NEMZETI BIZTONSÁGI FELÜGYELET

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK

A GAZDÁLKODÓ SZERVEZETEK MINŐSÍTETT ADATOT KEZELŐ RENDSZEREINEK ENGEDÉLYEZÉSÉHEZ ÉS ÜZEMELTETÉSÉHEZ

2020.

Iktatószám: 30710-1/884-1/2020.
Verzió: 2.0
Dátum: 2020. március 26.

PREAMBULUM

A minősített 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: Kr.) és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6.) Korm. rendelet (a továbbiakban: Er.) határozza meg.

Jelen dokumentum az Er. 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 az Er. keretei közt további biztonsági követelményeket határoz meg az állami szervezetek által üzemeltetett, hálózati kapcsolattal nem rendelkező minősített adatot kezelő rendszerekkel szemben.

Ez a dokumentum kiadása napján lép hatályba.

FIZIKAI BIZTONSÁG

Fizikai biztonság követelményei

1. Abban a helyiségben, ahová a minősített adatot kezelő rendszert telepítették,
    a) rögzíteni kell a kép-, hang- és adatrögzítésre alkalmas eszközök bevitelének és használatának szabályait,
    b) tilos biztonsági kamerás megfigyelőrendszert üzemeltetni,
    c) tilos a helyszínrajzban fel nem tüntetett informatikai eszközöket tárolni vagy üzemeltetni,
    d) a helyszínrajzban fel nem tüntetett számítógépes hálózati kapcsolatot meg kell szüntetni a kábelek eltávolításával vagy a fali portok lezárásával.

ADMINISZTRATÍV BIZTONSÁG

Biztonsági dokumentáció

2. A minősített adatot elektronikus rendszeren kezelő szervnek az Er.-ben leírtak szerint biztonsági dokumentációt kell készítenie az NBF honlapján közzétett minták alapján. A felhasználói nyilatkozatokat a felhasználói engedély selejtezéséig meg kell őrizni.
3. Az Üzemeltetés-biztonsági Szabályzat (a továbbiakban ÜBSZ) kötelező tartalmi elemei:
    a) a rendszer jellegének meghatározása (rendeltetése, minősítése, felhasználói),
    b) a rendszer felügyeletéért és üzemeltetéséért felelős szervezeti egységek és személyek meghatározása, kötelezettségeik,
    c) biztonsági adminisztráció (rendszerhez történő hozzáférés és annak megszűnése, kötelező képzések),
    d) lokációval kapcsolatos elemek,
        - az érintett helyszín meghatározása, fizikai körülhatárolása,
        - belépésre vonatkozó szabályok,
        - munkaidőn kívüli feladatvégzésre vonatkozó előírások,
        - a biztonságtechnikai eszközökkel kapcsolatos feladatok meghatározása,
    e) dokumentumbiztonsággal kapcsolatos elemek,
        - elektronikus és papír alapú adathordozók kezelésének szabályai,
        - iktatásra vonatkozó előírások,
        - minősítési jelölések alkalmazása,
        - tárolásra/továbbításra/ átadásra vonatkozó szabályok,
        - külső adathordozó használatára vonatkozó előírások,

- nyomtatás szabályai,

f) kép- és hang rögzítésére vonatkozó előírások,

g) hardverkonfiguráció / szoftverkonfiguráció részletes szabályai,

- üzembe helyezés,
- karbantartás
- telepítésre és frissítésre vonatkozó előírások
- biztonsági és naplózási beállítások

h) vírusvédelemre vonatkozó előírások

i) biztonsági incidensek kezelése

j) vészhelyzetben alkalmazandó előírások / a helyreállítás menetének folyamata

k) kockázatelemzés *(kizárólag Rendszerbiztonsági Követelmények (a továbbiakban: RBK) el nem készülte esetén kötelező tartalmi elem)*

l) konfigurációmenedzsment *(kizárólag RBK el nem készülte esetén kötelező tartalmi elem)*

m) alkalmazott segédletek listája *(kizárólag RBK el nem készülte esetén kötelező tartalmi elem)*

4. Az RBK kötelező tartalmi elemei:

a) a rendszer jellegének meghatározása (rendeltetése, minősítése, felhasználói),

b) a rendszer hardver- és szoftverkörnyezetéért felelős szervek és személyek meghatározása,

c) adatok ki- és bevitelére vonatkozó előírások,

d) a rendszer felhasználóinak meghatározása,

e) biztonsági menedzsment,

f) kockázatelemzés,

g) a telepítés helyszínének ismertetése,

h) hozzáférésre vonatkozó előírások (felhasználó-azonosítás, hozzáférés felügyelete)

i) ellenőrzési metodika

j) konfigurációmenedzsment

k) biztonsági jellegű események kezelésére vonatkozó előírások

l) biztonsági oktatás rendje

m) újraakkreditálás szabályai

Biztonsági segédletek

5. A minősített adatot kezelő elektronikus rendszer üzemeltetésével kapcsolatos tevékenységet olyan biztonsági segédletekben kell rögzíteni, amelyek a rendszer részét képezik és visszakereshetően tartalmazzák a biztonságos üzemeltetéshez kapcsolódó adatokat. A biztonsági segédleteknek az alábbiakat kell biztosítani:
    a) minősített adathordozó személyhez kötését,
    b) a kinyomtatott anyagok nyomon követését,
    c) az ellenőrzések, karbantartási események rögzítését.
6. Ezek megvalósítására ki lehet alakítani papír alapú, vagy elektronikus nyilvántartást az alábbiak teljesítésével:
    a) A minősített adatot tartalmazó adathordozók, vagy a hordozható munkaállomás átadását és visszavételét úgy kell végrehajtani, hogy a személyhez kötés biztosított legyen.
    b) A kinyomtatásra vonatkozó adatokat úgy kell rögzíteni, hogy azok azonosításhoz szükséges információt biztosítsanak a kinyomtatástól az iktatásba vételig.
    c) Biztosítani kell, hogy a végrehajtott ellenőrzések és karbantartási események, frissítések, illetve a biztonságot befolyásoló események (pl. vírusfertőzés, szabálytalan használat) rögzítésre kerüljenek.

Adathordozók kezelése

7. A rendszerben alkalmazott adathordozót a Kr.-ben és az Er.-ben foglaltak szerint kell kezelni. Alkalmazható az adathordozók szoftveres titkosítása.
8. I. osztályú biztonsági területen telepített minősített adatot kezelő elektronikus rendszerben beépített merevlemez alkalmazható.
9. A minősített adatokat kezelő elektronikus rendszeren egy adathordozón több adatforrás (nemzeti, NATO, EU) kezelhető, de a logikai elkülönítést biztosítani kell.
10. 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.
11. A „Titkos!” és „Szigorúan titkos!” minősítési szintű adathordozót fizikailag meg kell semmisíteni, nem újrafelhasználható.

Ellenőrzések rendje

12. Az alábbi táblázat a minősített adatot kezelő rendszerek ellenőrzésére vonatkozó kritériumokat tartalmazza. Az ellenőrzésről minden esetben dokumentáció készül.

Ellenőrzés tárgya	Ellenőrzést végző személy	Ellenőrzés gyakorisága
munkaállomás, csatlakozások állapota, sértetlensége	felhasználó	használat előtt
adathordozók	rendszeradminisztrátor, rendszerbiztonsági felügyelő	használat előtt
naplófájlok, nyomtatási napló, biztonsági mentések	rendszerbiztonsági felügyelő	4 hetente
engedélyezett telepített szoftverek	rendszeradminisztrátor	3 havonta
BIOS beállítások	rendszeradminisztrátor	3 havonta
ellenőrzési, karbantartási, merevlemez kiadási nyilvántartások	biztonsági vezető	6 havonta
TEMPEST matricák sértetlensége	rendszerbiztonsági felügyelő	3 havonta

HARDVERBIZTONSÁG

Kompromittáló kisugárzás elleni védelem

13. 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 az Er.-ben rögzített kompromittáló kisugárzás elleni védelemre (a továbbiakban: TEMPEST) vonatkozó követelményeknek, a telepítési helyszín adottságainak megfelelően.

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

15. A telepített eszközök esetében a megállapított zónától függetlenül a minősített adatot feldolgozó, Level A paraméterekkel rendelkező számítógépektől legalább 50 cm-es távolságot kell biztosítani más berendezésektől. Level B eszköz esetén ez a távolság jelátviteli eszköztől (pl. rádióadó-vevő) 1 m, más berendezéstől 50 cm. TEMPEST paraméterrel nem rendelkező berendezés esetén ezek a távolságok 2, illetve 1 méter.

Eszközök jelölése, lezárása és nyilvántartása

16. A minősített adatot kezelő rendszer hardver elemeinek nyilvántartását, jelölését, lezárást az Er.-ben foglaltak szerint kell elvégezni.

17. A rendszerbiztonsági felügyelő külső adathordozó csatlakoztatásának kísérletével és az alaplapi biztonsági beállítások megtekintésével köteles ellenőrizni a 23. a) pontban előírt nem használt csatlakozások tiltását.

Eszközök karbantartása

18. A minősített adatot kezelő rendszer karbantartásának szabályait az Er. tartalmazza.
19. A minősített adatot kezelő rendszer fő elemeinek cseréje, javításba adása, részegységeinek kivonása a biztonsági vezető engedélyéhez kötött. Az 1. sz. melléklet részletesen tartalmazza a minősített adatot kezelő rendszer módosításával kapcsolatos bejelentési és engedélyezési kötelezettségeket, intézkedéseket.
20. 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.
21. A TEMPEST tanúsítvánnyal rendelkező eszköz megbontást igénylő javítását csak az arra jogosult szervezet végezheti. Amennyiben a TEMPEST eszköz megbontása nem ennek megfelelően történik, vagy megsérül a zárócímke, akkor az eszköz elveszti a tanúsítványát.

SZOFTVERBIZTONSÁG

BIOS beállítások

22. A minősített adatot kezelő rendszer alaplapi biztonsági beállításait (BIOS/UEFI) adminisztrátori hozzáférést biztosító jelszóval kell védeni.
23. A BIOS-ban a következő biztonsági beállításokat kell elvégezni:
    a) nem használt kimeneti portok letiltása,
    b) nem használt vezetékes és vezeték nélküli hálózat kapcsolat hardveres tiltása,
    c) rendszerindítás korlátozása az elsődleges adathordozóra.

Operációs rendszer és biztonsági konfiguráció

24. A minősített adatot kezelő rendszert csak engedélyezett, jogtiszta licensszel, illetve gyártói támogatással rendelkező, naprakész operációs rendszerrel lehet üzemeltetni. A minősített adatot kezelő rendszeren a Microsoft Windows 10, illetve támogatással rendelkező Linux operációs rendszerek használata engedélyezett. A korábban engedélyezett, működő rendszerek esetében alkalmazható a Windows 7 operációs rendszer. Az operációs rendszer változtatása az NBF engedélyéhez kötött.
25. 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 forrását, valamint az illetéktelen használatra vonatkozó büntetőjogi következményeket tartalmazó figyelmeztető üzenet,

d) jelszavas képernyővédelem,

e) lomtár tiltása,

f) vendég fiók tiltása,

g) események 40-44. pontok szerinti naplózása,

h) fiók- és jelszóházirend.

Adatfájl csere

26. A letiltott portok feloldásával és külső adathordozó csatlakoztatásával járó adatfájl cserét ellenőrzött módon szükséges végrehajtani a jóváhagyott biztonsági szabályzatban foglaltak szerint.

Felhasználói szoftverek

27. A minősített adatot kezelő rendszerre csak a munkavégzéshez feltétlenül szükséges, jogtiszta licensszel, illetve gyártói támogatással rendelkező, naprakész szoftvereket lehet telepíteni.

Vírusvédelem

28. Az Er.-ben előírt vírusvédelemhez jogtiszta licensszel, illetve gyártói támogatással rendelkező, valamint offline frissíthető szoftvert kell alkalmazni, amelynek változtatása az NBF engedélyéhez kötött. A Microsoft operációs rendszerek részét képező Windows Defender is alkalmazható erre a célra.

29. 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 szükséges offline frissíteni.

30. A rendszer működésének felfüggesztése esetén a vírusvédelmi szoftvert csak az ismételt használatba vétel előtt szükséges frissíteni.
31. Vírus jelenlétére utaló jelenség észlelése esetén a felhasználónak fel kell függesztenie a munkát és értesítenie kell a rendszerbiztonsági felügyelőt.

Fiók- és jelszóházirend

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

a) „Korlátozott terjesztésű!” minősítési szintű adatokat kezelő rendszeren legalább 12 karakter,

b) „Bizalmas!” vagy annál magasabb minősítési szintű adatokat kezelő rendszeren legalább 15 karakter.

33. A jelszavak élettartama nem lehet 90 napnál hosszabb. A korábban használt 24 jelszó használata nem engedélyezett. A felhasználók figyelmét fel kell hívni a könnyen kitalálható jelszavak mellőzésére, illetve arra, hogy a jelszavak visszakereshető rögzítése elkerülendő.

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

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

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

37. 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 haladéktalanul le kell cserélni.

38. Az Er. alapján a minősített adatot kezelő rendszerhez történő sikertelen és jogosulatlan hozzáférési kísérletek naplózásra kerülnek. A harmadik sikertelen bejelentkezés után a felhasználó egy órára kizárásra kerül.

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

Naplóházirend

40. 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.

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

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

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

44. A rendszeradminisztrátor biztonsági mentést készít a 6 hónapnál régebbi naplófájlokról, amit iktatásba vett adathordozón kell tárolni, a biztonsági vezető által meghatározott helyen. A naplófájlokról készült biztonsági mentéseket 8 évig kell megőrizni.

Biztonsági mentés

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

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

Minősített adatot kezelő rendszer működésének felfüggesztése

47. Gazdálkodó szervezetek esetében 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.

48. 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 a karbantartási naplóban is rögzíteni kell.

49. A felfüggesztés ideje alatt a rendszer adathordozóját a minősítési szintjének megfelelő módon kell tárolni. A rendszer adathordozó nélküli elemei esetében is biztosítani kell az illetéktelen hozzáférés kizárását.

50. 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.

51. 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 rögzíteni szükséges.
52. 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, 2020. március 26

Készült: 1 pld. elektronikusan NBF honlap

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

Változás:	NBF engedélye	NBF tájékoztatása	Biztonsági vezető engedélye	Rögzítés a rendszer dokumentációban.
Minősítési szint és adatforrás	X			
Adatkezelési engedély (rendszerengedélyt érintő)	X			
Rendszerbiztonsági felügyelő személye			X	X
Adminisztrátor személye			X	X
Helyszín	X			X
Helyiség berendezése			X	X
Helyiségben más rendszerek		X	X	
Helyiségben bútorzat			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
Új (korábban nem engedélyezett) nyomtatási képesség	X			X
Részegység (videokártya, optikai meghajtó, egér, billentyűzet, mobil rack, stb)			X	X
Alapvető szoftver (Operációs rendszer, biztonsági szoftver, vírusvédelem)	X		X	X
További szoftver		X	X	X
Külső adathordozó használata			X	
Helyszíni javítás			X	X
Javításba adás (TEMPEST is)		X	X	X
Külső adathordozó hozzárendelése, megszüntetése			X	X
Vírusadatbázis frissítés				X
Op. rendszer és szoftver frissítés, karbantartás				X