikálása az IFO vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének a feladata.

A biztonsági események figyelése

37. A rendszerek működése során fellépő eseményeket megfelelő részletességgel naplózni kell. Az informatikai szakterületnek ezeket a naplóállományokat rendszeresen félévente ellenőriznie kell, az ellenőrzés eredményéről jelentést kell tennie az IFO vezetője részére. A biztonsági események folyamatos figyelése és észlelés esetén azok jelentése, valamennyi munkatárs, szerződött fél felelőssége.

A biztonsági események jelentése

38. Minden vélt vagy valós információbiztonsági incidenst a felhasználóknak azonnal jelenteniük kell az informatikai szakterület részére, amely jelenti azt az IFO részére. Az IFO vezetője dönt arról, hogy az esemény informatikai jellegűnek minősül, vagy olyan biztonsági esemény, melyről az elektronikus információs rendszer biztonságáért felelős személyt (a továbbiakban: IBF) is tájékoztatni kell.

39. A felhasználó köteles a tapasztalt jelenséget, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul az informatikai szakterület rendelkezésére bocsátani (pl. feljegyzés, képernyőkép).

40. A biztonsági esemény észlelésekor, a biztonsági eseményt meg kell szüntetni, vagy az esemény jellegéből adódóan azt izolálni szükséges. Az izolálást azonnal meg kell kezdeni, amelyért az informatikai szakterület a felelős az érintett felek bevonásával. Az információbiztonsági incidenst, valamint annak életútját írásos dokumentumban kell rögzíteni, a IFO felé jelentést a helpdesk@bv.gov.hu címen írásban és/vagy telefonon, az esemény jellegétől függően telefonon haladéktalanul kell megtenni. A jelentés nem tartalmazhat olyan szenzitív adatot (pl. személyes adatot), elemeket, amelyet harmadik fél nem ismerhet meg.

41. A felhasználó a fentiek szerint köteles eljárni, amennyiben az alábbi körbe tartozó informatikai biztonsági eseményt észlel, vagy ilyenre gyanakszik:
a) a felhasználói azonosítóval való visszaélés, illetéktelen rendszer- vagy adathozzáférés, bármely, a felhasználó által használt rendszer, infokommunikációs eszköz tekintetében (pl. elektronikus levelezés, szakrendszer stb.),
b) adathalász tevékenység, amely a felhasználó személyes adatainak vagy intézményi hozzáféréseinek, illetve az intézményt érintő – nem közérdekű vagy közérdekből nyilvános – adatok, információk megszerzésére irányul (pl. adathalász oldalak,

kéretlen levelek vagy közvetlen telefonhívások, amelyek személyes vagy munkahelyi információk megszerzésére irányulnak),

c) rosszindulatú szoftverek (vírusok, trójai programok stb.) jelenléte a felhasználó által használt rendszeren, infokommunikációs eszközön,

d) adatszivárgás, ami megvalósulhat nem közérdekű vagy közérdekből nyilvános adatok szándékos vagy véletlen továbbításával, kiszivárogtatásával azok megismerésére nem jogosult szervezetek, személyek vagy az adatok bizalmasságának megőrzése szempontjából megbízhatatlan rendszerek felé,

e) felhasználó használatában lévő informatikai eszköz (számítógép, notebook, mobil infokommunikációs eszköz) elvesztése, ezek megbontására utaló jelek.

42. Az Ibtv. 13. § (3) szerinti bejelentés-köteles informatikai biztonsági események:

a) katasztrófahelyzetet előidéző történés, cselekvés, mulasztás,

b) a bv. szervezet által működtetett infrastruktúrát érintő olyan meghibásodás, amely tömeges szolgáltatáskiesést vagy a szolgáltatásokban jelentős mértékű minőségromlást nem okoz, azonban veszélyezteti a szolgáltatások folyamatosságát, illetve az infrastruktúra üzembiztonságát (kiemelt jelentőségű hálózati szegmens esetén a redundáns hálózati elem kiesése, tápellátó rendszerek meghibásodása, felügyeleti, monitoring rendszerek meghibásodása stb.),

c) bv. szervezet által működtetett infrastruktúrát érintő olyan meghibásodás, amely a szolgáltatásokban kisebb mértékű minőségromlást okozhat, azonban a felhasználókat (ellátotti kört, ügyfeleket) tömegesen érintheti,

d) a bv. szervezet által működtetett infrastruktúrát érintő olyan meghibásodás, amely tömeges szolgáltatáskiesést, nagyszámú felhasználót vagy jelentős mértékű minőségromlást okozhat,

e) külső vagy belső támadás.

43. Az Ibtv. szerinti bejelentés-köteles informatikai biztonsági eseményekkel kapcsolatos bejelentésre vonatkozó részletes előírások (tartalom, továbbítás módja) az NKI GovCERT honlapján érhetők el.

Segítségnyújtás a biztonsági események kezeléséhez

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

45. A szabályozó eszközök rendszeres felülvizsgálata során az információbiztonsági események, incidensek kezelési folyamatához kapcsolódóan meg kell határozni és folyamatosan pontosítani kell a biztonsági események kiértékelésének, kategorizálásának (pl. súlyosság stb.) kritériumrendszerét. Tervezni kell azokat az erőforrásokat és vezetői támogatást, melyek szükségesek a biztonsági eseménykezelési lehetőségek bővítésére, hatékonyabbá tételére és fenntartására.

46. A biztonsági eseménykezelés a következő folyamatokra terjed ki, melynek felelőse az informatikai szakterület, érdekelt munkatársak, kijelölt szakértők.

a) Észlelés, jelentés;

b) Vizsgálat:

ba) incidensek okának azonosítása, elemzése, kivizsgálása,

bb) bizonyítékok gyűjtése,

bc) incidens behatárolása,

bd) A vizsgálat során meg kell állapítani, hogy:

da) milyen események történtek?

db) az események milyen és mekkora kárt okoztak, illetve okozhattak?

dc) milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?

dd) mik voltak az események kiváltó okai, előzményei?

c) Elszigetelés (az esemény jellegéből adódóan);

d) Megszüntetés, mely magában foglalja:

da) a szükséges intézkedések meghatározását,

db) az incidensekre hozott döntéseket, intézkedések dokumentációját,

dc) az intézkedések végrehajtását,

dd) az incidenssel kapcsolatos dokumentációt meg kell őrizni, egy esetleges peres (polgári, vagy büntető) eljárásban történő bizonyítás érdekében;

e) Helyreállítás

ea) helyreállítási felelősségek kijelölése,

eb) az ügymenet-folytonosságot érintő események esetén (az esemény jellegéből adódóan) az ügymenet-folytonossági tervben vagy a katasztrófa-elhárítási tervben rögzített módon kell eljárni,

ec) a helyreállítási tevékenység ellenőrzése.

Képzés a biztonsági események kezelésére

47. Az információbiztonsági incidensekkel kapcsolatos képzések, valamennyi állományi tag felé belépéskor, az adott munkakörhöz igazodóan, az alap információbiztonsági oktatás részeként megtörténnek. Ezen felül a munkakör megváltozása esetén, a féléves oktatásokon vagy súlyos információbiztonsági események után ismétlődő képzés történik a tudatosság fenntartása, illetve fejlesztése érdekében.

A biztonsági események kezelésének tesztelése:

48. Az informatikai szakterület meghatározott gyakorisággal teszteli az elektronikus információs rendszerre vonatkozó biztonsági eseménykezelési képességeket előre kidolgozott tesztek felhasználásával, annak érdekében, hogy meghatározza a biztonsági eseménykezelés hatékonyságát, dokumentálja az eredményeket, továbbá szükség esetén egyezteti azt az érintett szakterületekkel.

Biztonságtervezési eljárásrend

49. A jelen fejezet meghatározza a bv. szervezet által végzett biztonságtervezési eljárás folyamatait, az abban részt vevők körét, felelősségét, valamint az ellenőrzés rendjét.

50. A bv. szervezet vezetője az IFO vezetője és az IBF útján felügyeli a rendszer és környezete biztonsági állapotát.

51. A rendszerbiztonsági terv elkészítése során a jelen eljárásrendet kell alkalmazni azzal, hogy az IFO a tervek elkészítése, módosítása és felülvizsgálata során elvégzi a bv. szervezeten belül szükségessé váló egyeztetéseket.

52. A biztonságtervezéssel összefüggésben az IFO vezetője gondoskodik a rendszerdokumentáció, különösen az alábbi dokumentumok rendelkezésre állásáról és naprakészen tartásáról:
    a) rendszerbiztonsági tervek,
    b) architektúra leírások,
    c) adminisztrátori kézikönyvek, üzemeltetési leírások,
    d) felhasználói leírások.

53. Amennyiben külső támogató igénybe vételére kerül sor rendszer fejlesztése céljából, a partner szerződéses kötelezettségeként kell meghatározni a rendszerdokumentáció elkészítését, annak a bv. szervezet részére történő rendelkezésre bocsátását, továbbá szükség szerinti aktualizálását.

54. A rendszerbiztonsági tervet az Infrastruktúra és Üzemeltetési Osztály vezetője készíti el, azt az IFO vezetője hagyja jóvá.

55. Az elektronikusan készült és jóváhagyott rendszerbiztonsági tervet nem szerkeszthető formátumban kell tárolni és elérhetővé tenni az arra jogosultak számára, továbbá – az adathordozó típusától függetlenül – gondoskodni kell arról, hogy jogosulatlanok számára az ne legyen megismerhető, módosítható.

56. A rendszerbiztonsági terv összhangban tartalmazza különösen:
    a) a rendszer hatókörének, alapfeladatainak (biztosítandó szolgáltatásainak), biztonságkritikus elemeinek és alapfunkcióinak meghatározását,
    b) a rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályának meghatározását,
    c) a rendszer működési körülményeinek és más rendszerekkel való kapcsolatainak meghatározását,
    d) a távoli karbantartási és diagnosztikai kapcsolatok létrehozására, alkalmazására vonatkozó előírásokat,
    e) a rendszer biztonsági követelményeit,
    f) az aktuális vagy tervezett védelmi intézkedéseket és intézkedés-bővítéseket,
    g) a rendszerbiztonsági terv megismerésére jogosultak körét – az érintettek beosztásának, munkakörének megnevezésével.

57. A rendszerbiztonsági tervek rendelkezésre állását és aktualizálását az IFO vezetője – mennyiben az adott rendszerbiztonsági terv más gyakoriságot nem határoz meg – évenként ellenőrzi, szükség esetén intézkedik azok módosítására.

58. A rendszerbiztonsági tervet a rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása, vagy a védelmi intézkedések értékelése során feltárt problémák esetén haladéktalanul felül kell vizsgálni és – szükség esetén – aktualizálásáról intézkedni kell, amely feladatok elvégzéséért az IFO vezetője felelős.

Biztonságelemzési és -értékelési eljárásrend

59. A biztonságelemzés a biztonsági értékelés és a naplózási tevékenység alapul vételével, a naplóbejegyzések folyamatos elemzésével és értékelésével valósul meg. A naplózás

részletes szabályait a jelen kézikönyv naplózási eljárásrenddel kapcsolatos fejezete tartalmazza.

60. A jelen fejezet meghatározza a bv. szervezet által végzett biztonságelemzési és -értékelési eljárások részleteit, a folyamatokban részt vevők felelősségét, valamint az ellenőrzés rendjét.

61. Az éves biztonsági értékelés tartalmazza különösen, de nem kizárólagosan:
    a) a rendszerek biztonsági osztályba sorolásának felülvizsgálatát,
    b) az OVI űrlapok adattartalma ellenőrzését,
    c) az informatikai biztonsági ellenőrzések eredményei alapján meghatározott feladatok végrehajtásának értékelését, a folyamatban lévő cselekvési terv értékelését,
    d) az előző biztonsági értékelés óta bekövetkezett biztonsági események ismertetését, értékelését,
    e) az értékelési környezetet, az értékelő csoportot, az értékelés célját, az értékelést végzők feladatát.

62. A bv. szervezet a védelmi intézkedések értékelése keretében – az IBSZ-ben meghatározottak szerint – speciális vizsgálatot végeztet.

63. A speciális vizsgálat magában foglalhatja különösen
    a) a sérülékenységvizsgálatot,
    b) a rosszhiszemű felhasználó tesztet,
    c) a belső fenyegetettség értékelést,
    d) a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, továbbá
    e) a bv. szervezet által meghatározott egyéb biztonsági értékeléseket.

64. A speciális vizsgálatokat az IFO vezetője tervezi meg és gondoskodik azok végrehajtásáról az arra hatáskörrel rendelkező szerv útján. A speciális vizsgálat tervezéséről és előkészítéséről az IBF-et előzetesen tájékoztatja.

65. Az IFO vezetője gondoskodik a legalább 3. biztonsági osztályba sorolt rendszerek vonatkozásában a biztonsági mérési rendszerének kialakításáról és működtetéséről.

III. ÜZEMELTETÉSI RENDELKEZÉSEK

Konfigurációkezelési eljárásrend

66. A konfigurációkezelés biztosítja a tervek és a megvalósított produktív rendszer konzisztenciáját.

67. A konfigurációkezelés feladata a szervezet informatikai rendszereinek és rendszerkomponenseinek így előálló biztonsági állapotának alapkonfigurációként történő rögzítése az előélettel együtt, és a biztonsági állapot fenntartása a változtatások ellenőrzött módon történő végrehajtásán (lásd: változáskezelés) és a monitorozáson keresztül.

68. Az informatikai rendszerkomponenseiről nyilvántartást kell kialakítani.

69. A hardver és szoftver komponensek mellett javasolt felvenni (vagy hivatkozni rá) a kapcsolódó dokumentációkat és egyéb, kiegészítő komponenseket is, amelyek hasznosak lehetnek a produktív rendszer újraépítése során. Az adatok naprakészen tartása az IFO, bv. intézetek esetében az informatikai szakterület vezetőjének a feladata.

70. A konfigurációkezelési rendszerhez/dokumentumokhoz történő hozzáféréseket korlátozni kell a minimálisan szükséges szintre, csak az arra jogosult szakterület férhet hozzá.

71. A letesztelt, biztonsági szempontok szerint is megfelelően ellenőrzött, bevezetésre kész rendszereket dokumentálni kell, ezek alkotják a rendszerek alapkonfigurációját. A rendszerkomponensek változtatása során gondoskodni kell a frissítésről a változáskezelés folyamat részeként, annak biztosítása érdekében, hogy a rendszerek aktuális állapotát tükrözze vissza a konfigurációk nyilvántartása.

72. Az információs rendszer alapkonfigurációjának minimálisan szükséges elemei:
    a) hálózati aktív eszközök firmware verziója, valamint konfigurációs állományai,
    b) szakrendszereket futtató szerverek, minimális hardver követelményei,
    c) fájlszerver NTFS, SHARE jogosultság beállításainak aktuális leírása,
    d) adatbázisszerver aktuális telepített verziója,
    e) VPN szerver konfigurációs beállításai,
    f) munkaállomások minimális hardver követelményei, valamint azok beállításai,
    g) a telepített operációs rendszerek, szoftverek, szakrendszerek és frissítéseik telepítő lemezei, regisztrációs kulcsai, rendszergazdai jelszavait tároló zárt borítékok,
    h) a bv szervezet hálózatának topológiája,
    i) alkalmazások közötti kapcsolat vázrajza.

73. Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

74. Az áttekintések és frissítések összefüggésében az informatikai szakterület gondoskodik:
    a) az alapkonfiguráció frissítéséről, az elektronikus információs rendszerelemek telepítéséről és frissítések elvégzéséről,
    b) korábbi konfigurációk megőrzéséről,
    c) az elektronikus információs rendszer alapkonfigurációjáról, és annak további verzióiról – hogy szükség esetén lehetővé váljon –, illetve a változatlan állapot megőrzéséről,
    d) magas kockázatú területek konfigurálásáról,
    e) biztonsági szempontokból meghatározott módon konfigurált elektronikus információs rendszerelemek vagy eszközök biztosításáról azon személyek számára, akik az elektronikus információs rendszert külső helyszínen használják,
    f) megfelelő biztonsági eljárások alkalmazásáról az eszköz belső használatba vonásakor.

75. Az IFO Fejlesztési és Stratégiai Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy dokumentáltan nyomon követi a konfigurációváltozások felügyeletét (változáskezelés), ennek körében:

a) meghatározza a változáskezelési felügyelet alá eső változástípusokat,
b) meghatározza az egyes változástípusok esetén a változáskezelési vizsgálat kötelező és nem kötelező elemeit, előfeltételeit (csatolt dokumentációk, teszt jegyzőkönyvek stb.),
c) megvizsgálja a változáskezelési felügyelet elé terjesztett, javasolt változtatásokat, majd kockázatelemzés alapján jóváhagyja, vagy elutasítja azokat,
d) dokumentálja az elektronikus információs rendszerben történt változtatásokra vonatkozó döntéseket,
e) megvalósítja a jóváhagyott változtatásokat az elektronikus információs rendszerben,
f) visszakereshetően megőrzi az elektronikus információs rendszerben megvalósított változtatások dokumentumait, részletes leírását,
g) auditálja és felülvizsgálja a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységeket,
h) teszteli az új verziót a konfiguráció megváltoztatása előtt, dönt annak megfelelőségéről, dokumentálja az elektronikus információs rendszer változtatásait az éles rendszerben történő megvalósítása előtt (előzetes tesztelés és megerősítés.)

76. Az IFO vezetője által kijelölt személy megvizsgálja az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatását, még a változtatások megvalósítása előtt.

77. Az IFO vezetője által kijelölt személy a belső szabályozásban meghatározza a változtatásokhoz való hozzáférési jogosultságot, dokumentálja a hozzáférési jogosultságokat, jóváhagyja azokat, fizikai és logikai hozzáférés korlátozásokat alkalmaz az elektronikus információs rendszer változtatásaival kapcsolatban.

78. A konfigurációs beállítások körében az IFO vezetője által kijelölt személy:
a) meghatározza a működési követelményeknek megfelelő, biztonsági szempontból a lehető leginkább korlátozott módon – „szükséges minimum” elv alapján – az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja,
b) elvégzi a konfigurációs beállításokat a rendszer valamennyi elemében,
c) a meghatározott elemek konfigurációs beállításaiban azonosít, dokumentál és jóváhagy minden eltérést,
d) figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait.

79. A beállítást elvégző a rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa, meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

80. A beállítást elvégző meghatározott gyakorisággal átvizsgálja a rendszereket, meghatározza és kizárja vagy letiltja a szükségtelen vagy nem biztonságos funkciókat, portokat, protokollokat és szolgáltatásokat.

81. Az IFO Fejlesztési és Stratégiai Osztály vezetője által kijelölt személy meghatározza, felülvizsgálja és frissíti az elektronikus információs rendszerben nem futtatható (tiltott, úgynevezett feketelistás) szoftverek listáját és tiltja ezek futtatását.

82. Az IFO Fejlesztési és Stratégiai Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy gondoskodik az Elektronikus információs rendszerelem leltár meglétéről az alábbi tartalmi szempontok alapján:
    a) a leltár tartalmazza az elektronikus információs rendszer elemeit,
    b) meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt,
    c) gondoskodik arról, hogy a leltár pontosan tükrözze az elektronikus információs rendszer aktuális állapotát,
    d) az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet tartalmazza,
    e) legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez,
    f) gondoskodjon az elektronikus információs rendszerelem leltár frissítéséről az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában.

83. Az IFO Fejlesztési és Stratégiai Osztály vezetője által kijelölt személy gondoskodik a Konfigurációkezelési terv kialakításáról az alábbi szempontok alapján:
    a) kialakít, dokumentál és végrehajt egy, az elektronikus információs rendszerre vonatkozó konfigurációkezelési tervet, mely figyelembe veszi a szerepköröket, felelősségeket, konfigurációkezelési folyamatokat és eljárásokat,
    b) bevezet egy folyamatot a konfigurációelemek azonosítására a rendszer-fejlesztési életciklus folyamán és a konfigurációelemek konfigurációjának kezelésére,
    c) meghatározza az elektronikus információs rendszer konfigurációelemeit, és a konfigurációelemeket a konfigurációkezelés alá helyezi,
    d) védi a konfigurációkezelési tervet a jogosulatlan felfedéssel és módosítással szemben.

84. Az érintett szervezet kizárólag olyan szoftvereket és kapcsolódó dokumentációt használ, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

85. Az IFO Fejlesztési és Stratégiai Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy a másolatok, megosztások ellenőrzésére nyomon követi a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát.

86. Az IFO Fejlesztési és Stratégiai Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy ellenőrzi és dokumentálja az állománymegosztásokat, hogy meggyőződjön arról, hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

87. A bv. szerv a szakrendszerek jogszabályváltozásának nyomon követéséhez, valamint az infrastruktúra működtetéséhez support szerződés megkötésére jogosult.

88. A szakrendszerek külső támogatását biztosító feltételeket a szállítókkal megkötött szerződéseknek kell tartalmaznia. (Főnix rendszer Noémi felület, Távfelügyeleti rendszer-hibabejelentő és Microsoft).

Rendszer karbantartási eljárásrend

89. A rendszeren karbantartási feladat kizárólag karbantartási szerződés alapján, a BVOP esetében az IFO vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének engedélye alapján, az általa kijelölt személy felügyelete mellett végezhető.

90. A karbantartó személyzet által a létesítménybe hozott karbantartási eszközöket, kijelölt személy a nem megfelelő vagy jogosulatlan módosítások megakadályozása érdekében átvizsgálja.

91. A diagnosztikai és teszt programokat tartalmazó adathordozókat a kártékony kódok tekintetében, az elektronikus információs rendszerben történő használat előtt ellenőrzi.

92. Információs rendszerelem elszállítása esetén arról minden adatot és információt törölni kell, ennek ellenőrzését a BVOP esetében az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője végzi.

93. A karbantartási szerződésben kell meghatározni, a karbantartások gyakoriságát, a kapcsolat létesítésére vonatkozó részletes szabályokat.

94. Távoli karbantartás kizárólag azonos biztonsági képességekkel rendelkező információs rendszerből engedélyezett.

95. Távoli karbantartás kizárólag előzetes bejelentés esetén lehetséges. Távoli karbantartás esetén hálózati kapcsolat kizárólag a karbantartás idejére létesíthető. A karbantartás végén a kapcsolatot le kell zárni.

96. A helyi és távoli karbantartásokról készült feljegyzéseket a BVOP esetében az IFO, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy nyilvántartja és évente felülvizsgálja (5. melléklet).

97. A karbantartási, javítási tevékenység végén a karbantartott rendszerelem működéséről, meg kell győződni.

98. A távoli karbantartások naplózási követelményeit a naplózási rend tartalmazza.

99. A rendszeren karbantartási feladatot végrehajtó szervezetek személyek nyilvántartását a BVOP esetében az IFO, bv. intézetek esetében az informatikai szakterület vezetője által kijelölt személy a 6. melléklet alapján vezeti.

Adathordozókra vonatkozó eljárásrend

100. Az IFO Infrastruktúra és Üzemeltetési Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője nyilvántartást vezet az egyes adathordozó típusokról, az ahhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk tartalmáról.

101. Minden állományi tag kötelessége az adattárolók rendeltetésszerű használata. Az adathordozók kizárólag a munkavégzéshez szükséges adatok és szoftverek tárolására alkalmazhatóak.

102. Az adathordozókat és mobil eszközöket indokolással ellátott szolgálati jegyen kell igényelni.

103. A munkavégzéshez adathordozókat és mobil eszközöket a felhasználók számára a szervezeti egység vezetője igényelhet. Az igénylés teljesítését a BVOP esetében az IFO vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének javaslata alapján a bv. szerv vezetője hagyja jóvá.

104. Adathordozó igénylése során jelezni kell, hogy az igénylő kizárólag a bv. szerv területén történő használatra vagy azon kívüli használatra is igénybe kívánja-e venni az igényelt adathordozót, illetve azt, hogy a titkosított vagy titkosítás nélküli adathordozót kíván-e igényelni.

105. Cserélhető adathordozó igénylése kizárólag indokolt esetben hagyható jóvá.

106. A kiadott adathordozókat és mobil eszközöket külső fél számára átadni nem lehet.

107. Az adathordozó vagy mobil eszköz kiadása az informatikai szakterület munkatársainak feladata.

108. Az adathordozó vagy mobil eszköz kiadását dokumentálni kell, ennek során átadás-átvételi bizonylatot, és ha adatot tartalmaz, adatkísérő lapot kell kitölteni.

109. Az igénybe vevő az aláírásával az adathordozó vagy mobil eszköz átvételét igazolja, illetve azt, hogy megismerte az eszköz kezelésének szabályait, és az eszközért felelősséget vállal.

110. A bv. szerv területén kívüli használatra is vonatkozó igénylés esetén az adathordozón vagy mobil eszközön tárolt adatok védelmére való felkészítéséről az informatikai szakterület gondoskodik. Ennek biztosítását az IFO Infrastruktúra és Üzemeltetési Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője ellenőrzi.

111. Az adathordozó vagy mobil eszköz visszavételét az érintett szervezeti egység vezetője kezdeményezheti. Az adathordozót vagy mobil eszközt az informatikai szakterület számára fizikailag vissza kell juttatni.

112. Az adathordozók vagy mobil eszközök visszavétele az informatikai szakterület munkatársainak a feladata. A leadott adathordozót vagy mobil eszközt össze kell vetni az átadás-átvételi bizonylattal és az adatkísérő lappal, eltérés esetén jegyzőkönyvet kell felvenni és értesíteni kell az IFO vezetőjét, bv. intézetek esetében az informatikai szakterület vezetőjét, aki gondoskodik a szükséges intézkedések megtételéről.

113. Az informatikai szakterület az eszköz visszavételét követően az eljárásrend vonatkozó fejezeteinek előírásai szerint gondoskodik az adathordozók biztonságos törléséről vagy amennyiben ez nem lehetséges, a biztonságos tárolásáról, selejtezéséről és megsemmisítéséről.

114. Az adathordozó vagy mobil eszköz hibája vagy biztonsági incidens bekövetkezése esetén az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője is jogosult a visszavétel kezdeményezésére az eszközt használó személy és az érintett szervezeti egység vezetőjének, továbbá az IBF egyidejű tájékoztatásával. Biztonsági esemény esetén az IBF is kezdeményezheti a visszavételt.

115. Minden egyes kiadott adathordozóról és mobil eszközről az informatikai szakterület nyilvántartást vezet. A nyilvántartás vezetéséről az IFO Fejlesztési és Stratégiai Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője gondoskodik.

116. A nyilvántartásnak az alábbiakat kell tartalmaznia az adathordozók tekintetében:
    a) adathordozó egyedi azonosítója,
    b) adathordozó típusa,
    c) a titkosított, titkosítatlan,
    d) kiadás és visszavétel dátuma, ideje,
    e) adathordozót használó személy neve és szervezeti egysége,
    f) telephelyen kívüli használatra vonatkozóan történt igénylés esetén ennek tényét.

117. A nyilvántartásnak legalább az alábbiakat kell tartalmaznia mobil eszközre vonatkozóan:
    a) mobil eszköz egyedi azonosítója,
    b) mobil eszköz típusa,
    c) kiadás és visszavétel dátuma, ideje,
    d) mobil eszközt használó személy neve és szervezeti egysége.

118. Az adathordozók és mobil eszközök selejtezésének, megsemmisítésének tényét a nyilvántartásban is át kell vezetni.

119. A nyilvántartás vezetését és tényleges állapotnak való megfelelését az IBF ellenőrizheti. Az ellenőrzés tényét és eredményét dokumentálni kell és szükség esetén az érintettek tudomására kell hozni azt a javasolt helyesbítő intézkedésekkel együtt.

120. Az adathordozókhoz vagy mobil eszközökhöz történő hozzáférés és az adathordozókkal való műveletvégzés jogosultsága az azokra rögzített információ biztonsági kategóriájától függ, továbbá attól, hogy az adott adathordozó vagy mobil eszköz beépített-e vagy sem.

121. Az informatikai szakterület jogosultságigénylő lapok alkalmazásával meghatározza, dokumentálja és nyilvántartja az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, valamint a jogosultságok tartalmát és időtartamát. A dokumentálás elektronikus úton is történhet.

122. A beszerzett, még készletnyilvántartásban nem szereplő és használatba nem vett adathordozókat és mobil eszközöket elkülönítetten és elzártan kell tárolni. Használatba vételük a megfelelő megjelölések után történhet meg.

123. Az adathordozókat vagy mobil eszközöket a gyors hozzáférés érdekében egyedi azonosítót, a vonatkozó terjesztési korlátozásokat, kezelési figyelmeztetéseket és megfelelő biztonsági jelzéseket tartalmazó címkével kell ellátni, melyről nyilvántartást kell vezetni. A megfelelő jelölésről és címkézésről az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője gondoskodik.

124. Az azonosító megegyezik az adathordozó (USB pendrive-ok, memóriakártyák, hordozható HDD-k és SSD-k) mint tárgyi eszköz készletkezelés során alkalmazott azonosítójával, kivéve az egyszerű vagy jelöléssel való ellátásra fizikailag alkalmatlan eszközök (CD, DVD, mágnesszalag), melyek csak számszerűen kerülnek nyilvántartásba.

125. Az adathordozók vagy mobil eszközök USB porton keresztüli csatlakoztatását kontrollálni kell és ezt technikai eszközzel való kikényszerítéssel kell biztosítani. Ennek során kizárólag az engedélyezett adathordozók vagy mobil eszközök esetében szabad az USB porton keresztüli csatlakozást engedélyezni, minden más esetben tiltani kell a csatlakoztatást. Ennek megvalósításáért az IFO Infrastruktúra és Üzemeltetési Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője felel.

126. Az adathordozók vagy mobil eszközök tárolása során az adathordozó fizikai védelmének szintje el kell, hogy érje azon rendszer védelmi szintjét, amelyhez kapcsolódó adatokat tárol az adathordozó.

127. A tárolás során a gyártói előírásokat be kell tartani és a gyártó által előírt megfelelő környezeti paramétereket biztosítani kell.

128. Az adathordozók vagy mobil eszközök öregedésének következtében bekövetkező adatvesztések elkerülése érdekében az adathordozó gyártója által megadott élettartamánál hosszabb ideig tárolandó adatról másolatot kell készíteni és azt elkülönített helyen kell tárolni (másik épületben).

129. Az adathordozókat vagy mobil eszközöket úgy kell tárolni, hogy azok ne sérüljenek vagy károsodjanak.

130. Adathordozó vagy mobil eszközök más személy részére történő átadására a kiadás és visszavétel szabályai érvényesek.

131. A másodpéldányok kezelésével kapcsolatos előírásokat a mentési és archiválási eljárásrend tartalmazza.

132. Adathordozók szállítása, bv. szerv területéről történő kivitele csak a bv. szerv vezetőjének, BVOP esetében az IFO vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének engedélyével történhet. Szállítási feladatot elsősorban az informatikai szakterület munkatársai hajthatnak végre. A szállítási engedélyben meg kell határozni:
    a) eseti vagy rendszeres,
    b) az érintett adathordozók körét,
    c) a szállítás célját,
    d) földrajzi helyét (hova történik a szállítás),
    e) a szállításra jogosultak körét,
    f) az alkalmazandó fizikai és logikai (pl. titkosítási) védelmi elemeket,
    g) a dokumentálás módját (pl. jegyzőkönyv elkészítése, adathordozók nyilvántartásának vezetése).

133. A dokumentálás során legalább az alábbiakat rögzíteni kell:

a) az adathordozó egyedi azonosítója,
b) a szállító személy azonosító adatai,
c) szállítás pontos ideje (indulás, érkezés),
d) szállítással kapcsolatos egyéb események.

134. Az adathordozókat vagy mobil eszközöket szállítás közben védeni kell a jogosulatlan hozzáféréstől, módosítástól, visszaélésektől, fizikai sérülésektől.

135. Az adathordozókat vagy mobil eszközöket megfelelő tároló dobozban vagy kézitáskában kell szállítani, szükség esetén gondoskodva a nem bontható csomagolás alkalmazásáról is.

136. A mágneses adathordozó szállításakor fokozottan ügyelni kell a nyilvánvalóan erős mágneses tér (például nagyfeszültségű távvezetékek) elkerülésére.

137. Az adathordozók vagy mobil eszközök postai vagy futárszolgálat általi szállítása – az Állami Futárszolgálat kivételével – nem megengedett.

138. Adathordozó felügyelet nélkül nem hagyható.

139. Meghibásodott adathordozók vagy mobil eszközök esetén az eszköz javításra vagy cserére történő kivitele a bv. szerv területéről – még garanciális esetben is – az adatok lementését követően, az adathordozón lévő adatok visszaállíthatatlan törlése után lehetséges.

140. Titkosítási eljárást kell alkalmazni az adathordozókon vagy mobil eszközökön, ha a tárolt információk bizalmassága és sértetlensége más, egyszerűbb módon (pl. személyes őrzés) nem biztosítható.

141. A használandó kriptográfiai mechanizmusokat, titkosításra használt szoftvert az IFO vezetője jelöli ki, legalább AES 128 bites erősségű titkosítás alkalmazása kötelező.

142. Az adathordozókkal kapcsolatos eszközbeszerzéseknél figyelembe kell venni, hogy a külső használatra (is) tervezett adathordozók esetében a beszerzendő eszközökre titkosítási eljárás alkalmazható legyen (akár beépített titkosítással rendelkezzenek).

143. Az adathordozók tartalmát törölni kell, ha
a) az adathordozó tartalmára már nincs szükség,
b) az adathordozó kikerül a bv. szerv tulajdonából,
c) az adathordozó karbantartás céljából átadásra kerül külső fél számára,
d) az adathordozó újra felhasználásra kerül,
e) az adathordozó selejtezésre kerül.

144. A törlés során a bv. szervezet egységes iratkezelési szabályzatának vonatkozó előírásait is figyelembe kell venni. Az adathordozókat vagy mobil eszközöket olyan módszerek alkalmazásával kell törölni, hogy az adatok a későbbiekben ne legyenek helyreállíthatók.

145. A visszaállíthatatlan törlés a szoftveres úton történő törlés esetében ugyanazon adathordozó legalább 3-szoros felülírását jelenti, adatot nem tartalmazó véletlen

mintákkal. A visszaállíthatatlan törlést az informatikai szakterület munkatársai hajtják végre.

146. A törlést minden esetben dokumentálni kell, mely során legalább az alábbiakat rögzíteni kell:
   a) az adathordozó azonosítója,
   b) a törlés alkalmazott módszere,
   c) a törlést végző személy neve
   d) a törlés dátuma és időpontja,
   e) a törlés eredményes (sikeressége).

147. Az adathordozó vagy mobil eszköz a törlést követően más felhasználó számára munkavégzésre ismételten kiadható.

148. Az adathordozók vagy mobil eszközök selejtezése során a bv. szervezet egységes iratkezelési szabályzatának vonatkozó előírásait kell értelemszerűen alkalmazni jelen kézikönyvben foglalt kiegészítésekkel.

149. Minden olyan információ-feldolgozó eszközt ellenőrizni kell a selejtezésüket megelőzően, amely adathordozót tartalmaz, hogy az adathordozók eltávolításra kerültek-e belőle annak érdekében, hogy az adatok visszaállíthatatlanul törlésre vagy megsemmisítésre kerüljenek. Az ellenőrzésről az informatikai szakterület vezetője gondoskodik.

150. A selejtezésre szánt, illetve selejtezett adathordozókat a megsemmisítésig elkülönítetten és elzártan, az illetéktelen hozzáféréstől védve kell tárolni. A megfelelő tárolása az informatikai szakterület feladata.

151. Az adathordozók megsemmisítése során a bv. szervezet egységes iratkezelési szabályzatának vonatkozó előírásait kell értelemszerűen alkalmazni az alábbi kiegészítésekkel.

152. A megsemmisítendő adathordozókról az informatikai szakterület összesítő jegyzéket készít, amely legalább a következőket tartalmazza (adathordozónként):
   a) az adathordozó egyedi azonosítója,
   b) az adathordozó típusa,
   c) az adathordozón tárolt adatok jellege.

153. A megsemmisítését és a megsemmisítési eljárás típusát az informatikai szakterület vezetője hagyja jóvá, illetve határozza meg a jegyzék alapján.

154. Az adathordozók megsemmisítése belső ellátás keretében történik a büntetés-végrehajtási szervezet részéről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről szóló 44/2011. (III. 23.) Korm. rendelet alapján kijelölt bv. szerveknél.

155. A kijelölt bv. szervvel kötött szerződésben rögzíteni kell a titoktartási feltételeket, a megsemmisítés biztonsági követelményeit és a szerződőnek garanciát kell vállalnia az adatok visszaállíthatatlan megsemmisítésére.

156. A kijelölt bv. szervnek az adatok megsemmisítéséről jegyzőkönyvet kell készítenie és ezt eljuttatnia a megsemmisítést kérő számára az alábbiak szerint:
    a) az adathordozók egyértelmű azonosítója,
    b) a megsemmisítés alkalmazott módszere,
    c) a megsemmisítést végző neve és aláírása,
    d) a megsemmisítés dátuma, helye és időpontja,
    e) a megsemmisítés eredménye (sikeressége).

157. Mágnesszalagok: el kell távolítani a tokból, majd mechanikusan be kell zúzni, kémiai úton megsemmisíteni vagy elégetni. Az utóbbi esetben a szalagokat be kell tenni az égetőbe rövid darabokban vagy lazán betöltve jól összekeverve sokkal nagyobb mennyiségű papírhulladékkal együttesen. Nem szabad azokat az égetőbe feltekercselve vagy összepréselt blokkokban betenni, mert nem semmisülnek meg teljes mértékben.

158. Lemezek: a lemezt szabálytalan alakú darabokra kell vágni (legalább 8 darabra), a darabokat deformálni kell vagy elégetni.

159. Merevlemezek: fel kell nyitni, és el kell égetni; vagy a mágneses felületet el kell távolítani dörzspapírral vagy más durva módszerrel, vagy szét kell szedni és az adathordozót apró darabokra vágni, pl. lemezvágó ollóval.

160. Más szilárd anyagú tárolók: össze kell törni (kis darabokra) vagy el kell égetni.

Naplózási eljárásrend

161. A bv. szerveknél a biztonsági események megelőzése, kivizsgálása és nyomon követhetősége érdekében olyan elektronikus naplózási rendszert kell kialakítani, hogy utólag minden esetben meg lehessen határozni, hogy ki, mikor, honnan, milyen bizalmas adathoz, milyen célból (olvasás/létrehozás/módosítás/törlés) fért hozzá.

162. A biztonsági elemzés célja a nemkívánatos esemény bekövetkeztének megelőzéséhez szükséges információk megszerzése és kezelése, valamint az, hogy meg lehessen állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy kísérletét.

163. A naplózási rendszernek alkalmasnak kell lennie mindegyik felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására.

164. A különböző elektronikus információs rendszerek naplóállományainak egységes értelmezhetősége érdekében olyan naplózási architektúrát kell kialakítani, ami biztosítja, hogy:
    a) ahol csak technikailag lehetséges, a naplózás szerveroldalon történjen,
    b) automatikus mechanizmus gondoskodjon az egyes rendszerek, eszközök rendszerórájának szinkronizálásáról.

165. A naplóbejegyzéseket védeni kell az illetéktelen hozzáféréstől. Elektronikus naplóknál ezt megfelelő jogosultsági beállításokkal kell biztosítani, azokhoz csak a naplózási feladatokkal, illetve a napló adatok ellenőrzésével, vizsgálatával megbízott, arra jogosult személyek férhessenek hozzá.

166. Az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének felelőssége, hogy az informatikai rendszer biztosítsa az események naplózását, a naplóesemények kiértékelhető formátumban jelenjenek meg és az elemző részére a naplóelemzés idejére teljes körűen elérhetővé váljanak.

167. Mind a privilegizált felhasználói tevékenységet, mind a biztonsági eseményeket nyomon kell követni az egyes elektronikus információs rendszerekben.

168. Gondoskodni kell a naplóállományok rendszeres mentéséről vagy redundáns storage-on való tárolásáról és rendszeres felülvizsgálatáról, valamint arról, hogy a privilegizált felhasználók se tudjanak nyomtalanul módosítani a naplózási beállításokon.

169. A naplóadatok törlésére, megsemmisítésére a logikai törlésre vonatkozó szabályokat értelemszerűen kell alkalmazni.

170. A naplózó rendszernek az alábbi tevékenységeket kell nyomon követnie:
    a) minden felhasználó vonatkozásában a felhasználók authentikációs tevékenysége (bejelentkezés, kijelentkezés, jelszómódosítás, sikertelen bejelentkezési kísérlet),
    b) az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben,
    c) a privilegizált felhasználók a rendszer bármely rétegébe történő be-és kijelentkezése,
    d) a privilegizált felhasználók tevékenysége a rendszer bármely rétegében,
    e) a felhasználói jogosultságok módosítása,
    f) konfigurációs beállítások módosítása,
    g) rendszeresemények, esetleges hibák.

171. A naplózó rendszernek az alábbi típusú események rögzítésére kell kiterjedniük:
    a) rendszerindításokat, -leállításokat,
    b) rendszerriasztásokat, meghibásodási jelentéseket,
    c) a rendszerben fellépő hibákat,
    d) felhasználók felvételét, törlését, felfüggesztését, jogosultságának módosítását,
    e) naplózási funkciók indítását és leállítását,
    f) naplóállomány létrehozását, törlését (külön jegyzőkönyvben rögzítve),
    g) a rendszerdátum, -idő megváltoztatását,
    h) szoftverkonfiguráció megváltozását,
    i) nyilvános hálózaton keresztüli kapcsolatnál (pl. távoli karbantartás és segítségnyújtás) létrehozást és bontást; ellenoldali fél adatait; forgalom jellege; továbbított vagy fogadott állomány neveit, elérési útvonalát,
    j) tűzfal/IPS/terheléselosztó rendszereken átmenő forgalmat,
    k) programleállásokat,
    l) az azonosítási és a hitelesítési mechanizmus használatát,
    m) személyi műveleteket, amelyek a rendszer biztonságát érintik.

172. Az esemény típusának megfelelően az általános feldolgozási eseményt az eseménynaplóban, a biztonsággal összefüggő eseményeket pedig a biztonsági naplóban kell rögzíteni.

173. Az egyes rendszerek naplózásának kialakításába be kell vonni naplózással érintett rendszert használó szakterületet is annak érdekében, hogy meghatározásra kerüljenek

azok a többletismeretek, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek.

174. Az IFO Infrastruktúra és Üzemeltetési Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője, valamint az IBF a naplózási tevékenységet bármikor megvizsgálhatja annak megállapítása érdekében, hogy alkalmas-e a biztonsági események kivizsgálására, javaslatokat tehetnek a naplózási rendszer átalakítására.

175. Az eltérő megőrzési idő a személyes adatokat kezelő rendszerek (EIR-alapnyilvántartás szerint) vonatkozásában az információs önrendelkezési jogról szóló törvény rendelkezései alapján a napló állományok megőrzési ideje az adatállományok törlését követő 10 év.

176. A naplózási rendszerben rögzítésre kerülő adatok minimuma:
   a) felhasználó azonosítója,
   b) számítógép azonosítója vagy pontos helye,
   c) a használt hálózati cím,
   d) a bekövetkezett esemény pontos dátuma és ideje (rögzíteni, hogy a naplózás UTC vagy helyi idő alapján történik),
   e) a bekövetkezett esemény részletei,
   f) a használt szoftver/alkalmazás.

177. A naplók tárkapacitását a bv. szerv javaslata alapján a BVOP IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének kötelessége megtervezni, figyelembevéve, hogy a naplók általános megőrzési ideje 30 nap.

178. Az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének kötelessége a kapacitás-felhasználás nyomon követése, ami alapján a későbbiekben a kapacitásigény módosítható.

179. A napló tárkapacitás figyelését a rendszerek felügyeleti tevékenységébe kell beépíteni.

180. A naplózást úgy kell beállítani, hogy amennyiben a naplóállomány eléri a kritikus mennyiséget, úgy automatikusan kerüljön archiválásra a napló, ezzel biztosítva a naplóbejegyzések felülírásának megakadályozását. Ezen túlmenően szükséges, hogy a rendszer automatikus értesítést küldjön az informatikai szakterületnek, amennyiben tárkapacitás növeléséről kell gondoskodni.

181. Az informatikai rendszerben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén az automatikusan riasztást küldjön az informatikai szakterületnek.

182. A naplózási hiba javításáról az IFO Infrastruktúra és Üzemeltetési Osztály vezetője, bv. intézetek esetében az informatikai szakterület vezetője haladéktalanul gondoskodik.

183. A naplóvizsgálat célja a naplóbejegyzések vizsgálata a nem megfelelő vagy szokatlan jelenségek, ismétlődések, folyamatok feltárása érdekében.

184. Az informatikai rendszerben az eseménynaplókat az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének

havonta teljes egészében vagy riasztás esetén az érintett naplófájlokat haladéktalanul át kell vizsgálni és a mentésükről gondoskodni kell.

185. A biztonsági napló adatait rendszeresen, de legalább havonta egy alkalommal ellenőrizni, értékelni és archiválni kell, mely során meg kell határozni, hogy mely eseményeket kell jegyzőkönyvezni, melyek azok az események, amelyek szankciókat vonnak maguk után, és mik ezek a szankciók. Az ellenőrzést a BVOP IFO Infrastruktúra és Üzemeltetési Osztályának vezetője, bv. intézetek esetében az informatikai szakterület vezetője hajtja végre.

186. A naplóvizsgálatról és annak eredményéről a bv. szervezet jelentési rendjére vonatkozó általános szabályok szerint kell jelentést készíteni.

187. Az informatikai rendszerben valamennyi naplóbejegyzést időbélyeggel kell ellátni, melyhez a rendszerórát kell alapul venni. A naplókban található időbélyegek helyi/UTC időket tartalmaznak.

188. Az informatikai rendszert úgy kell kialakítani, hogy hálózati időszinkron protokoll segítségével szinkronizálja a rendszerórákat az egyezményes koordinált világidőhöz. Az üzemeltető hálózatában a gépeket a rendelkezésre álló belső forráshoz (BM time szerver) kell szinkronizálni, a további elemek pedig ehhez szinkronizálnak (fa topológia szerint).

189. Hatósági előírás alapján a tolerálható időeltérés mértéke 1 tizedmásodperc. Az informatikai szakterület feladata, hogy olyan rendszer kiépítéséről gondoskodjon, amelyben nincs két olyan elem, melyek között tizedmásodpercnél nagyobb időeltérés alakulhat ki.

190. Az IFO-nak az informatikai rendszert a külön eljárásrendben foglalt logikai védelmi intézkedések felhasználásával központilag úgy kell kialakítani, hogy a naplóinformációk védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

191. A naplók általános megőrzési ideje 30 nap, ennél hosszabb megőrzési időt kizárólag jogszabályi előírás alapján lehet meghatározni.

192. Az eltérő megőrzési időket a 7. melléklet határozza meg.

193. Az eseménynaplók és az azok kezeléséhez kapcsolódó biztonsági naplók tárolását a következő szempontok figyelembe vételével kell megoldani:
    a) a naplóadatokat időbélyegzővel kell ellátni,
    b) a naplóadatoknak sértetlenül rendelkezésre kell állniuk időrendben a megőrzési időn belül,
    c) biztosítani kell, hogy az adatokban keletkezésük után változtatást ne lehessen végrehajtani,
    d) az adatok nem juthatnak illetéktelenek kezébe.

194. A naplóinformációk mentését be kell vonni az informatikai rendszer mentési rendszerébe. A mentési folyamat kialakítása és integrálása az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének felelőssége. A mentéseket a napló tárkapacitással összhangban úgy kell kialakítani, hogy a naplóbejegyzések ne vesszenek el.

195. Az informatikai rendszert fel kell készíteni a következő naplózással kapcsolatos követelmények teljesítésére:
    a) biztosítania kell a naplóbejegyzések előállítási lehetőségét a Naplóbejegyzések tartalma pontban meghatározott naplózható eseményekre,
    b) lehetővé kell tennie az IFO vezetőjének és szükség szerint az IBF-nek is annak kiválasztását, hogy mely naplózható események legyenek naplózva az informatikai rendszer egyes elemeire,
    c) naplóbejegyzéseket kell előállítania a Naplózandó események pontban meghatározottak szerinti eseményekre a Naplóbejegyzések tartalma pontban meghatározott szabályok szerint.

196. A naplógeneráló rendszer üzemben tartása az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének a kötelezettsége.

A mentéssel kapcsolatos általános rendelkezések

197. A bv. szerv mentési rendszerét az üzletmenet folytonosságának szempontjából fontos elektronikus adatok folyamatos rendelkezésre állásának biztosítására figyelemmel kell kialakítani és működtetni, melyről az informatikai szakterület vezetője gondoskodik.

198. A mentési rend célja, hogy kialakítsa azokat az eljárásokat, feladatokat és felelősségeket, amelyekkel biztosítani lehet az üzleti szempontból „fontos”, vagy annál magasabb adatosztályba sorolt adatok előírt rendelkezésre állását.

199. Az elektronikusan tárolt adatok védelme, a biztonság növelése, a károk megelőzése, elhárítása és csökkentése érdekében a bv. szervezet mentési és archiválási eljárásrendet működtet.

200. Az informatikai rendszerekben kezelt, feldolgozott, tárolt adatok rendelkezésre állását azok rendszeres és indokolt esetben soron kívüli mentésével az informatikai szakterület biztosítja.

201. A bv. szervezet által használt sajátos, szakfeladatot támogató, külön függelékben meghatározott rendszerek adatbázisai esetében az informatikai szakterület gondoskodik az ott meghatározott automatikus mentési gyakoriságról.

202. A bv. szervezet által használt működéstámogató általános rendszerek esetében az informatikai szakterületi napi, heti, illetve havi automatikus inkrementális mentésről gondoskodik, biztosítva, hogy a mentés eredményét az adott rendszer tárolja.

203. A bv. szervezet által használt valamennyi rendszer esetében az informatikai szakterület mágnesszalagos adattárolóra, bv. intézetek esetében külső HDD-re havonta egy alkalommal rendszer szintű teljes mentést készít, amelynek elkülönített és biztonságos off-site tárolásáról gondoskodik.

204. A bv. szervezet vezetője kijelöl egy biztonsági tárolási helyszínt (továbbiakban biztonsági tárolási helyszín), ahol az elektronikus információs rendszer mentéseinek másodlatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja. A

biztonsági tárolási helyszínnek el kell különülnie az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

205. Minden mentésnek biztosítani kell az adatok kezeléséhez szükséges szoftverkörnyezet következetes helyreállíthatóságát (operációs rendszer, adatbázis-kezelő, stb.)

206. A mentési rendszert úgy kell kialakítani, hogy
   a) biztosítsa minden olyan adat mentését, amely az auditálás, ellenőrzés eszköze lehet (naplófájlok, riportok, stb.),
   b) minden olyan eszköz konfigurációja mentésre kerüljön, amely részt adat kezelésében (tárolásában, továbbításában (pl. hálózati aktív eszközök),
   c) alkalmas legyen olyan környezet helyreállítására, mely lehetővé teszi valamely igazolható állapothoz való visszatérést,
   d) a bv. szerv szakmai működése szempontjából alapvető fontosságú sajátos rendszerek mentése legalább két példányban készüljön, melyeket elkülönítetten kell tárolni.

207. A szerverek mentésére vonatkozó adatokat a 8. melléklet a következő elemekkel tartalmazza:
   a) a mentések típusát (központi, helyi),
   b) a mentések mértékét (teljes vagy inkrementális – kumulatív vagy differenciális),
   c) a mentést végrehajtó szervezeti egység megnevezését,
   d) a mentések gyakoriságát.

208. A mentett adatokat a mentési eljárás sikeres lefutásától függetlenül, a vonatkozó mellékletben meghatározott tevékenységek érvényesülését valamennyi mentési feladatra vonatkozóan szúrópróba-szerűen, de legalább félévente a BVOP IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője ellenőrzi.

209. Az előző pont szerinti ellenőrzés lefolytatása kiterjed
   a) a mentett állomány véletlenszerű kiválasztására,
   b) a kiválasztott állomány átmeneti helyre történő visszatöltésére,
   c) a mentett állományok helyreállíthatóságának vizsgálatára,
   d) teszt elvégzésének dokumentálására.

210. A mentések végrehajtásának elektronikus mentési naplóban (automatikus vagy egyedileg vezetett) való rögzítéséről a bv. szerv informatikai szakterületének vezetője gondoskodik.

211. A mentési napló minimálisan tartalmazza:
   a) a mentés kezdő és záró időpontját,
   b) a mentendő és mentett állomány elérési útját,
   c) a mentés megvalósulásának eredményét.

Archiválás

212. Az archiválás során az adatok a rendszerből kikerülnek és azok csak adathordozón léteznek tovább.

213. A bv. szervezet szakmai működése szempontjából alapvető fontosságú sajátos rendszerek havi archiválásáról az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője gondoskodik.

214. A bv. szerv általános működését támogató rendszerekben kezelt, feldolgozott, tárolt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell.

215. Az archivált adatállományokat tároló adathordozók ellenőrzéséről az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője háromévente dokumentáltan – jegyzőkönyv felvételével – gondoskodik.

216. Az archivált adatállományokat tároló adathordozók ellenőrzése kiterjed:
   a) az adathordozó sértetlenségére és további alkalmazhatóságára,
   b) a tárolt adatállomány sértetlenségéről és rendelkezésre állásáról.

Adattrezor archiválás

217. A bv. szervezet szakmai működése szempontjából alapvető fontosságú sajátos rendszerek mentett adatainak adattrezorba történő havi továbbítására – *az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól* szóló 2015. évi CCXXII. törvény 2. § (1) bekezdés, illetve 25. § (4a) bekezdés rendelkezéseire figyelemmel – az IFO vezetője gondoskodik.

218. Az adattrezor archiválással kapcsolatos előírásokat a *Büntetés-végrehajtás Országos Parancsnokának a FŐNIX rendszer archiválási rendjéről* szóló 12/2018. (III. 5.) OP szakutasítása tartalmazza.

219. A bv. szerv informatikai szakterület vezetője felelős:
   a) a mentési, archiválási rend rendszeres ellenőrzéséért,
   b) a mentési rendet érintő változások követéséért, illetve a mentési rendről szóló dokumentációk felülvizsgálatáért,
   c) mentési feladatokkal megbízott rendszergazda által jelentett incidensek kezelésére vonatkozó intézkedések foganatosításáért, illetve szükség esetén a kezeléshez szükséges erő-források biztosításáért,
   d) a helyi mentések visszatöltéssel történő ellenőrzéséért,
   e) a helyi archívumban elhelyezett médiák rendszeres ellenőrzéséért,
   f) a helyi mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások ellenőrzéséért,
   g) a kezelésére bízott informatikai rendszerben tárolt elektronikus adatok mentésének, archiválásának rendszeres, előírásszerű végrehajtásáért,
   h) a mentések, archiválások végrehajtása során feltárt incidensek jelentéséért, illetve ebben a dokumentumban meghatározott követelmények alapján az incidensek kezeléséért,
   i) a mentések visszatöltéssel történő ellenőrzések végrehajtásáért,
   j) az archívumban elhelyezett médiák rendszeres ellenőrzéséért, időszakonként történő átcsévéléséért, vagy átmásolásáért,
   k) a mentéssel, archiválással, illetve visszatöltéssel kapcsolatos dokumentálások elvégzéséért.

IV. ÜZLETMENET-FOLYTONOSSÁGI ELJÁRÁSREND

220. Az üzletmenet folytonossági eljárásrend célja, hogy a bv. szerv informatikai környezete működésének folytonossága fenntartása érdekében megfelelő iránymutatást, segítséget

nyújtson valamely, működéshez szükséges informatikai, infokommunikációs erőforrás sérülése, kiesése esetén, meghatározva a bv. szerv informatikai környezetének felfüggesztését okozó események előfordulásakor alkalmazandó teendőket, az erőforrások pótlásának rendjét, illetve az üzletmenet folytonosság biztosításában közreműködők, értesítendők elérhetőségét.

Üzletmenet-folytonosság fenntartása

221. Valamennyi rendszer esetében a BVOP IFO vezetője meghatározza a rendelkezésre állási követelményeket.

222. A rendszerek erőforrásainak és folyamatainak üzemeltetéséért, fenntartásáért felelős informatikai szakterületi vezető a folyamatosan beérkező információk alapján megvizsgálja, hogy:
   a) az esemény mely erőforrások kiesését eredményezte,
   b) a kialakult helyzet kapcsán milyen további erőforrások kiesésével szükséges számolni,
   c) az előzetes prognózis alapján a kieső erőforrások helyreállítása mennyi időt vesz igénybe,
   d) a kiesett folyamatok milyen minőségben állíthatók helyre;

223. Az üzletmenet-folytonosság alapvető célja, hogy a bv. szervezet folyamatait támogató informatikai erőforrások a rendelkezésre álló üzemidőben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek annak érdekében, hogy az üzleti folyamatok zavarai által okozott közvetlen és közvetett károk minimálisak legyenek.

224. A működés-folytonossági tervnek részletesen meg kell határoznia a kívánt üzletmenet-folytonosság fenntartásához szükséges megelőző, helyettesítő, illetve visszaállító intézkedések megvalósításához szükséges feltételeket, szervezeti és szervezési lépéseket és a megvalósítás módját.

225. A tervezés egyik lényeges eleme a kiesési kockázatok elemzése, amelynek során mérlegelni kell az okozott kár nagyságát és az üzemzavari események, a veszélyhelyzetek bekövetkezésének gyakoriságát.

226. A kieső erőforrások ismeretében az informatikai szakterület vezetője megvizsgálja, hogy mely folyamatok, mely területeken álltak meg és a bv. szervezet ügyeleti tevékenységéről és a jelentések rendjéről szóló utasításban meghatározottak szerint megteszi a szükséges intézkedéseket.

Működés-folytonosság irányításának területei

227. A kritikus informatikai folyamatok védelme érdekében a meghibásodások és a rendellenességek elhárítása során:

a) a működés-folytonosságának fenntartását szolgáló eljárás a megelőző és helyreállítást vezérlő eljárások (működés-folytonossági terv, katasztrófa-elhárítási terv) együttes alkalmazásával mérsékelni kell a különböző rendellenességek és az elektronikus információs rendszer meghibásodása által okozott fennakadásokat, melyeket okozhatnak többek között természeti katasztrófák, balesetek, berendezésekben keletkezett hibák, vagy szándékos cselekmények;
b) elemezni kell a meghibásodások, fennakadások és üzemzavarok következményeit;
c) a működés-folytonosságának irányítása ki kell, hogy terjedjen a kockázatok azonosítására és csökkentésére alkalmas ellenőrző eszközökre, a kárt okozó események következményeinek korlátozására, valamint a lényeges tevékenységek időben történő újraindítására;
d) azonosítani kell a kritikus működési folyamatokat magában foglaló minden vagyontárgyat;
e) valószínűsíteni kell, hogy az informatikai biztonsági incidensek milyen megszakadásokat okozhatnak;
f) meg kell határozni a szükséges kiegészítő megelőző és mérséklő intézkedéseket;
g) biztosítani kell a személyzet biztonságát és az információfeldolgozó berendezések és a bv. szervezet tulajdonának védelmét;
h) meg kell fogalmazni és dokumentálni kell a működésfolytonosságra vonatkozó azon terveket, amelyek az informatikai biztonsági követelményekkel foglalkoznak;
i) rendszeresen felül kell vizsgálni és frissíteni kell a kidolgozott terveket és folyamatokat;
j) biztosítani kell, hogy a működés folytonosságának az irányítása beépítésre kerüljön a szervezet folyamataiba.

Működés-folytonosság irányítás folyamata

228. A működés-folytonosság tervezését – az azonosított elektronikus információs rendszerek biztonsági osztályba sorolása alapján – alapvetően projektszerűen kell megvalósítani.
229. A működés-folytonosság biztosítási folyamatának kialakítása során figyelembe kell venni:
    a) az informatikai biztonsági kockázatok felmérésének eredményét és a bekövetkezési valószínűséget,
    b) a folytonosság megszakadásából (megszakításából) következő hatások, következmények felmérésének és elemzésének eredményeit,
    c) a működés-folytonossági tervekben meghatározottakat.

Működés-folytonosság és hatásvizsgálat

230. A megfelelő működés-folytonosság az informatikai rendszer folyamatos üzemi működésének az a szintje, amely során a kiesés kockázatának szintje a bv. szervek számára még elviselhető.

231. Az elviselhetőség határát a folyamat – támogatás szempontjából kritikus rendszereinek – egy meghatározott (maximált) kiesési ideje határozza meg.

232. A működés-folytonosság megfelelő szintjét a szükséges megelőző, illetve (a kiesés bekövetkezése után) visszaállító intézkedésekkel kell biztosítani, amely intézkedéseket előre meg kell tervezni (működés-folytonossági terv, katasztrófa-elhárítási terv).

233. A működés-folytonosság tervezés eredménye a működés-folytonossági terv, amely részletesen meghatározza a kívánt működés-folytonosság fenntartásához szükséges feltételeket, szervezeti és szervezési lépéseket, valamint szabályozza a megvalósítás módját.

Feladat-, felelősség- és hatáskörök a működés-folytonosság területén

234. Minden rendszer esetében a működés-folytonossági eljárásrendek aktualizált állapotban tartása az informatikai szakterület vezetőjének a felelőssége.

235. A működés-folytonossági és katasztrófa-elhárítási feladatok ellátásáért az IFO vezetője felelős.

236. Az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője gondoskodik a rendszer beszerzése esetén a rendszer tartalmának és egyéb paramétereinek egyeztetése mellett a működés-folytonosságra és katasztrófa-elhárításra vonatkozó követelmények meghatározásáról.

237. Az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője jogosult és köteles az üzletmenet-folytonosság megfelelőségét rendszeres és dokumentált szakmai tesztek során ellenőrizni.

A működés-folytonossági terv

238. A bv. szervezet elektronikus információs rendszereinek működés-folytonosságának biztosítása érdekében az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője megelőzési tervet és visszaállítási tervet készít.

239. A megelőzési terv tartalmazza mindazon rendelkezéseket, amelyek az informatikai rendszer folytonos üzemét valamilyen módon veszélyeztető tényezőkkel kapcsolatosak;

240. A megelőzési terv kiterjed:
   a) a rendszer megbízható üzemeltetésére és az üzemeltetésére vonatkozó intézkedésekre;
   b) a rendszer kritikus elemeinek üzemi és katasztrófa tartalék megoldásaira és ezek üzemkészségét biztosító intézkedésekre;
   c) a rendszer üzemét biztosító környezeti rendszerek karbantartási, illetve az ezekkel kapcsolatos biztonsági intézkedésekre;
   d) az üzemeltetési dokumentáció és dokumentumok rendszerezett és biztonságos tárolására;
   e) az adathordozók rendszerezett és biztonságos tárolására;
   f) az üzemeltető, a karbantartó és a kárelhárító személyzet rendelkezésre állását és bevethetőségét biztosító intézkedésekre;
   g) a külső szervizre, a tartalékképzési megoldásokra vonatkozó, és a biztosítási szerződé-sekkel kapcsolatos intézkedésekre;
   h) a mentési tervre, amely meghatározza a mentési rendszer generációit és hierarchiáját;

i) a rendszer konfigurációjában, az üzemelő szoftverben megvalósítandó változások szabályozott kivitelezésére, valamint a szoftverfejlesztések elkülönített kivitelezésére és a fejlesztett szoftverek rendszerbe történő integrálására vonatkozó legfontosabb intézkedésekre;
j) vírusvédelmi és vírusmenedzsment intézkedésekre;
k) a megelőzésben fontos szerepet játszó, az alkalmazói rendszerek használatára történő rendszeres oktatásra, illetve az informatikai biztonság olyan szintű oktatására, amely kiterjed a rendszerekben kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának megőrzése érdekében betartandó szabályokra és az érvényesítendő védelmi intézkedésekre;
l) tesztelési és tréning tervre, amely meghatározza a tesztelés formáit.

241. A visszaállítási terv alapvető célja az üzemzavari vagy katasztrófa események bekövetkezése esetén az esemény azonosítása, a szükséges emberi és eszköz erőforrások haladéktalan mozgósítása, valamint, hogy a visszaállítás a lehető leggyorsabban és szervezetten történjen meg a tervben meghatározott utasítások szerint.

242. A visszaállítási terv tartalmazza:
a) a visszaállítási terv célját és használatát;
b) az üzemzavari és katasztrófa események meghatározását;
c) az események bekövetkezési és kezelési időszakait;
d) az eseménykezelő team összetételét, feladatait és hatáskörét;
e) visszaállítási intézkedéseket a következő lépésekre: azonnali válasz (riadóterv), futtató környezet helyreállítás, funkcionális helyreállítás, üzemeltetési szintű helyreállítás, áttelepülés (katasztrófa esetén), normalizáció az áttelepülés után.

A működés-folytonossági tervek vizsgálata, karbantartása

243. A tervek tesztelését egy szimulált esemény bekövetkezésével és a terv szerinti visszaállítással kell megvalósítani. Ennek keretében az eseménykezelő szervezet, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

244. A teszt értékelése során a működés folytonosságát biztosító terveket módosítani, aktualizálni kell, és gondoskodni kell azok egymáshoz való illesztéséről. A terveket a folytonosan változó helyzethez, körülményekhez (személyzet, stratégia, infrastruktúra), követelményekhez (szabályok, kockázatok) is hozzá kell igazítani.

Oktatás, tréning és tesztelés

245. Az oktatás célja a működés-folytonosság jelentőségének tudatosítása, a működés-folytonosság tervezés alapismereteinek átadása, a megelőzési és visszaállítási tervben foglaltak megismerése és elsajátítása.

246. A működés-folytonossági terv tesztelése és tréningje akkor válik elindíthatóvá, ha a szervezet által a működés-folytonossági terv készítési fázisa végén elfogadott intézkedési tervben foglaltak olyan szinten megvalósultak, hogy a működés-folytonossági terv tesztje és tréningje meghatározott üzemzavari/katasztrófa eseményre kivitelezhető.

247. A működés-folytonossági terv tesztje szimulált esemény bekövetkezésével és a terv szerinti visszaállítással kerül megvalósításra, amelynek keretében az eseménykezelő

team, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

Hibabejelentés

248. A napi normális üzemviteltől eltérő esemény bekövetkezése esetén (az eszköz eddig szokatlan hangot ad, szagot áraszt, kigyullad vagy füstöl, szikrázik stb.) a felhasználó köteles az informatikai végponti eszközt áramtalanítani, vagy a lehetőségek szerint szabályosan leállítani. Köteles minden olyan tőle elvárható intézkedést megtenni, amely biztosítja, hogy az esemény által okozott rendkívüli, vagy veszélyhelyzet nem ölt ellenőrizhetetlen méretet. A hibaesemény kezelése során a felhasználó köteles betartani a tűzvédelmi és munkavédelmi szabályokat.

249. Hibaesemény bekövetkezésekor az azt észlelő személy köteles a hibát lokalizálni, a hibaeseményt és körülményeit rögzíteni, a kieső szolgáltatás, vagy eszköz pótlására intézkedni, vagy az erre vonatkozó intézkedést kezdeményezni. Ezt követően köteles a jelentési kötelezettségének a meghatározott módon eleget tenni.

250. A hibaesemény ún. második szintű support tevékenységét az IFO szakértői látják el, igénybevételét az infrastruktúra rendszergazda, illetve a szakterület vezetője kezdeményezheti. Support szerződés hiányában, a külső szakértelem (harmadik szintű support) igénybevételét kizárólag az IFO vezetője engedélyezheti. Support szerződés hatálya alatt, az abban meghatározott eljárási rendet kell követni.

251. A hibaeseményeket a helyi informatikai szervezeti egység köteles nyilvántartásba venni a hibaesemény releváns körülményeinek nyilvántartásával. Ennek érdekében a hibabejelentésnek az alábbi adatokat minimálisan tartalmaznia kell:
    a) a hiba bekövetkezésének pontos idejét, helyszínét és helyét,
    b) a hibát észlelő személy azonosítását biztosító adatokat,
    c) a hibabejelentést végző személy azonosítását biztosító adatokat,
    d) szükség esetén a viszont értesítéshez, kiszálláshoz szükséges pontos adatokat (postai cím, távbeszélő- vagy telefax készülék száma stb.),
    e) hiba által érintett eszközt, szolgáltatást,
    f) a hiba jelenséget, azonosított hiba esetén a hibakódot és a teljes hibaszöveget,
    g) a hiba bekövetkezésének és megjelenésének körülményeit,
    h) a hiba kijavítása érdekében eddig tett javítási lépéseket, eljárásokat,
    i) az azonnali hibajavítás megkezdésére vonatkozó igényt, vagy a kiváltásra, pótlásra történt intézkedés tényét és formáját,
    j) második vagy harmadik típusú support igénybevételének szükségességét, tényét.

252. A szolgáltatási szerződésben vagy a rendszerdokumentációban rögzített hibabejelentő adattartalma eltérhet az itt meghatározott adatoktól.

253. Az informatikai ügyeleti és/vagy készenléti rendszer működésének hiányában a felhasználó hivatali munkaidőben a hiba kijavítására segítséget kérhet az informatikai szakterülettől, amely saját erő-eszköz számvetése alapján köteles együttműködni a hiba lokalizálásában, kijavításában vagy a kijavításhoz szükséges intézkedések és jelentések megtételében. A hivatali munkaidő kereteit meghaladó hibakezelést a bv. szerv ügyeleti szolgálata saját informatikai szervezeti egységének vezetője útján kezdeményezi.

254. Az alkalmazás- vagy infrastruktúra rendszergazda által észlelt, az informatikai rendszerre vonatkozó hibaeseményeket, a hiba körülményeinek pontos dokumentálásával a HelpDesk nyilvántartás hiányában a szerver gépkönyvében kell rögzíteni.

255. Az alkalmazás- vagy infrastruktúra rendszergazda által észlelt, az informatikai rendszerre vonatkozó hibaeseményeket a helpdesk@bv.gov.hu e-mail címen kell bejelenteni. A beérkező hibajelentést tárgyától függően a megfelelő informatikai szakterület (Infrastruktúra és Üzemeltetési Osztály, Fejlesztési és Stratégiai Osztály) felé továbbítják.

256. A rendszergazda köteles a hiba kijavítását legjobb tudása szerint elvégezni, tudáshiány esetén köteles segítséget igénybe venni. Kapcsolódó szolgáltatások esetén köteles a társszervet a hiba tényéről tájékoztatni. Csatlakozó infrastrukturális hiba esetén köteles a hiba bekövetkezésének tényét haladéktalanul jelezni a külső szerv, vagy szolgáltató felé az együttműködési megállapodásban vagy szolgáltatási szerződésben rögzített forma szerint. A géptermi szerverek hibája esetén köteles a hiba kijavíthatósága érdekében a tőle elvárható minden intézkedést megtenni, jogosult az alrendszer rendszergazdájával konzultálni, javaslatot tenni a hiba kijavítására teendő intézkedések megtételére.

257. Az alkalmazás- vagy infrastruktúra rendszergazda az informatikai infrastruktúra hibájáról szóló jelzést köteles kivizsgálni és annak megalapozottságáról vagy megalapozatlanságáról a bejelentőt viszont tájékoztatni.

258. A felhasználó hibajavítás okán sem jogosult a végponti eszköz, perifériája vagy alkalmazása tekintetében módosításokat, konfigurációváltoztatásokat, rendszerhangolást végezni. Amennyiben a hiba szándékos felhasználói tevékenységből, vagy mulasztásból történt, úgy a helyi informatikai szervezeti egység köteles hibajegyzőkönyvet felvenni, majd a hibát elhárítani. A jegyzőkönyvet a felhasználóval (munkahelyi vezetőjével) is alá kell íratni, addig a hiba javítása nem kezdhető meg.

Az üzemszünettel kapcsolatos elhárítási feladatok

259. Az informatikai incidensek szintjei a katasztrofális (informatikai katasztrófán kívül):
   a) jelentős, ha az incidens hatására informatikai veszélyhelyzet áll elő,
   b) nem jelentős, ha az incidens hatására informatikai katasztrófahelyzet és informatikai vészhelyzet sem áll elő.

260. Informatikai üzemeltetési probléma, ha nem jelentős informatikai incidens következtében előálló olyan állapot, amely esetén az incidens hatására bekövetkezett hiba kijavítása a mindennapi üzemeltetési keretek között végrehajtható. Elhárításakor az üzemeltetésre vonatkozó általános szabályok az irányadók.

261. Az üzemszünet olyan üzemzavar vagy előre tervezett leállítás, amely nem teszi lehetővé a kommunikációs hálózat vagy a rendszer(ek) üzemszerű működését.

262. Feldolgozási rendek:
   a) teljes üzemszüneti feldolgozási rend: a kommunikációs hálózat és/vagy a működési tevékenységet támogató valamely rendszer valamennyi alrendszerének üzemszerű működésének hiányában alkalmazott eljárás,

b) részleges üzemszüneti feldolgozási rend: a kommunikációs hálózat hiánya vagy a működési tevékenységet támogató valamely rendszer egyes alrendszere(inek) üzemszerű működésének hiánya következtében alkalmazott eljárás,
c) tartalék megoldás: helyi üzemzavar hiányában alkalmazott eljárás, melynek során az üzemszerű adatfeldolgozás más feldolgozó, amely a feldolgozó helyszínén üzemszerűen elvégezhető.

263. Az üzemszünet időtartamának kezdete a bv. szervezet üzemszünet esetében az az időpont, amikor az elrendelő a közlést megteszi.

264. Az üzemszünet időtartamának vége az az időpont, amelyet a bv. szervezet üzemszünet esetében valamennyi felhasználóval közölt.

265. Központi üzemszünet olyan üzemzavar, vagy előre tervezett leállítás, mely minden felhasználó számára meggátolja a kommunikációs hálózat vagy a rendszer(ek) üzemszerű működését.

266. Helyi üzemszünet olyan üzemzavar vagy előre tervezett leállítás, mely meghatározott helyhez tartozó felhasználók számára gátolja meg a kommunikációs hálózat vagy a rendszerek üzemszerű működését.

267. Manuális naplók, nyilvántartások a bv. szervezet valamely rendszer által alkalmazott gépi naplók, nyilvántartások manuális vezetésére a rendszerek által előre kiadott naplók, nyilvántartások vagy ezek helyettesítésére kialakított naplók, nyilvántartások.

Üzemszüneti feldolgozási rend bevezetésének elrendelése és visszavonása

268. A működési tevékenységet támogató valamely rendszer központi üzemzavara esetén a következők szerint kell eljárni:
a) Abban az esetben, ha működési tevékenységet támogató valamely rendszer központi üzemzavara következtében a rendszer használata munkaidőben előreláthatóan négy órát meghaladóan nem lehetséges, szükségessé válik a teljes vagy részleges üzemszüneti feldolgozási rend központilag elrendelt bevezetése. A speciális eseteket az egyes feladatokhoz tartozó üzemszüneti feldolgozási rendekben kell meghatározni. A négy órára vonatkozó előírástól jogszabályi előírás alapján az egyes rendszerek tekintetében el lehet térni.
b) Az üzemzavar észlelését/megállapítását követően az IFO Infrastruktúra és Üzemeltetési Osztály vezetőjének, bv. intézetek esetében az informatikai szakterület vezetőjének vizsgálnia kell a rendszer használhatóságát, melynek eredményéről soron kívül telefonon és e-mailben értesítenie kell az üzemszüneti feldolgozási rend bevezetéséért felelős személyt.
c) Teljes üzemszüneti feldolgozási rend központi bevezetését kell meghatározni abban az esetben, ha az érintett rendszerben központi üzemzavar következett be.
d) Részleges üzemszüneti feldolgozási rend központi bevezetését kell meghatározni abban az esetben, ha az érintett rendszer valamely alrendszere vagy egyes alrendszerei vonatkozásában központi üzemzavar következett be.
e) A teljes vagy részleges üzemszüneti feldolgozási rend bevezetését az IFO vezetője, bv. intézetek esetében az intézet parancsnoka rendeli el.

269. A felhasználók részére küldendő email üzenetek fenti okok alapján legalább az alábbi adatokat kell tartalmaznia:
   a) az üzemszünet elrendelőjének nevét, beosztását,
   b) az üzemszüneti feldolgozási rend bevezetésének kezdő időpontját (és, hónap, nap, óra, perc),
   c) a rendszerek megnevezését melynél az üzemzavar bekövetkezett,
   d) jelen kézikönyv adott feladatokhoz tartozó rendelkezésekre történő hivatkozást, amelyet alkalmazni kell az üzemszüneti feldolgozási rend időtartama alatt,
   e) az üzemszerű működés helyreállításának várható időpontját, az erről szóló tájékoztatás formájának meghatározását.

270. Üzemszüneti feldolgozási rend bevezetésének elrendelése helyi üzemszünet esetében:
   a) Abban az esetben, ha helyi üzemzavar következtében a rendszer használata előreláthatóan négy órát meghaladóan nem lehetséges, szükségessé válik az üzemszüneti feldolgozási rend helyileg történő bevezetése. A négy órára vonatkozó előírástól jogszabályi előírás alapján az egyes rendszerek tekintetében el lehet kérni.
   b) Az üzemszüneti feldolgozási rend helyi bevezetését a bv. szerv vezetője rendeli el, az illetékességi területén működő szervezeti egységek tekintetében. Az üzemszünetet elrendelő vezető az érintett szervezeti egységeket telefonon és email útján az informatikai szakterület közreműködésével értesíti.

Katasztrófa-elhárítási terv

271. Informatikai katasztrófa: az informatikai incidenseknek az a szintje, illetve olyan állapot, amely megszünteti, hogy bizonyos időszakra megakadályozza az informatikai erőforrások folyamatos működését, és károkat, veszteségeket okoz és a szakmai vagy funkcionális folyamatokat támadó informatikai erőforrások kiesése előreláthatólag időben meghaladja a felhasználók által elvárt, elfogadható időtartamot. Elhárításakor az jelen fejezet rendelkezéseit kell alkalmazni.

272. Ilyen eseményt előidézhet különösen, de nem kizárólagosan:
   a) a bv. szerv épületeit sújtó tűzvész, robbanás vagy más külső behatás,
   b) az elektromos hálózat tartós kiesése,
   c) a telekommunikációs hálózat tartós kiesése,
   d) kritikus informatikai rendszerek súlyos üzemzavara.

273. A bv. szervezetnek rendelkeznie kell informatikai rendszerekre vonatkozó az informatikai katasztrófák elhárítására szolgáló tervekkel (Informatikai Katasztrófa-elhárítási Terv a továbbiakban: IKT).

274. A bv. szerveknek az IKT figyelembevételével kell elkészíteniük a helyi informatikai rendszerükre szóló katasztrófa elhárítási tervet.

275. Az IKT célja, hogy:
   a) globális helyettesítő megoldásokat adjon a megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett katasztrófa esemény után az informatikai rendszer funkcionalitása degradált vagy eredeti állapotába visszaállítható,

b) az informatikai katasztrófahelyzet bekövetkezése esetén a káros hatásokat minimalizálja,
c) a szakmai vagy funkcionális tevékenység folytatásához szükséges sérült informatikai erőforrásokat mielőbb pótolja,
d) a károsodott informatikai erőforrások helyreállítását a normál üzemeltetési szintre a lehető legrövidebb időn belül biztosítsa.

276. Az IKT-nak tartalmaznia kell:
a) a rendszer megnevezését,
b) a rendszer elhelyezési helyének megnevezését,
c) a rendszer elhelyezési helyének címét,
d) a rendszer elhelyezésének pontos leírását,
e) a végrehajtásért felelős személy beosztását,
f) az IKT készítőjének nevét, beosztását és a terv készítésének dátumát,
g) az IKT jóváhagyójának nevét, beosztását és a terv jóváhagyásának dátumát,
h) az értesítendő személyek listáját,
i) a visszaállítandó rendszer elemeinek listáját,
j) a visszaállítási vagy helyreállítási tevékenységeket, ezen belül:
ja) a feladat megnevezését,
jb) a feladatért felelős személy beosztását,
jc) a szükséges információt vagy dokumentációt,
jd) a visszaállításhoz minimálisan szükséges informatikai rendszer elemeinek listáját, az adott tevékenység egyéb feltételeit (így különösen a helység biztosítása, szállítás megszervezése, áramforrás, hálózat biztosítása, informatikai eszközpark felállítása),
je) a visszaállítás elvárt időtartamát a feltételektől függően,
jf) az ellenőrzési listát, felelősök meghatározását, beosztását,
k) mellékleteket (különösen: értesítési lista).

277. Nem kell készíteni IKT-t azon rendszerekre, amelyek üzemeltetése külső szolgáltató által felügyelt és a szolgáltató saját környezetében lévő infrastruktúrán valósul meg. Ezen erőforrások által okozott szolgáltatáskiesések megszüntetésére vonatkozó eljárás a szolgáltatóval kötött szerződésben jelen fejezetben foglaltak figyelembevételével kell rögzíteni.

278. Az elkészült IKT-kat az IFO vezetője, bv. intézetek esetében az intézet parancsnoka hagyja jóvá az IKT sikeres tesztelését igazoló dokumentumok alapján.

279. Az IKT-kat a Robotzsaru iratkezelő rendszerben iktatni kell, az alkalmazandó IKT-k alapadatairól és tárolási helyéről az informatikai szakterület nyilvántartást vezet, amelyet a bv.hu honlapon közzéteszi. Az informatikai szakterület biztosítja, hogy az IKT-val érintett informatikai rendszerek nyilvántartásához az érintettek hozzáférjenek.

280. A bv. szerv informatikai katasztrófavédelmi tervet belső honlapján teszi közzé.

Informatikai katasztrófa-elhárítási folyamat fázisai

281. A bv.szerv informatikai katasztrófa-elhárítás folyamata felkészülési fázisból, válasz fázisból, visszaállítási fázisból és helyreállítási fázisból áll.

282. Felkészülési fázis: az informatikai katasztrófa előtti adminisztratív, szervezési és technikai intézkedéseket tartalmazza az informatikai katasztrófák csökkentése érdekében. A felkészülési fázisban kerül sor a konkrét részletes elhárítási folyamatok és eljárások kidolgozására, tesztelésére, az alkalmazottak oktatására. A fázis fő feladatai:
   a) az informatikai rendszer elemeire a szakmai területek vezetőivel egyetértésben a 2. pont figyelembevételével meg kell határozni azokat az időtartamokat, amelyek még elfogadhatók egy probléma elhárítására – ezek az időtartamok jelentik a legfőbb szempontot az informatikai incidensek értékelésekor,
   b) az informatikai katasztrófa-elhárításhoz szükséges dokumentációk elkészítése, összeállítása (mentés-visszaállítási, elhárítási – visszaállítási és helyreállítási – folyamatok és eljárások leírásai, szerződések, értesítési listák, konfigurációs állományok, hardver és szoftver elemek stb.) és rendszeres karbantartása, naprakész állapotban tartása,
   c) a visszaállítás és helyreállítás erőforrás igényének becslése,
   d) probléma bejelentési lehetőség biztosítása,
   e) az IKT-k elkészítése, jóváhagyása, iktatása, nyilvántartásban rögzítése, tesztelése és oktatása.

283. Válasz fázis: tartalmazza a katasztrófa észlelése után közvetlenül elvégzendő legsürgősebb feladatokat, valamint a kárelhárítás további feladatit. A fázis fő feladatai:
   a) a bekövetkezett informatikai incidens felmérése,
   b) a kialakult helyzet értékelése,
   c) az informatikai katasztrófahelyzetté minősítés,
   d) az érintettek riasztása és tájékoztatása,
   e) jelen cím szerinti katasztrófa-elhárítási tevékenység végrehajtása (halaszthatatlan kárelhárítási, kárenyhítési intézkedések).

284. Visszaállítási fázis: az a tevékenység, amely a büntetés-végrehajtás szakmai vagy funkcionális folyamatait támogató sérült informatikai előírások – akár csökkentett funkcionalitással is – újra működőképes állapotba hozására nyújt rövidtávú, gyors megoldást.

285. Helyreállítási fázis: az informatikai erőforrások eredeti vagy új helyszínen teljes funkcionalitással történő, hosszútávú, véglegesnek szánt újraindítására adott megoldás megvalósítása. A fázis főbb feladatai:
   a) az eredetivel legalább azonos minőségű erőforrás telepítése és működésbe állítása,
   b) a fázis akkor ér véget, amikor az informatikai erőforrás az eredetivel legalább azonos módon működőképes és az informatikai erőforrást ismét a normál üzemállapotnak megfelelő, a kívánt minőségben képes nyújtani.

Informatikai katasztrófa-elhárítás felelősei

286. A felkészülési fázisában:
   a) elhárítási folyamatok és eljárások kidolgozása: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
   b) IKT-k tesztelése: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
   c) alkalmazottak oktatása: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője közösen a humán szakterület vezetőjével,
   d) a 282. a) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője

e) a 282. b) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
f) a 282. c) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
g) a 282. d) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
h) a 282. d) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője.

287. A válasz fázisában:
a) a 283. a) pontban foglaltak: informatikai szakterület munkatársai,
b) a 283. b) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője
c) a 283. c) pontban foglaltak: büntetés-végrehajtás országos parancsnok gazdasági és informatikai helyettese, bv. intézetek esetében az intézet parancsnoka,
d) a 283. d) pontban foglaltak: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője, BVOP ÜTI,
e) a 283. e) pontban foglaltak: informatikai szakterület, a végrehajtásban érintett szakterületek.

288. A visszaállítási fázisában: informatikai szakterület.

289. A helyreállítási fázisában: IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője, a rendszer helyreállításában érintett szakterületek.

Informatikai katasztrófa terv (továbbiakban IKT) felülvizsgálata

290. Az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője köteles az IKT-kat évente egyszer felülvizsgálni.

291. Az évenkénti felülvizsgálatokon túl köteles felülvizsgálni, ha
a) az informatikai szervezetben vagy az informatikai erőforrásokban az adatvédelmet, adatbiztonságot, informatikai biztonságot vagy az IBK tartalmát érintő változás következett be,
b) az informatikai erőforrásokban funkcionális, architekturális vagy egyéb változás következett be,
c) működést meghatározó jogszabályi környezetben változás következett be,
d) informatikai katasztrófa következett be, a helyreállítást követően,
e) az elvégzett IKT tesztek eredményei alapján, ha az indokolt.

Informatikai katasztrófa terv tesztelése

292. Az IKT-kat, annak elkészítését és bármilyen módosítását követően, de legalább évente egyszer tesztelni kell.

293. A tesztelés célja az IKT-k megfelelőségéről illetve az IKT-k végrehajtásában résztvevők felkészültségéről való meggyőződés.

294. Az éves tesztelésről tervet kell készíteni, amelyért az IFO vezetője, bv. intézetek esetében az informatikai szakterület vezetője a felelős.

295. Az éves tesztelési terv különösen tartalmazza:

a) a tesztelendő informatikai erőforrásokat,
b) a tesztelés módját és ütemezését.

296. Az IKT-k teszteléséről jegyzőkönyvet kell vezetni.

297. A teszt befejezésével értékelni kell a teszt lefolyását, be kell gyűjteni javaslatokat, véleményeket. A teszt abban az esetben sikeres, ha az IKT-k végrehajtásával az informatikai erőforrás teljes funkcionalitásával helyreállt. A tesztelés abban az esetben sikertelen, ha az IKT-k végrehajtásával az informatikai erőforrás teljes funkcionalitásában nem állt helyre.

298. Ha a tesztelés sikertelennek bizonyul, a hibafelderítést és a kijavítást követően soron követően az üzemeltetési rend figyelembe vételével a tesztelést meg kell ismételni.

Az IKT-val érintett informatikai erőforrások

299. Az IKT-kat az alábbi informatikai erőforrásokra kell elkészíteni:
a) géptermek teljes hardver és szoftver infrastruktúrája,
b) hálózati és hálózati szolgáltatások,
c) központi és elosztott alkalmazás-környezetek erőforrásai,
d) munkaállomás környezetek erőforrásai,
e) infrastruktúra-üzemeltetés erőforrásai.

V. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

Kártékony kódok elleni védelem

300. A kártékony kódok elleni védekezésről, valamint a bv. szervezet rendszereinek ki- és belépési pontjai védelméről az IFO gondoskodik.

301. A vírusvédelmi rendszert a bv. szervezet zárt célú hálózatában működő összes kiszolgáló szerverre és munkaállomásra alkalmazni kell. A szerverekre és munkaállomásokra vonatkozó eltérő vírusvédelmi követelményeket az IFO vezetője határozza meg.

302. A vírusvédelmi rendszer központi felügyeletét, frissítését, konfigurálását az informatikai szakterület látja el.

303. A rendszer központi ütemezés alapján havi rendszerességgel teljes ellenőrzést végez a felügyelt eszközökön.

304. A rendszer végrehajtja a kezelt állományok valós idejű folyamatos ellenőrzését, amikor azokat letöltik, megnyitják, vagy elindítják az állományok letöltése, megnyitása, elindítása alkalmával, továbbá az IFO vezetője által meghatározott beállítások alapján időzített folyamatként teljes vírusellenőrzéseket végez.

305. Kártékony kódok észlelése esetén a rendszer blokkolja vagy karanténba helyezi azokat és riasztást küld az IFO rendszeradminisztrátora részére.

306. A vírusvédelmi rendszer optimalizált frissítési eljárásának biztosítása érdekében a bv. szervekben kijelölt kiszolgáló szerverek decentralizáltan szolgálják ki a vírusadatbázis

frissítési szolgáltatást. A frissítések megjelenést követően automatizált módon telepítésre kerülnek.

307. A vírusvédelmi rendszer felügyeletére központi menedzsment felület áll rendelkezésre.

308. A kártékony kódok elleni védelmi rendszer az elektronikus levelezésre is kiterjesztésre kerül és megvalósítja a ki- és bemenő e-mail forgalom valós idejű vizsgálatát.

309. Az elektronikus levelezés vizsgálata során szűrni kell a beérkező kéretlen leveleket. A védelmi rendszeren keresztül jutó spam gyanús küldeményeket a felhasználók kötelesek a spam@bv.gov.hu címre továbbítani. Az IFO a küldemény vizsgálatát követően dönt a spamszűrő szabálykészletének módosításáról.

310. A bv. szerv által üzemeltetett szerverek és kliensek vírusvédelméről a központi menedzsment felügyelettel rendelkező Symantec Endpoint Protection szoftver gondoskodik. A kliensek alatt a vastagklienseket és a hordozható munkaállomásokat értjük.

	Szerver	**Kliens**
Frissítés gyakorisága	Automatikus napi	Automatikus napi
Ellenőrzések	Valósidejű Ütemezett, havi szintű, melynek teljesülését a vírusvédelmi rendszergazda szúrópróbaszerűen ellenőrzi.	Valósidejű Ütemezett, havi szintű, melynek teljesülését a vírusvédelmi rendszergazda szúrópróbaszerűen ellenőrzi.
Riasztások	Vírustalálat és frissítési probléma esetén a központi modul riasztást küld a bvop-uzemeltetes@bv.gov.hu e-mail címre	Vírustalálat és frissítési probléma esetén a központi modul riasztást küld a bvop-uzemeltetes@bv.gov.hu e-mail címre

Hibajavítás

311. Az informatikai szakterület
   a) azonosítja, belső eljárásrendje alapján jelenti és kijavítja, vagy kijavíttatja az elektronikus információs rendszer hibáit;
   b) telepítés előtt teszteli a hibajavítással kapcsolatos szoftverfrissítéseket a szervezet feladatellátásának hatékonysága, az előre nem látható következmények szempontjából;
   c) a biztonságkritikus szoftvereket frissítésük kiadását követő 1 hónapon belül telepíti vagy telepítteti;
   d) beépíti a hibajavítást a konfigurációkezelési folyamatba;
   e) a hibajavítási állapotok központi kezelésének megvalósításához helpdesk rendszert üzemeltet.

Rendszer felügyelet

312. Az informatikai szakterület
   a) felügyeli az elektronikus információs rendszert annak érdekében, hogy észlelje a kibertámadásokat vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;
   b) azonosítja az elektronikus információs rendszer jogosulatlan használatát;
   c) felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakciók nyomon követésére;
   d) védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;
   e) erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, ami-kor fokozott kockázatra utaló jelet észlel;
   f) meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek;
   g) kezeli és megőrzi az információs rendszer kimeneti információit a vonatkozó jogszabályoknak, szabályzatoknak és üzemeltetési követelményeknek megfelelően.

Naplózás

313. Az informatikai szakterület az elektronikus információbiztonsággal kapcsolatos naplózási szabályokat rendszerenként meghatározza a jelen fejezetben foglaltak szerint.

Határvédelem

314. A bv. szervezet az egyes telephelyei adatátviteli kapcsolatának biztosítására *a kormányzati célú hálózatokról* szóló 346/2010. (XII. 28.) Korm. rendelet alapján a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ Zrt.) által üzemeltetett kormányzati célú zárt hálózatot, a Nemzeti Távközlési Gerinchálózatot (a továbbiakban: NTG) veszi igénybe.

315. A bv. szervezet a belső hálózat védelmének biztosítása érdekében igénybe veszi a NISZ Zrt. által biztosított határvédelmi funkciókat, továbbá saját határvédelmi megoldást (tűzfal) alkalmaz a hálózati forgalom kezelésére.

316. A rendszer túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelmét a NISZ Zrt. biztosítja.

317. A tűzfal felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt.

318. A nyilvánosan hozzáférhető rendszerelemeket (pl. levelező rendszer) fizikailag vagy logikailag alhálózatokban kell elhelyezi, elkülönítve a szervezet belső hálózatától.

319. A szervezeten belül működő, nem nyilvánosan hozzáférhető elektronikus információs rendszerekhez kizárólag az alkalmazott határvédelmi eszközökön felügyelt interfészeken keresztül lehet kapcsolódni a külső hálózatokból.

320. A szervezeten kívülre történő kapcsolódások határvédelmi eszközökön felügyelt interfészeken keresztül, az ott alkalmazott szabályok alapján valósulhat meg.

321. A tűzfal alkalmazásához kapcsolódó szabályokat az IFO vezetője határozza meg.

Külső hozzáférések kezelése

322. A bv. szervezet által üzemeltetett elektronikus információs rendszerhez a szervezeten kívüli hálózatokból csak a bv. szervezet felügyeletében lévő megbízható, kriptográfiai módszerrel titkosított csatornán (megfelelő RSA titkosítású VPN csatorna vagy APN kártyás mobil kommunikációs csatorna) keresztül lehet csatlakozni.

323. A külső hozzáféréseket biztosító eszközök kiosztását az IFO vezetője engedélyezi, a kiosztott eszközökről az IFO nyilvántartást vezet.

Az adatátvitel bizalmasságának és sértetlenségének védelme

324. A bv. szervezet belső hálózatán a továbbított információk bizalmassága és sértetlensége biztosítása érdekében a belső kommunikációs eszközökön az informatikai szakterület kialakítja
   a) a hálózati aktív eszközökön a port szintű engedélyezési eljárást;
   b) a MAC address szűrést az eszközök egyedi azonosításához;
   c) az eszközök egyedi jelszavas védelmét.

325. A bv. szervek egymás közötti kommunikációja során az NTG zárt hálózat biztosítja a továbbított információk bizalmasságát és sértetlenségét.

326. A külső hálózatokból történő elérés során a „Külső hozzáférések kezelése” alcím alatt meghatározott védelmi intézkedések biztosítják a továbbított információk bizalmasságát és sértetlenségét.

327. Külső adathordozón történő adattovábbítás során az adatok jelszavas védelméről gondoskodni kell.

Funkciók szétválasztása

328. A bv. szervezetnél alkalmazott elektronikus információs rendszerekben szét kell választani a felhasználók által végzett adatfeldolgozási funkciókat, valamint az irányítási feladatellátáshoz kapcsolódó funkciókat.

329. Az egyes funkciókhoz történő felhasználói hozzáférésekhez külön felhasználói azonosítás szükséges.

330. A jelen fejezetben meghatározottakon túl az egyes rendszerekhez meg kell határozni az IBSZ szerinti szerepköröket.

Nyilvános kulcsú infrastruktúra tanúsítványok

331. A bv. szervek a munkáltatói okiratok elektronikus előállításához elektronikus aláírási szolgáltatást vesznek igénybe.

332. A nyilvános kulcsú tanúsítványokat a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartása alapján a NISZ Zrt.-től szerzi be.

Mobilkódok korlátozása

333. A bv. szervezet elektronikus információs rendszereiben a mobil kódok futtatására az alábbi szabályok kerülnek alkalmazásra:
   a) JavaScript, VBScript, Java applet futtatása engedélyezett;
   b) ActiveX vezérlők futtatása központi házirendek beállításával tiltott;
   c) Flash tartalom futtatása az IFO vezetője által engedélyezett jogosultsági csoport részére engedélyezett;
   d) MS Office makrók futtatása engedélyezett.

Egyéb, a rendszer- és információsértetlenséggel kapcsolatos rendelkezés

334. A bv. szervezet elektronikus információs rendszerén keresztüli hangátviteli szolgáltatást a NISZ Zrt. biztosítja az NTG zárt hálózaton keresztül.

335. A bv. szervezet zárt hálózatán belül a Windows tartományi hitelesítési eljárások igénybevételével megbízható és hiteles név/cím feloldási rendszer működik. A hibatűrést a BVOP-n működő redundáns, valamint a bv. szervekhez telepített helyi tartományi névkiszolgálók biztosítják.

336. A rendszer maradvány információt (pl.: átmeneti fájlok) a felhasználást követő automatikus törléssel védi.

337. A rendszer megvédi a munkaszakaszok hitelességét.

338. A rendszer elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára.

VI. JOGOSULTSÁGKEZELÉS

339. A rendszerekhez hozzáférést biztosító jogosultságok igénylése, engedélyezése és visszavonása, kiadása és visszavétele az IBK-ban meghatározottan, minden esetben dokumentáltan történhet.

340. Jogosultságot kizárólag a felhasználó közvetlen vezetője igényelhet vissza, az igényelt jogosultságokat kizárólag vezető hagyhatja jóvá.

341. A jogosultságok a munkatárs munkakörére tekintettel engedélyezhetők (kiadhatók), a munkatárs számára csak a munkaköre ellátásához szükséges és elégséges jogosultságok igényelhetők vagy adhatók ki. A rendelkezés megtartásáért és megtartatásáért a közvetlen vezető és az alkalmazások adatgazdái felelősök.

342. A jogosultságokat, jogosultságcsoportokat úgy kell kialakítani, illetve a már meglévőket átalakítani, hogy megkülönböztethetőek legyenek a munkakör, feladatkör, azon belül a tevékenység jellege szerint:
   a) az informatikai jogosultságok és jogosultságcsoportok, illetve a felhasználói jogosultságok és jogosultságcsoportok;

b) a felhasználói jogosultságokon belül a lekérdező, az ügyintéző, valamint a privilegizált felhasználó és – amennyiben az alkalmazás jellegzetességei indokolják – adminisztrátor jogosultságok, illetve jogosultságcsoportok.

Az informatikai rendszerekhez történő hozzáférés

Személyügyi rendszerrel való kapcsolat

343. A munkatársak közül
a) a hivatásos állomány hivatásos szolgálati jogviszonyának és
b) a rendvédelmi alkalmazottaknak rendvédelmi igazgatási jogviszonyának
c) a munkavállalók munkaviszonyának
létesítésére, módosítására és megszüntetésére vonatkozó adatok rögzítésére az egységes személyügyi rendszerben, a SZENYOR-ban történik, és e rendszerből a jogosultságkezeléshez szükséges összes alapadat átadásra kerül a jogosultságkezelő rendszer számára.

344. Tartós távollét esetén a munkatárs jogosultságai felfüggesztésre kerülnek. A jogosultságok felfüggesztésének megtörténtének ellenőrzését a bv. szervezet egységes ellenőrzési szabályzata szerint kell végrehajtani.

345. A tartós távollét megszűnését követően a jogosultságok felfüggesztését vissza kell vonni.

346. Amennyiben a munkatárs jogviszonya vagy munkaviszonya módosul, a meglévő jogosultságokat vissza kell vonni, továbbá a munkatárs módosult jogviszonynak megfelelő jogosultságait az IBK-ban szabályozott módon ki kell alakítani.

347. Szervezeten belüli áthelyezés esetén – az áthelyezést követően – a közvetlen vezető haladéktalanul vizsgálja felül a jogosultságokat.
348. A munkatárs jogviszonya megszűnése esetén a jogosultságait vissza kell vonni, amit a leszerelési lapon az informatikai szakterület igazol.

A felhasználói név képzése és használata

349. A felhasználó a rendszert csak egyértelmű azonosítást követően (felhasználói név és jelszó), a számára meghatározott és biztosított jogosultságok keretei között használhatja. A felhasználói jogosultságokat *Login lapon* (9. melléklet) kell kérni. A névre szóló felhasználói jogosultságokat engedélyezés után az informatikai szakterület állítja be, és biztosítja a felhasználói jogosultságokat.

350. A felhasználó profil az IBSZ-ben meghatározott névkonvenció alapján kerül létrehozásra. A kezdeti jelszót az első belépés alkalmával kötelezően meg kell változtatni és ezt a rendszer kikényszeríti. A felhasználó a belépéshez szükséges jelszót a login lapon kapja meg.

351. A bv. szervezet az azonosítási, autentikációs és jogosultságkezelési feladatok támogatására a tartományvezérlő szervereken központi címtárat üzemeltet.

352. A felhasználó azonosítást követően feljogosítást kap a jogosultságai használatához.

353. A jelszavak kezelésére az IBSZ rendelkezései az irányadóak.

354. Az IBSZ alapján a rendszer használata során a felhasználót kizárólagos személyi használatú azonosítóval kell ellátni, amelyhez egyedi jelszót az alábbiak szerint kell biztosítani:
   a) legalább 8, legfeljebb 12 karakter hosszú,
   b) kisbetűk, nagybetűk, számok és speciális karakterek közül legalább háromfélét tartalmaz,
   c) nem tartalmaz könnyen kitalálható, ismétlődő karaktersorozatot,
   d) nem utal a felhasználó személyére,
   e) érvényességi ideje legfeljebb 90, egyes rendszerek esetében 60 nap,
   f) a 12 legutóbb használt jelszótól különbözik,
   g) nem lehet azonos a bejelentkezési azonosítóval, annak valamilyen egyszerű módosításával, az informatikai rendszerben ismert paranccsal vagy alkalmazásnévvel.

355. A felhasználók jogosultsága 5 sikertelen próbálkozás után felfüggesztésre kerül, ismételt hozzáférésre 30 perc letelte után van lehetőség.

356. Az IBSZ értelmében meghatározott jelszó szabályoktól eltérő jelszókezelések körét az alábbi táblázat tartalmazza.

Rendszer	Az eltérés leírása (beállított érték)	Indoklás
RZSNEO	5 karakter hosszú, 30 naponta változik	A fejlesztő által meghatározott jelszópolitika.
RSA kulcs	A jelszó nem jár le	A fejlesztő által meghatározott jelszópolitika.
TÉR	A jelszó nem jár le	A fejlesztő által meghatározott jelszópolitika.
SZENYOR	A jelszó nem jár le	A fejlesztő által meghatározott jelszópolitika.
Attenti terheltkezelő rendszer	60 nap	A fejlesztő által meghatározott jelszópolitika.

Jelszóborítékok kezelése

357. A BV IBSZ-ben rögzített szabályok figyelembevételével az alábbi rendszerek, eszközök esetében szükséges jelszóboríték:
   a) Symantec Endpoint Protection admin jelszó,
   b) Symantec Messaging Gateway admin jelszó,
   c) Routerek admin/root jelszava,
   d) Tűzfal admin/root jelszava,
   e) Notebook drivelock admin jelszava,

f) Titkosított mentések jelszavai.

358. Jelszóborítékok kezelésének szabályai
   a) a jelszóborítékok tárolási helyét és az összes jelszóborítékra vonatkozó információt az erre a célra létrehozott nyilvántartás tartalmazza.
   b) A jelszóborítékban lévő jelszavakat rendszerenként, alkalmazásonként külön-külön, nem átlátszó, nem átvilágítható borítékban kell elhelyezni. A borítékon egyértelműen fel kell tüntetni, hogy mely eszközhöz, mely alkalmazáshoz tartozik.
   c) A jelszóboríték felbontásáról kizárólag az informatikai üzemeltetésért felelős dönthet és erről értesíti az informatikáért felelős vezetőt.
   d) A jelszóboríték dokumentált felbontását követően, az informatikai eszközön, szoftveren folytatott munka végeztével, az adott felhasználónévhez tartozó jelszót meg kell változtatni és az új jelszót jelszóborítékban kell elhelyezni.
   e) A lecserélt jelszavakat tartalmazó borítékokat iratmegsemmisítővel meg kell semmisíteni az új jelszóboríték elkészítését követően.
   f) Amennyiben a régi jelszóra visszaállíthatósági művelet végrehajtása érdekében miatt volt szükség, akkor a megsemmisítést tilos elvégezni.

Külső adathordozókkal összefüggő jogosultságkezelés

359. A külső adathordozók (pl. CD, DVD, USB) használata csak a munkakör ellátásához szükséges esetben, engedély alapján, személyhez kötötten, megfelelő jogosultság birtokában történhet.

360. Kivételesen – munkaszervezési okból – munkaállomáshoz kötötten is történhet a külső adathordozók használatának engedélyezése.

361. Az előző két pontban foglalt jogosultságot a felhasználó számára a közvetlen vezető kezdeményezésére az engedélyező vezető jóváhagyja.

362. A külső adathordozók használatát biztosító jogosultságok visszavonására az indokoltság megszűnését követő munkanapon a felhasználó közvetlen vezetője intézkedni köteles.

Hálózati tárhelyekkel összefüggő jogosultságkezelés

363. A felhasználók és a szervezeti egységek számára szervezeti egységekbe sorolt struktúrában tárhelyek állnak rendelkezésre.

364. A hálózati környezetben csak nem minősített adat helyezhető el úgy, hogy szerzői-, szomszédosjog, személyes-, különleges adat, illetve üzleti-, magántitok nem sérülhet. Az adatok védelméért az adatot elhelyezőt is felelősség terheli.

365. A fájlmegosztó szerveren a megosztást úgy kell kialakítani, hogy a hozzáférés a „vendég” felhasználó (guest) és a „mindenki” csoport (everyone), valamint a létrehozó tulajdonos (creator owner) számára tiltott legyen.

366. A fájlmegosztó szerveren a megosztásnak az alábbi funkcionalitást kell biztosítani:
   a) user - felhasználó
   b) group - csoport, szervezeti egység

c) other - egyéb, nem a szervezeti egység, vagy a szervezeti egységhez tartozó felhasználó
d) admin - superuser, infrastrukturális rendszergazda, informatikai fenntartó szervezet

sor-szám	struktúra azonosító	user jog	group jog	other jog	admin jog	megjegyzés
1.	\felhasznalonev\ Dokumentumok /Privát mappa/	O, Í,	-	-	-	felhasználó fájljai amit még nem kíván mások számára láthatóvá tenni. nem kerülnek mentésre
2.	\szervezeti egyseg\belso	O, Í,	O, Í,	-	O, Í,	szervezeti működés iratai névre szólóak, vagy beosztáshoz kötöttek központosítottan kerülnek mentésre
3.	\szervezeti-egyseg\publikus	O, Í,	O, Í,	O	O, Í,	szervezeti egység posta kifelé központosítottan kerülnek mentésre

O = olvasási és az olvasási jogosultsághoz kötődő jog (pl. tallózás)
Í = írási és az íráshoz kötődő jogosultságok (pl. módosítás, törlés)

367. Az egyes funkciók részletezve:
a) személyes dokumentumok - a rendszergazda sem jogosult az alkönyvtárakat tallózni (azaz a tartalmát olvasni). Az adatok rendelkezésre állását redundáns adattároló rendszerek biztosítják. A tárhely alapértelmezetten felhasználónként 50Mbyte méretben maximált, amelyet adott alkalmazás működésének biztosítása érdekében növelhető, egyéb esetben tilos;
b) A szervezeti egység (group) számára a \szervezeti-egyseg\Belso alkönyvtár struktúra biztosítja, hogy a szervezeti egység tagjai a szolgálati feladatok ellátása során készített, a szolgálati feladatokhoz köthető állományait a szervezeti munkamegosztás rendszerében a szervezeti egység számára megosztott módon tudják tárolni. A szervezeti egységek \szervezeti egység\Belso alkönyvtárainak összessége a büntetés-végrehajtási szervezet irodai alkalmazásaival előállított adatvagyona, amely központi, generációs mentését az informatikai szervezetnek biztosítania kell;
c) A szervezeti egység (group) számára a \szervezeti egység\Publikus alkönyvtár struktúra biztosítja, hogy a szervezeti egység kizárólag olvasási jogosultsággal más szervezeti elemek részére a helyi hálózaton állományokat osszon meg (publikáljon). A megoldás szolgálja az egyes szervezeti egységek közötti közvetlen adatcsere lehetőségét úgy, hogy az eredetileg megosztott dokumentum más szervezeti egységek számára nem szerkeszthető, azaz az eredeti dokumentum védelme biztosított;
d) A helyi hálózatokban alkalmazott méretkorlátozás - quota - beállításáról a rendelkezésre álló kapacitás alapján, az informatikai szakterület vezetője gondoskodik;
e) A munkaállomásba épített lokális adattárolás a tartományi felhasználó számára tiltott. Az erőforrások elérésének és alkalmazásának korlátozását tartományi, vagy

szervezeti egységre vonatkozó házirend szintjén (domain, OU policy) biztosítani kell. Azokon a munkaállomásokon, ahol a lokális adattárolás, vagy archiválás az igénybe vett szolgáltatás korlátaiból következően engedélyezett, a fájl műveleteket naplózni kell. A központi tárolást úgy kell biztosítani, hogy megvalósuljon a felhasználói adatok és hozzáférések gépfüggetlen elérése. A tartományi működésre alkalmatlan szolgáltatásokat az IFO vezetője engedélyezi.

368. A hálózatba kapcsolt munkaállomások esetében a felhasználó felelőssége, hogy a munkahelyi feladataival kapcsolatos adatokat, dokumentumokat a szervezet által biztosított központi tárhelyre mentse.
369. A felhasználó rendelkezésére bocsátott eszközökön kizárólag a munkahelyi feladatok ellátásához szükséges adatok, dokumentumok tárolhatók.

370. A szervezet fenntartja magának a jogot, hogy azokat az adatokat, dokumentumokat, amelyek valamilyen jellemzőjük (fájltípus, név) alapján feltehetően nem kapcsolódnak a felhasználó munkavégzéséhez, előzetes figyelmeztetést követően törölje.

371. Az adatok, dokumentumok visszaállítása az informatikai szakterülettől dokumentáltan kérhető, a dokumentum vagy könyvtár nevének és pontos elérésének megadásával.

372. A szervezeti egységből történő kilépést követően a szervezeti egység vezetője köteles az ott tárolt adatok megőrzéséről, törléséről 5 napon belül gondoskodni.

Külső rendszerekkel összefüggő jogosultság

373. A külső rendszerek vonatkozásában a szakmai felügyelet a rendszert üzemeltető külső szervezet által biztosított lehetőségeknek megfelelően kell alkalmazni.

374. A külső rendszerek elérését biztosító jogosultságok kezelésére vonatkozó előírásokat a bv. szervezet és a külső rendszert üzemeltető szerv közötti szerződés, együttműködési megállapodás alapján a szakmai működésért felelős terület által kidolgozott és kiadmányozott rendszerhasználati – vagy annak megfeleltethető – rendelkezésnek kell tartalmaznia.

375. A külső rendszerek elérését biztosító jogosultságok esetében is biztosítani kell, hogy – amennyiben az technikai szempontból megvalósítható – az igénylések kezelése login lap formanyomtatványon megvalósítható legyen. Amennyiben ez technológiai okokból nem megvalósítható, az eltérő igénylési eljárást szabályzatban rögzíteni kell.

376. A külső rendszerek elérését biztosító jogosultságok igénylésére, engedélyezésére és visszavonására az általános szabályokat kell alkalmazni, azonban ettől szakmai működésért felelős vezető megfelelő rendelkezésben – szakmai vagy munkaszervezési okból – eltérhet. Ebben az esetben meg kell határozni, hogy az eltérően kezelt jogosultságokat milyen szabályok szerint kell kezelni.

377. Amennyiben a külső rendszer elérését meghatározott számú felhasználóra kell korlátozni, a jogosultságok engedélyezéséről és visszavonásáról (újra osztásáról) a szakmai működésért felelős vezetője dönt.

378. Amennyiben a külső rendszer elérése díj ellenében történik, a rendszer használatának indokoltságát a felhasználó közvetlen vezetője rendszeresen köteles ellenőrizni.

379. A külső rendszer elérését biztosító jogosultságok visszavonására az indokoltság megszűnését, illetve felhasználó más munkakörbe helyezését követő munkanapon a felhasználó közvetlen vezetője intézkedni köteles.

380. A külső rendszer elérését biztosító jogosultságok nyilvántartását – eltérő jogszabály, országos parancsnoki rendelkezés, illetve az IFO által jóváhagyott belső megállapodás hiányában – az IFO végzi. A nyilvántartást lehetőség szerint a jogosultságkezelő alkalmazás segítségével kell vezetni.

381. A közvetlen vezető a szervezeti egység számára kiadott, külső rendszerek elérését biztosító jogosultságokat minden év március 31-éig köteles felülvizsgálni. Ennek keretében a feleslegessé vált jogosultságok visszavonásra, a szükségesnek ítélt jogosultságok engedélyezésére igénylést kell kezdeményeznie. A felülvizsgálatok eredményéről szervenként minden év március 31-éig tájékoztatni kell a szakmai felügyelet vezetőjét és az IFO-t.

Felhasználói tesztrendszerekkel kapcsolatos jogosultságkezelés

382. A felhasználók számára kialakított tesztkörnyezetben üzemelő rendszerekhez létrehozott jogosultságok kezelésére az IBK-t e fejezetben foglalt eltérésekkel kell alkalmazni.

383. Az e fejezet szerinti jogosultságok igénylése és jóváhagyása – az általános szabályoktól eltérően – történhet központilag is
   a) a szakmai felügyelet vezetője,
   b) IFO,
   c) és a projekt vezetője intézkedése alapján.

384. Az e fejezet szerinti jogosultságok legfeljebb az igényléstől számított három év időtartamra állíthatók be.

Jogosultságkezelés kialakítása új fejlesztések során

385. Új informatikai rendszer, alkalmazás vagy modul kialakítása során – amennyiben ennek technikai akadálya nincs – a jogosultságkezelést a jogosultságkezelő szolgáltatás alkalmazásával kell megvalósítani.

Az informatikai rendszerek használatához szükséges jogosultságok kialakításának szabályai

386. A rendszer használatához, a rendszerben tárolt adatok kezeléséhez szükséges jogosultságokat, továbbá ezek lehetséges felhasználói körét a rendszer működtetéséért felelős szervezeti egység határozza meg az IFO-val történt egyeztetés alapján.

387. Az újonnan kialakított jogosultságok kódját/azonosítóját úgy kell kialakítani, hogy az első karakterei annak az alkalmazásnak vagy rendszernek a rendszerazonosító kódja legyen, amelyhez a jogosultság biztosítja a hozzáférést további karakterei pedig lehetőség szerint utaljanak a jogosultság rendeltetésére továbbá illeszkedjen a névkonvenciós szabályokhoz.

388. Jogosultságok informatikai rendszerben történő kialakítása és funkciókhoz rendelése – a szakmai igények alapján, a biztonsági, információvédelmi szempontok, valamint az informatikai lehetőségek figyelembevételével – az informatikai szakterület feladata.

389. Új alkalmazás, új funkció, új jogosultság, új szolgáltatás megrendelése során az előző pontokban foglaltak az irányadók.

390. A bv. szervezet a jogosultságigénylő adatlapokat, űrlapokat, formanyomtatványokat a Tudástárban közzéteszi és a szakmai felügyelettel történő konzultáció alapján folyamatosan aktualizálja.

391. A munkakör betöltéséhez szükséges jogosultságot körét a felhasználó közvetlen munkahelyi vezetője igényli az integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszerben.

392. A BVOP tekintetében az IFO, a bv. intézetek tekintetében a parancsok engedélyezi a jogosultságok beállítását.

393. Az informatikai szakterület a munkakör betöltéséhez szükséges jogosultságokat beállítja, majd rögzíti a beállítás dátumát és aláírásával igazolja a beállítás tényét a Login lapon.

394. A Login lapnak tartalmaznia kell a felhasználó nevét, login nevét, hadrendi számát, beosztását, rendfokozatát, valamint a számára beállított jogosultságokat.

395. A Login lap 1. számú aláírt példányát a Robotzsaruban nyilván kell tartani, az eredeti példányt lefűzve az informatikai szakterület tárolja. A Login lapból felhasználó kérelmére egy másolati példányt át kell adni.

Privilegizált felhasználókra vonatkozó rendelkezések

396. Privilegizált felhasználó feladatkörök: munkaköri leírás, vagy szerződéses felhatalmazás alapján végzett tevékenység, amely során az informatikai rendszer komponenseit, azok kapcsolatait fejlesztik, üzemeltetik, a komponensek állapotát felügyelik, vagy megváltoztatják informatikai szolgáltatások létrehozása, biztosítása és fenntartása érdekében.

397. Privilegizált felhasználói jogosultság: az adott szakmai folyamatot támogató informatikai szolgáltatás vonatkozásában:
    a) a nem szolgáltatás felületről végezhető tevékenységet lehetővé jog, függetlenül a szolgáltatás informatikai környezetétől,
    b) a technikai szolgáltatásokhoz és a nem szakmai folyamatot támogató szolgáltatásokhoz (tipikusan a fejlesztői alkalmazás-szolgáltatások) történő hozzáférés is,
    c) azon jogosultságok, amelyek bv. szervezet rendelkezése alapján kizárólag informatikusok feladatkört ellátóknak osztható ki.

398. Privilegizált felhasználói szerepkör: az informatikai rendszerben valamely feladat, feladatcsoport ellátását lehetővé tevő jogosultságok halmaza. A feladat jellegétől függően központi és helyi informatikus szerepköröket különböztetünk meg:
    a) rendszergazda,
    b) alkalmazás rendszergazda,
    c) fejlesztő.

399. Rendszergazda feladatai:
    a) ellátja az adatátviteli hálózatbiztonsági eszközök hardver- és szoftver felügyeletét
    b) gondoskodik a hálózaton áthaladó információk biztonságáról, a hálózati támadásoktól való védelemről,
    c) biztosítja a hálózati infrastruktúra működőképességét, felügyeletét.
    d) végrehajtja a rendszeres és eseti futtatási, archiválási, monitorozó tevékenységeket az alkalmazás üzemszerű működése érdekében,
    e) kialakítja a szerverek üzemi környezetét, telepíti és konfigurálja az szerverek szoftvereit,
    f) gondoskodik a szerverek üzemszerű működéséről,
    g) elvégzi a szükséges karbantartási műveleteket, teljesítmény-monitorozást végez,
    h) elvégzi a programverziók telepítését,
    i) munkaállomások, nyomtatók, valamint a helyi hálózati és adatátviteli eszközök és egyéb számítástechnikai műszaki eszközök üzemeltetése, és ezen eszközök üzemszerű működésének biztosítása, hibák elhárítása,
    j) a felhasználói munkaállomás futó szoftverek, paramétereinek beállításainak meghatározása az optimális működés biztosításának érdekében.

400. Alkalmazás rendszergazda feladatai:
    a) koordinálja az alkalmazás üzemszerű és szakmailag megfelelő működését, ennek érdekében: kapcsolatot tart az alkalmazás-informatikai rendszer fejlesztőjével, üzemeltetőjével, valamint utasítás alapján a szakmai felügyeletet ellátó szakterülettel,
    b) továbbá gondoskodik a fejlesztők által előállított verziók betöltéséről, teszteli a letöltött verziókat és a feltárt hibákról értesíti a fejlesztőket, illetve üzemeltetőket.

401. Fejlesztő feladatai:
    a) ellátja az alkalmazás fejlesztői feladatokat
    b) telepíti a szoftverfrissítéseket,
    c) végrehajtja a rendszeres és eseti futtatási, archiválási, monitorozó tevékenységeket az alkalmazás üzemszerű működése érdekében,
    d) elvégzi a programverziók telepítését,

Külső munkavállaló jogosultságaira vonatkozó rendelkezések

402. A bv. szervek külső munkavállalóira az adott szervezeti egységre vonatkozóan külső munkavállalói jogosultságtáblát kell kialakítani, amelynek részleteit (elsősorban kioszthatóó jogosultságok tekintetében) a szerv vezetője az irányítása alatt álló szerv tekintetében szabályozhatja, jóváhagyhatja.

403. Amennyiben a munkaszervezés hatékonysága érdekében szükséges, a bv. szerv vezetője – vezető munkakört betöltő – koordinátort jelölhet ki, aki felhatalmazása alapján jogosult

a külső munkavállalói jogosultságokkal kapcsolatos teendőket – az engedélyezést is beleértve – elvégezni.

404. A BVOP esetében a külső munkavállalói jogosultságokat az érintett engedélyező vezetőnek kell jóváhagynia.

405. A külső munkavállalói jogosultságok közé kizárólag azon – külső munkavállalóknak is kiadható – jogosultságok vehetők fel, amelyek a külső munkavállalót foglalkoztatót foglalkoztató szervezeti egység működése során a külső munkavállalók rendszeres feladatainak ellátásához szükségesek.

406. A külső munkavállaló felhasználói felvétele az informatikai rendszerbe a Kézikönyv szabályozásai alapján az erre a célra kialakított formanyomtatványon (Login lap) történik.

407. A külső munkavállaló felhasználó közvetlen vezetője
   a) az adott szervezeti egységre vonatkozó, munkavégzéshez szükséges jogosultságokat kérelmezi,
   b) a feladat ellátásához nem szükséges jogosultságokat haladéktalanul visszavonatja.

408. Külső munkavállaló számára jogosultságot konkrét feladatára tekintettel, csak a legszükségesebb időtartamra lehet engedélyezni. A jogosultság visszavonására a közvetlen vezető soron kívül köteles intézkedni, amennyiben a jogosultság használatának indoka megszűnt.

409. A külső munkavállalók számára kiadott jogosultságokat a külső munkavállalót foglalkoztató szervezeti egység vezetőjének évente, a tárgyévet követő év március 31-ig felül kell vizsgálni.

A jogosultságkezelés szabályai és szereplői

410. A bv. szervezet informatikai rendszereinek használata a területi (központi, helyi) és illetékességi szabályokhoz igazodik.

411. A bv. szerv helyi illetékességi jogosultság birtokában – az adott jogosultság keretein belül – a szerv felhasználója a saját illetékessége szerinti adatok elérésére jogosult.

412. Az országos illetékességű jogosultság birtokában – az adott jogosultság keretein belül - felhasználó valamennyi szerv adatainak elérésére jogosult.

413. Országos illetékességű jogosultság a bv. szervek felhasználói számára, valamint azon felhasználók esetében engedélyezhető, akiknek munkaköre, vagy feladatköre ezt kifejezetten indokolja.

414. Eltérő illetékességű jogosultságokat a felhasználó munkakörére, konkrét feladatára tekintettel, csak a legszükségesebb időtartamra lehet engedélyezni. Amennyiben a jogosultság használatának indoka megszűnt, a felhasználó munkavégzés helye szerinti közvetlen vezetője a jogosultság visszavonásáról soron kívül köteles intézkedni.

A közvetlen vezető

415. A közvetlen vezető felelős a szervezeti egység jogosultsági körének meghatározásáért, valamint a szervezeti egységhez tartozó felhasználó jogosultságainak aktualizálásáért. Ennek érdekében a közvetlen vezető igényelheti a szervezeti egység jogosultsági körének megváltoztatását (új jogosultság engedélyezését, vagy meglévő visszavonását), valamint – az IBK-ban meghatározott keretek között – szervezeti egység felhasználói számára jogosultságot igényelhet.

416. A közvetlen vezetőre saját jogosultságai tekintetében a felhasználókra vonatkozó szabályokat kell alkalmazni. E pont nem alkalmazandó, amennyibe a közvetlen vezető egyben engedélyező vezető is.

417. Új munkatárs szervezeti egységhez rendelése vagy a munkatárs munkakörének megváltozása esetén a közvetlen vezető az IBK-ban leírt feladatait az adatváltozást követő 3 munkanapon belül köteles végrehajtani.

418. A közvetlen vezető az IBK-ban foglalt feladatait másra nem delegálhatja. Távolléte esetén az említett feladatot felettes vezetője vagy a szervezeti egység helyettesítési rendje szerinti vezető látja el.

Engedélyező vezető

419. Az engedélyező vezető az általa vezetett szerv, vagy szervezeti egység vezetőinek igénylése alapján engedélyezi a szervezeti egységek jogosultságait, valamint az egyéni jogosultságigényléseket.

420. Az engedélyező vezető az IBK-ban foglalt feladatait a szervezeti hierarchiában az általa vezetett szervhez vagy szervezeti egységhez tartozó más vezetőre delegálhatja, amennyiben ezt az általa kiadott rendelkezés kifejezetten lehetővé teszi.

421. Az engedélyező vezető távolléte esetén feladatait a szerv helyettesítési rendje szerinti vezető látja el. Amennyiben szükséges, az engedélyező vezető előzetesen gondoskodik a helyettesek kijelölésről és a jogosultságkezelő alkalmazásban történő beállíttatásáról.

422. Az engedélyező vezető a közvetlen szervezeti egysége felhasználói tekintetében ellátja a közvetlen vezetői feladatokat is.

A jogosultság-adminisztrátor

423. A jogosultság adminisztrátor feladatokat a bv. szervnél az informatikai szakterület kijelölt munkatársai látják el.

424. A jogosultság adminisztrátor feladata:
   a) együttműködik a szervezeti egységek vezetőivel a jogosultsági körök meghatározásában, felülvizsgálatában,
   b) javaslatot tehet a jogosultsági körök módosítására,
   c) közreműködik az extra jogosultságok engedélyezési és visszavonási folyamatában, felülvizsgálatában

d) végrehajtja a jogosultsági körök kialakítására, illetve a jogosultságok kiadásával és visszavételével kapcsolatos technikai feladatokat,
e) rögzíti a külső munkavállalók jogosultságkezelő alkalmazásba történő felvételét és kiléptetését,
f) vezetői jogosultságok nyilvántartását,
g) a feladatok ellátásáról minden év március 31-ig összefoglaló jelentést készít.

425. A jogosultság-adminisztrátor feladata jogosultsági körök kialakításához, illetve az extra jogosultságok beállításához kapcsolódó technikai műveletek végrehajtása, amelyek eredményeképpen szervezeti egység, a felhasználó számára jogosultsági körök, illetve jogosultságok használhatóvá válnak. A feladat magába foglalja a jogosultsági körök igénylésének megfelelő létrehozását, jogosultságokkal való feltöltését és a felhasználókhoz a megfelelő jogosultságok rendelését.

426. A jogosultság-adminisztrátor a jogosultságok elektronikus úton történő igénylésének teljeskörű megvalósításáig az iratkezelési szabályoknak megfelelően kezeli a hozzá elektronikus úton beérkező igénylési kérelmek kinyomtatott és iktatott példányait.

A jogosultságkezelés felügyelete

427. A jogosultkezelés felügyeletét az IFO látja el, amely magában foglalja:
a) a jogosultágkezelő rendszer folyamatos figyelemmel kísérését,
b) a jogosultágkezelő alkalmazások szakmai felügyeleti feladatainak ellátását,
c) a jogosultágkezelést támogató technikai eszközök felülvizsgálatának, aktualizálásának kezdeményezését.

428. A bv. szervek jogosultsági köreinek tartalmát az IBF és az IFO együttműködve időszakosan összeveti és értékeli, a lényeges eltérések okait feltárja, az érintett vezetőkkel egyeztetve javaslatot tehet a jogosultság kezelés egységesítésére.

429. Az IFO vezetője
a) közreműködik az informatikai fejlesztések jogosultságkezelési elemeinek kidolgozásában és megvalósításában, véleményezi a kialakított jogosultságkezelési megoldásokat,
b) szakmailag támogatja a jogosultságadminisztrátorok munkáját,
c) a jogosultságkezeléssel kapcsolatban a hozzá beérkezett megkeresésekről, tájékoztatásokról nyilvántartást vezet,
d) jogosultságkezeléssel kapcsolatban ellenőrzést végez.

430. Az IBF feladatai ellátása érdekében tájékoztatást kérhet:
a) a jogosultság adminisztrátoroktól,
b) a rendszer működtetéséért felelős szervezeti egység munkatársától és
c) az érintett felhasználótól, amennyiben az ügy fontossága indokolja.

Elektronikus aláírások, valamint a távoli hozzáférés kezelésének szabályozása

431. Az elektronikus aláírásokhoz szükséges tanúsítványok:

Megnevezése	Típusa	Azonosítás típusa	Kibocsátó	Hordozó média	Kezelése
RSA	SecurID alapú VPN technológia	kétfaktoros authentikáció		Token	Informatika Főosztály
e-szigno	Tanúsítvány	Pinkód	Microsec	Szoftveres	Jogi Főosztály
Robotzsaru	Tanúsítvány	Pinkód	BM	Szoftveres	Koordinációs Főosztály
Giro	Tanúsítvány	Pinkód	MÁK	Chipkártya	Közgazdasági Főosztály
APN	Mobiltechnológia	Pinkód	T-systems	sim kártya	Informatika Főosztály
EESZT	Tanúsítvány	Pinkód	ÁEK	e-személyi	Egészségügyi Főosztály
KIRA	Tanúsítvány	Pinkód	MÁK	e-személyi	Közgazdasági Főosztály

432. A bv. szerv egyedileg azonosítja és hitelesíti a meghatározott eszközöket vagy eszköztípusokat, mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük. A birtoklás alapú hitelesítésre szolgáló eszközök kiadását kizárólag a kezelésre jogosult szakterület végezheti.

433. Az RSA kulcsok szerveroldali adminisztrációját az IFO-nál lévő alkalmazás rendszergazda végzi. A tanúsítványok és a kliensprogram telepítését a felhasználó végzi az IFO által kiadott telepítőkészlet és iránymutatás alapján

Az elektronikus aláírások használata

Alkalmazás	Használat célja	Védelmi szint		
		Fizikai védelem	Fájl szintű védelem	Jelszavas védelem
RSA	Távoli hozzáférés	Személyes	Eszközzel együtt	Igen
e-szigno	Elektronikus aláírás	Lemezszekrény	Eszközzel együtt	Igen
Robotzsaru	Elektronikus aláírás	Lemezszekrény	Eszközzel együtt	Igen
Giro	Elektronikus aláírás	Lemezszekrény	Eszközzel együtt	Igen
APN	Távoli hozzáférés	Személyes	Eszközzel együtt	Igen
EESZT	Token	Lemezszekrény	Eszközzel együtt	Igen
KIRA	Elektronikus aláírás	Lemezszekrény	Eszközzel együtt	Igen

434. A rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket vagy eszköz típusokat, mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.

435. A bv. szerv megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét.

436. A birtoklás alapú hitelesítő eszköz elvesztését és egyéb kompromittálódását a felhasználó azonnal köteles jelezni az IFO-nak, aki gondoskodik a fiók és a Token azonnali letiltásáról.

437. A letiltott eszköz újra aktiválása kizárólag a kezelésre jogosult szakterület engedélye alapján történhet.

438. Az elektronikus aláírások és tanúsítványok lejáratát az adott alkalmazáshoz tartozó alkalmazás rendszergazda, illetve a tanúsítvány kibocsátója figyeli.

439. A birtoklás alapú hitelesítési eszközök nyilvántartása az adott szakterület feladata. A nyilvántartás aktualitásának biztosításáért, a nyilvántartás naprakészen tartásáért az adott szakterület vezetője felel.

VII. ZÁRÓ RENDELKEZÉSEK

440. Jelen eljárásrendet évente felül kell vizsgálni.
441. Az eljárásrend a hatályos Cselekvési Tervel együtt érvényes, melynek kiadására az IFO vezetője és az IBF 2020. augusztus 30-ig intézkedik.