BELÜGYMINISZTÉRIUM
NEMZETI BIZTONSÁGI FELÜGYELET

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK

ÚTMUTATÓ AZ ÁLLAMI SZERVEZETEK MINŐSÍTETT ADATOT KEZELŐ RENDSZEREINEK ENGEDÉLYEZÉSÉHEZ ÉS ÜZEMELTETÉSÉHEZ

2018.

Iktatószám: BM/7312-2/2018.
Verzió: 1.1
Dátum: 2018. augusztus 3.

PREAMBULUM

A minősítet adatok védelmének alapvető szabályait a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.), a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet (a továbbiakban: 90/2010. Korm. rend) és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6.) Korm. rendelet (a továbbiakban: 161/2010. Korm. rend) határozza meg.

Jelen dokumentum a 161/2010. Korm. rend 4. § (1) bekezdés h) pont felhatalmazása alapján kerül kiadásra, mely felhatalmazza a minősített adatok hatósági felügyeletét ellátó Nemzeti Biztonsági Felügyeletet (a továbbiakban: NBF), hogy meghatározza az elektronikus biztonságra vonatkozó irányelveket, követelményeket és az engedélyezés szakmai követelményrendszerét.

A dokumentum segítséget kíván nyújtani a minősített adatot kezelő rendszerek tervezésében és üzemeltetésében, illetve a 161/2010. Korm. rend keretei közt további biztonsági követelményeket határoz meg az állami szervezetek által üzemeltetett, hálózati kapcsolattal nem rendelkező minősített adatot kezelő rendszerekkel szemben.

Ez a dokumentum 2018. szeptember 3-án lép hatályba.

SZEMÉLYI ÉS FIZIKAI BIZTONSÁG

Személyi biztonság

1. A minősített adatot kezelő rendszer felhasználóinak a törvényben meghatározott kivételekkel rendelkezniük kell felhasználói engedéllyel és aláírt titoktartási nyilatkozattal.
2. A felhasználóknak a törvényben meghatározott kivételekkel „Bizalmas!” és magasabb minősítési szintű adatok kezelése esetén az általuk hozzáférhető legmagasabb minősítési szintű adatnak megfelelő személyi biztonsági tanúsítvány is szükséges. Az előbbi feltételek a rendszerbiztonsági felügyelőre és a rendszeradminisztrátorra is vonatkoznak.
3. A rendszerbiztonsági felügyelőt és a rendszeradminisztrátort írásban kell kijelölni a feladat végrehajtására.

Fizikai biztonság

4. „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszer adminisztratív zónában is telepíthető. „Bizalmas!” és annál magasabb minősítési szintű adatot kezelő rendszert biztonsági területen kell telepíteni.
5. Abban a helyiségben, ahová a minősített adatot kezelő rendszert telepítették,
    a) tilos kép-, hang- és adatrögzítésre alkalmas eszközt bevinni,
    b) a munkavégzés alatt szolgálati mobiltelefon akkor vihető be, ha a hang- és képrögzítő funkciói, valamint az akusztikus kicsatolás jelentette kockázatok és azok kezelésének módja rögzítésre kerül az üzemeltetés-biztonsági szabályzat kockázatkezelésében,
    c) tilos biztonsági kamerás megfigyelőrendszert üzemeltetni,
    d) tilos a helyszínrajzban fel nem tüntetett informatikai eszközöket tárolni vagy üzemeltetni,
    e) a helyszínrajzban fel nem tüntetett számítógépes hálózati kapcsolatot meg kell szüntetni a kábelek eltávolításával vagy a fali portok lezárásával.
6. A II. osztályú biztonsági területre a személyi biztonsági tanúsítvánnyal nem rendelkező személy csak kísérettel léphet be. A ki és belépést regisztrálni kell.

ADMINISZTRATÍV BIZTONSÁG

Biztonsági dokumentáció

7. A minősített adatot elektronikus rendszeren kezelő szervnek biztonsági dokumentációt kell készítenie. A biztonsági dokumentáció betartása minden felhasználó számára kötelező. A biztonsági dokumentáció az üzemeltetés-biztonsági szabályzatból (a továbbiakban: ÜBSZ) és a rendszerbiztonsági követelményekből (a továbbiakban: RBK) áll. Az ÜBSZ-t minden minősített adatot kezelő rendszernél el kell készíteni. Az

RBK-t „Bizalmas!” és magasabb minősítési szintű, illetve hálózati kapcsolattal rendelkező „Korlátozott terjesztésű!” és magasabb minősítési szintű adatokat kezelő elektronikus rendszer esetében kell elkészíteni.

8. A biztonsági dokumentációt az NBF honlapján közzétett aktuális minták alapján kell elkészíteni. Az ÜBSZ elolvasásáról és tudomásulvételéről minden felhasználónak írásbeli nyilatkozatot kell tennie. Az ÜBSZ elolvasásáról szóló felhasználói nyilatkozatot a felhasználói engedély selejtezéséig kell megőrizni.

Biztonsági segédletek

9. A minősített adatot kezelő elektronikus rendszer üzemeltetésével kapcsolatos tevékenységet a biztonsági segédletekben kell rögzíteni. A biztonsági segédletek részét képzi a
    a) merevlemez kiadási napló,
    b) nyomtatási napló,
    c) ellenőrzési napló,
    d) karbantartási napló,
    e) hibás bejelentkezés nyilvántartása.
10. A biztonsági segédleteket nyilvántartásba kell venni és rendszeresen vezetni kell.
11. A minősített adatot tartalmazó adathordozók átadását és visszavételét a merevlemez kiadási naplóban kell vezetni. Amennyiben nem kivehető merevlemezt, hanem beépített adathordozóval rendelkező hordozható munkaállomást használnak, annak az átadását és átvételét is dokumentáltan kell végrehajtani. Ha a titkos ügykezelő és a rendszeradminisztrátor egy személy, akkor a merevlemez kivételét saját esetben nem kell adminisztrálni.
12. A minősített adatok nyomtatását a nyomtatási naplóban kell rögzíteni. Ha a minősített adatot kezelő elektronikus rendszer nem tartalmaz nyomtatót, nyomtatási naplót nem kell felfektetni. Amennyiben a minősített adatot kezelő elektronikus rendszer a Nyilvántartó helyiségben került telepítésre és a kinyomtatott minősített adatot a titkos ügykezelő azonnal nyilvántartásba veszi, nyomtatási naplót nem kell felfektetni. A rendszerbiztonsági felügyelő összehasonlítja a nyomtatási napló bejegyzéseit a minősített adatot kezelő rendszer nyomtatásról szóló naplóbejegyzéseivel.
13. A rendszerbiztonsági felügyelő az ellenőrzési naplóban rögzíti az elektronikus biztonsági előírások betartásának, rendszerbiztonsági feladatok végrehajtásának, hardverek védelmének, biztonsági beállítások, naplófájlok, biztonsági mentések, a jogosulatlan hozzáférési kísérletek, a rendszerhez nem tartozó eszközök illetéktelen csatlakoztatása elleni védelme, valamint a TEMPEST követelmények ellenőrzésének eredményét.
14. A rendszeradminisztrátor a karbantartási naplóban rögzíti az operációs rendszer és a vírusvédelmi szoftver frissítésének, illetve a további karbantartási tevékenységek elvégzését.

15. A minősített adatot kezelő elektronikus rendszernél legalább egy-egy vírus- és biztonsági esemény jelentő formanyomtatványt kell elhelyezni. A kitöltött formanyomtatványt nyilvántartásba kell venni.

Adathordozók kezelése

16. A minősített adatot kezelő elektronikus rendszerben alkalmazott adathordozót nyilvántartásba kell venni. Az adathordozón fel kell tüntetni a nyilvántartási számát, a rajta tárolható minősített adat nemzeti, EU, NATO jelölését (a továbbiakban: adatkör) és a legmagasabb minősítési szintet.

17. II. osztályú biztonsági területen telepített „Korlátozott terjesztésű!" minősítési szintű minősített adatot, illetve legfeljebb „Bizalmas!" minősítési szintű nemzeti minősített adatot kezelő elektronikus rendszerben beépített merevlemez alkalmazható, ha a merevlemez engedélyezett eljárással titkosításra került, ellenkező esetben kivehető merevlemezt kell alkalmazni. A merevlemez titkosítására szoftveres titkosító program használata engedélyezett. „Bizalmas!" és magasabb minősítési szintű adatokat kezelő elektronikus rendszerben kivehető merevlemezt kell alkalmazni vagy hordozható munkaállomás esetében, annak elzárását kell biztosítani a 20. pontban foglaltak szerint.

18. I. osztályú biztonsági területen telepített minősített adatot kezelő elektronikus rendszerben beépített merevlemez alkalmazható.

19. A minősített adatokat kezelő elektronikus rendszeren egy adathordozón több adatkör kezelhető.

20. A minősített adatot kezelő elektronikus rendszerben alkalmazott kivehető merevlemezt a minősítési szintjének megfelelően kell tárolni. „Korlátozott terjesztésű!" minősítési szintű adatot kezelő elektronikus rendszer kivehető merevlemeze a 90/2010. Korm. rend szerint zárható irodabútorban és lemezszekrényben is tárolható. „Bizalmas!" és annál magasabb minősítési szintű adatot kezelő elektronikus rendszer kivehető merevlemezét biztonsági tárolóban kell tárolni. A hordozható munkaállomást a minősítési szintjének megfelelően elzárva kell tárolni.

21. A biztonsági tárolót kizárólag a titkos ügykezelő nyithatja ki. Használat előtt a titkos ügykezelő adja ki a merevlemezt a felhasználó részére. Az átadás tényét a merevlemez kiadási naplóban dokumentálni kell. Használat után a felhasználó a merevlemez kiadási naplóban dokumentáltan visszaadja a merevlemezt a titkos ügykezelő részére.

22. Az adathordozókat életciklusuk végén ki kell vonni a használatból. A „Korlátozott terjesztésű!" és „Bizalmas!" minősítési szintű adatot tartalmazó adathordozót biztonságos adattörlési eljárást alkalmazó szoftverrel kell törölni, hogy a rajta tárolt minősített adat ne legyen helyreállítható. „Korlátozott terjesztésű!" minősítési szintű adathordozót háromszoros, „Bizalmas!" minősítési szintű adathordozót hétszeres törlési-felülírási metódussal kell törölni. Az SSD meghajtókat ATA Secure Erase eljárással kell törölni. A biztonságos eljárással törölt adathordozó újrafelhasználható.

23. A „Titkos!” és „Szigorúan titkos!” minősítési szintű adathordozót fizikailag meg kell semmisíteni, nem újrafelhasználható.

24. A törlést és a megsemmisítést erre a feladatra alakított, legalább 3 főből álló bizottság létrehozásával, jegyzőkönyv felvétele mellett, az erre vonatkozó adminisztratív szabályok betartásával kell végrehajtani.

HARDVERBIZTONSÁG

Kompromittáló kisugárzás elleni védelem

25. A „Titkos!” és „Szigorúan titkos!” minősítési szintű nemzeti minősített adatot kezelő rendszernek, valamint a „Bizalmas!”, vagy annál magasabb minősítési szintű külföldi minősített adatot kezelő rendszernek meg kell felelnie a kompromittáló kisugárzás elleni védelemre (a továbbiakban: TEMPEST) vonatkozó követelményeknek.

26. A TEMPEST követelményeket árnyékolt eszközök alkalmazásával, COTS eszközök árnyékolt helyiségben történő telepítésével vagy a megfelelő védőtávolságok tartásával kell teljesíteni.

27. Az adatkezelő helyszíneken a kezelt adatok minősítési szintjétől és a megállapított zóna besorolástól függően kell meghatározni az alkalmazott eszközök TEMPEST szintjét.

28. A TEMPEST követelményeknek való megfelelést tanúsítványokkal, illetve az NBF és a NATO által elvégzett zóna méréssel és zóna besorolással kell igazolni.

Eszközök jelölése, lezárása és nyilvántartása

29. A minősített adatot kezelő rendszer gépházán, képernyőjén, billentyűzetén, nyomtatóján és egyéb fő elemein jól láthatóan fel kell tüntetni a rendszeren kezelhető minősített adat legmagasabb minősítési szintjét.

30. A minősített adatot kezelő rendszer megbontható hardver eszközeit matricával, biztonsági címkével le kell zárni az illetéktelen hozzáférés megakadályozása, illetve felfedése érdekében.

31. A rendszerbiztonsági felügyelő külső adathordozó csatlakoztatásának kísérletével és a BIOS beállítások megtekintésével köteles ellenőrizni a 39. b) pontban előírt nem használt csatlakozó tiltását. A rendszerbiztonsági felügyelő a 13. pont előírásai szerint dokumentálja az ellenőrzés eredményét.

32. Az eszközök lezárásának sértetlenségét minden használat előtt ellenőrizni kell. A lezárások sérülését jelenteni kell, a kivizsgálást követően helyre kell állítani a biztonságot.

33. A minősített adatot kezelő rendszer hardver elemeiről naprakész nyilvántartást kell vezetni.

Eszközök karbantartása

34. A minősített adatot kezelő rendszer karbantartását a rendszerbiztonsági felügyelő engedélyezi. A karbantartást csak olyan személy végezheti, aki megfelel a szükséges személyi biztonsági követelményeknek. Ha eltávolították a minősített adatot tartalmazó adathordozót, vagy az engedélyezett eljárásokkal törölték, akkor nem szükséges a személyi biztonsági követelmények teljesítése.

35. A minősített adatot kezelő rendszer fő elemeinek cseréje és javításba adása a biztonsági vezető engedélyéhez és az NBF tájékoztatásához kötött. A minősített adatot kezelő rendszer részegységeinek kivonása, cseréje és javításba adása a biztonsági vezető engedélyéhez kötött. Az 1. sz. melléklet részletesen tartalmazza a minősített adatot kezelő rendszer változásaival kapcsolatos bejelentési és engedélyezési kötelezettségeket, intézkedéseket.

36. A TEMPEST tanúsítvánnyal rendelkező eszköz gyártója a tanúsítványban érvényességi időt határozhat meg. Ha lejárt az érvényességi idő, a gyártó újraméri az eszköz kisugárzását és arról új TEMPEST tanúsítványt állít ki.

37. A TEMPEST tanúsítvánnyal rendelkező eszköz megbontást igénylő javítása csak TEMPEST hatósági engedéllyel rendelkező szervezet által engedélyezett. Amennyiben a TEMPEST eszköz megbontása nem ennek megfelelően történik, vagy mégsérül a zárócímke, akkor az eszköz elveszti a tanúsítványát.

SZOFTVERBIZTONSÁG

BIOS beállítások

38. A minősített adatot kezelő rendszer BIOS beállításait adminisztrátori hozzáférést biztosító jelszóval kell védeni.

39. A BIOS-ban a következő biztonsági beállításokat kell elvégezni:

    a) külső adathordozók letiltása,

    b) nem használt kimeneti portok letiltása,

    c) nem használt vezetékes és vezeték nélküli hálózat kapcsolat hardveres tiltása,

    d) rendszerindítás korlátozása az elsődleges merevlemezre.

Operációs rendszer és biztonsági konfiguráció

40. A minősített adatot kezelő rendszert csak engedélyezett, jogtiszta licensz-szel, illetve gyártói támogatással rendelkező, naprakész operációs rendszerrel lehet üzemeltetni. A minősített adatot kezelő rendszeren a Microsoft Windows 7 és 8.1, illetve támogatással rendelkező Linux operációs rendszerek használata engedélyezett. A Microsoft Windows 10 operációs rendszer használata legfeljebb nemzeti „Szigorúan titkos!”, NATO és EU „Korlátozott terjesztésű!” minősítési szintű adatokat kezelő rendszeren engedélyezett.

41. A minősített adatot kezelő rendszer használata előtt el kell végezni az operációs rendszer biztonsági konfigurációját. Az operációs rendszeren a következő biztonsági beállításokat kell elvégezni:
    a) bejelentkezés Ctrl + Alt + Del billentyűkkel,
    b) előző felhasználó neve nem jelenik meg,
    c) rendszeren kezelt minősített adat minősítési szintjét és adatkörét tartalmazó figyelmeztető üzenet,
    d) jelszavas képernyővédelem,
    e) lomtár tiltása,
    f) vendég fiók tiltása,
    g) események előírt naplózása,
    h) fiók- és jelszóházirend.
42. Az operációs rendszert legalább havonta, offline módon frissíteni kell.

Adatfájl csere

43. A letiltott portok feloldásával és külső adathordozó csatlakoztatásával járó adatfájl cserét a felhasználó a külső adathordozó használatát engedélyező formanyomtatványon igényli. Az adatfájl cserét a biztonsági vezető engedélyezi.
44. A letiltott portok ideiglenes feloldását és adatfájl cserét a rendszerbiztonsági felügyelő felügyeletével a rendszeradminisztrátor végzi.
45. Fájl másolása iktatásba vett, kizárólag erre a célra alkalmazott adathordozó használatával történhet, amin feltüntetésre került az adathordozón kezelhető minősített adat legmagasabb minősítési szintje. Minden adathordozó vírusmentességét ellenőrizni kell. Magasabb minősítési szintű adatok nem importálhatóak más rendszerből.
46. Az adatfájl csere végrehajtása után a portokat újra le kell tiltani, majd az adatcserét dokumentálni kell a karbantartási naplóban. A kitöltött és iktatásba vett külső adathordozó használatát engedélyező formanyomtatványt a felhasználói engedély selejtezéséig kell megőrizni.

Felhasználói szoftverek

47. A minősített adatot kezelő rendszerre csak a munkavégzéshez feltétlenül szükséges, jogtiszta licensz-szel, illetve gyártói támogatással rendelkező, naprakész szoftvereket lehet telepíteni.
48. A szoftverek telepítését a biztonsági vezető engedélyével a rendszeradminisztrátor végzi. Az operációs rendszer és biztonsági szoftver telepítése és változtatása az NBF engedélyéhez kötött.
49. A minősített adatot kezelő rendszerre telepített szoftverekről naprakész nyilvántartást kell vezetni.

Vírusvédelem

50. A minősített adatot kezelő rendszeren a rosszindulatú szoftverek azonosítása és eltávolítása érdekében állandóan üzemelő vírusvédelmet kell alkalmazni.

51. A minősített adatot kezelő rendszeren csak engedélyezett, jogtiszta licensz-szel, illetve gyártói támogatással rendelkező vírusvédelmi szoftvert lehet alkalmazni.

52. A vírusvédelmi szoftvernek rendszerindításkor és külső adathordozó csatlakoztatásakor automatikus ellenőrzést kell végrehajtania, ennek hiányában a fájlokhoz történő hozzáférés előtt a víruskeresést manuálisan kell elindítani. A minősített adatot kezelő rendszerre telepíteni kívánt szoftveren vagy annak frissítésén vírusellenőrzést kell végrehajtani.

53. A vírusvédelmi szoftver vírusdefiníciós adatbázisát

    a) „Korlátozott terjesztésű!” minősítési szintű adatokat kezelő rendszeren legalább 4,

    b) „Bizalmas!” minősítési szintű adatokat kezelő rendszeren legalább 3,

    c) „Titkos!” és „Szigorúan titkos!” minősítési szintű adatokat kezelő rendszeren legalább 2 hetente kell offline frissíteni.

54. A vírusvédelmi szoftver vírusdefiníciós adatbázisát akkor is rendszeresen frissíteni kell, ha a minősített adatot kezelő rendszert nem használják.

55. Vírus jelenlétére utaló jelenség észlelése esetén a felhasználónak fel kell függesztenie a munkát, ki kell töltenie a Vírus esemény bejelentő lapot, majd értesítenie kell a rendszerbiztonsági felügyelőt.

Fiók- és jelszóházirend

56. A felhasználó azonosítása egyedi felhasználónév és jelszó alapján történik. A minősített adatot kezelő rendszerhez való hozzáférést biztosító jelszónak kis és nagy betű, szám és speciális karakter négyes kombinációból legalább hármat kell tartalmaznia. A jelszó hossza

    a) „Korlátozott terjesztésű!” minősítési szintű adatokat kezelő rendszeren legalább 8,

    b) „Bizalmas!” minősítési szintű adatokat kezelő rendszeren legalább 10,

    c) „Titkos!” és „Szigorúan titkos!” minősítési szintű adatokat kezelő rendszeren legalább 12 karakter.

57. A jelszavak élettartama nem lehet 90 napnál hosszabb. A korábban használt 24 jelszó használata és a jelszavak tárolása, valamint a könnyen kitalálható jelszavak használata nem engedélyezett.

58. A minősített adatot kezelő rendszerben kizárólag a rendszeradminisztrátor rendelkezik rendszergazdai jogosultságokkal.

59. A minősített adatot kezelő rendszer rendszerszintű jelszavai közé a rendszeradminisztrátor felhasználói fiókjához tartozó jelszó és a BIOS jelszó tartozik.

60. A rendszerszintű jelszavakat különálló, iktatásba vett, lepecsételt, lezárt borítékban, a rendszerre vonatkozó rendszerengedély által meghatározott legmagasabb minősítési szint biztonsági feltételeinek megfelelően kell tárolni.

61. Szükség esetén a rendszerszintű jelszavakat tartalmazó borítékok felbontására a rendszeradminisztrátor jogosult. A rendszeradminisztrátor akadályoztatása esetén a biztonsági vezető jogosult a rendszerszintű jelszavakat tartalmazó borítékok felbontására. Felbontás esetén a rendszerszintű jelszavakat új, azonos iktatási számmal megjelölt, lepecsételt lezárt borítékokban kell elhelyezni. Ha a rendszerszintű jelszavakat tartalmazó borítékot illetéktelen személy bontotta fel, a jelszavakat azonnal le kell cserélni.

62. A minősített adatot kezelő rendszerhez történő sikertelen és jogosulatlan hozzáférési kísérletek naplózásra kerülnek. A felhasználói hiba miatti sikertelen belépési kísérletet a hibás bejelentkezések nyilvántartásába kell rögzíteni. A harmadik sikertelen bejelentkezés után a felhasználó egy órára kizárásra kerül.

63. A felhasználói hibák és a jogosulatlan hozzáférési kísérletek megkülönböztetése érdekében a naplófájlokat és a hibás bejelentkezések nyilvántartását rendszeresen össze kell hasonlítani és ellenőrizni kell.

64. A felhasználó hozzáférését engedélyező formanyomtatványt iktatásba kell venni. A felhasználó hozzáférését engedélyező formanyomtatványt a felhasználói engedély selejtezéséig kell megőrizni.

Naplóházirend

65. A minősített adatot kezelő rendszer naplófájlban rögzíti a rendszeren végzett következő eseményeket:

    a) rendszerindítás, újraindítás, leállítás,

    b) felhasználói belépések, belépési kísérletek, kilépések,

    c) felhasználók és felhasználói csoportok jogosultságainak és privilégiumainak módosítása,

    d) nyomtatás,

    e) naplózási funkció indítása, illetve leállítása,

    f) a biztonsági naplózás adatrekordjainak törlése vagy ezekről másolat készítése,

    g) a rendszer dátum és idő módosítása,

    h) rendszer erőforrásokhoz történő hozzáférési kísérletek,

    i) automatikus riasztási funkciók működésének leállítása,

    j) valamely felhasználó rendszerre történő felvitele,

k) valamely felhasználó rendszerről történő leválasztása vagy hozzáférésének letiltása.

66. A naplófájl az előző pontban felsorolt események típusán kívül tartalmazza a felhasználó azonosítóját, az események dátumát, illetve az események sikeres, sikertelen kimenetelét.

67. A rendszerbiztonsági felügyelő a biztonsági dokumentációban meghatározott időközönként ellenőrzi a naplófájlok bejegyzéseit.

68. A minősített adatot kezelő rendszeren biztosítani kell az utolsó 6 hónapban készült naplófájlok elérhetőségét.

69. A rendszeradminisztrátor biztonsági mentést készít az elmúlt 6 hónapnál régebbi naplófájlokról. A naplófájlokról készült biztonsági mentést iktatásba vett adathordozón kell elhelyezni, amire javasolt az újraírható lemezek használata. A naplófájlokról készült biztonsági mentéseket 8 évig kell megőrizni. A naplófájlokról készült biztonsági mentést tartalmazó adathordozót a biztonsági területen található biztonsági tárolóban kell elhelyezni.

Biztonsági mentés

70. A minősített adatot kezelő rendszeren tárolt nem minősített dokumentumokról biztonsági mentés készíthető. A biztonsági mentés végrehajtásának módját, gyakoriságát és a rendszertől való elkülönített tárolását az ÜBSZ-ben kell meghatározni.

71. A biztonsági mentések kezelésénél figyelembe kell venni, hogy a minősített adatokról sokszorosított elektronikus példány készül, amelynek kezelése (iktatás, átadás, tárolás, betekintés, stb.) meg kell, hogy feleljen az általános szabályoknak.

Minősített adatot kezelő rendszer működésének felfüggesztése

72. Felhasználói igény hiányában a biztonsági vezető engedélyezheti a minősített adatot kezelő rendszer működésének felfüggesztését. A minősített adatot kezelő rendszer működésének felfüggesztése és az ismételt használata az NBF felé bejelentés-köteles.

73. A minősített adatot kezelő rendszer működésének felfüggesztését az NBF honlapján elérhető formanyomtatványon kell engedélyezni. A kitöltött és az érintettek által aláírt formanyomtatványt iktatásba kell venni, megőrzési ideje 8 év. A működés felfüggesztését át kell vezetni az ÜBSZ-be és a karbantartási naplóban is rögzíteni kell.

74. A minősített adatot kezelő rendszer adathordozóját a minősítési szintjének megfelelő módon kell tárolni. A rendszer elemeit – adathordozó nélkül – a biztonsági területen kell tárolni.

75. A rendszeradminisztrátor a minősített rendszer újbóli használata előtt felelős az operációs rendszer és a vírusadatbázis aktuális állapotra történő, majd rendszeres frissítéséért, továbbá a biztonsági konfiguráció végrehajtásáért.

76. A rendszerbiztonsági felügyelő a minősített rendszer újbóli használata előtt köteles ellenőrizni a rendszer naprakészségét, a biztonsági konfigurációt és a rendszerrel kapcsolatos további személyi, fizikai, adminisztratív biztonsági követelmények teljesülését. Az ellenőrzés eredményét az ellenőrzési naplóban kell rögzíteni.

77. A minősített adatot kezelő rendszer működésének meghosszabbítására irányuló rendszerengedély kérelem benyújtása előtt és az NBF által végrehajtott hatósági ellenőrzésről szóló értesítő kézhezvételét követően végre kell hajtani a fentiekben leírt frissítési, biztonsági konfigurációs és ellenőrzési tevékenységet.

Budapest, 2018. augusztus 3.

1. SZ. MELLÉKLET: MINŐSÍTETT ADATOT KEZELŐ RENDSZER VÁLTOZÁSAIVAL KAPCSOLATOS BEJELENTÉSI ÉS ENGEDÉLYEZÉSI KÖTELEZETTSÉGEK, INTÉZKEDÉSEK

Változás:	NBF engedélye	NBF tájékoztatása	Biztonsági vezető engedélye	Biztonsági vezető tájékoztatása	Rögzítés a rendszer dokumentációban, karbantartási naplóban
Minősítési szint és adatkör	X				
Adatkezelési engedély (rendszerengedélyt érintő)	X				
Rendszerbiztonsági felügyelő személye			X		X
Adminisztrátor személye			X		X
Helyszín	X				X
Helyiség berendezése			X		X
Helyiség berendezése (TEMPEST)			X		X
Helyiségben más rendszerek		X	X		
Helyiségben más rendszerek (TEMPEST)		X	X		
Helyiségben bútorzat				X	
Helyiségben bútorzat (TEMPEST)			X		
ÜBSZ átdolgozása			X		
RBK átdolgozása			X		
Felhasználók hozzáadása, törlése			X		
Munkaállomások, szerverek száma	X				X
Rendszer kapcsolat (külső vagy más rendszer, létesítés, megszüntetés)	X				X
Fődarab (monitor, alaplap, számítógépház, nyomtató, szkenner)		X	X		X
Részegység (videokártya, optikai meghajtó, egér, billentyűzet, mobil rack)			X		X
Alapvető szoftver (Operációs rendszer, biztonsági szoftver, vírusvédelem)	X				X
További szoftver		X	X		X
Külső adathordozó használata			X		
Helyszíni javítás (kivéve TEMPEST eszköz)			X		X
Javításba adás (kivéve TEMPEST eszköz)		X	X		X
TEMPEST javítás	X				X
Külső adathordozó hozzárendelése, megszüntetése			X		X
Vírusadatbázis frissítés					X
Op. rendszer és szoftver frissítés, karbantartás					X