

NEMZETI BIZTONSÁGI FELÜGYELET

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK

az állami szervezetek minősített adatot kezelő rendszereinek
engedélyezéséhez és üzemeltetéséhez

2021.

Iktatószám: 30710-3/556/2021

Verzió: 3.0

Dátum: 2021. június 4.

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: 90/2010. Korm. rendelet) 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 és célja, hogy – az Er. rendelkezéseinek megfelelően – az állami szervek által üzemeltetett, hálózati kapcsolattal nem rendelkező minősített adatot kezelő rendszerekre vonatkozóan meghatározza az elektronikus biztonságra vonatkozó irányelveket, követelményeket és az engedélyezés szakmai követelményrendszerét, továbbá segítséget nyújtson a minősített adatot kezelő rendszerek tervezésében és üzemeltetésében.

FIZIKAI BIZTONSÁG

1. Fizikai biztonsági követelmények

- 1.1. A 90/2010. Korm. rendeletben és az Er.-ben foglaltakon túl a minősített adatot kezelő rendszer telepítési helyszínén:
- a) tilos a helyszínrajzon fel nem tüntetett informatikai eszközöket tárolni vagy üzemeltetni,
 - b) a külső kapcsolódás kizárása érdekében a használaton kívüli kapcsolati lehetőségeket meg kell szüntetni, vagy elérhetetlenné kell tenni,
 - c) a minősített adatot megjelenítő eszközt úgy kell elhelyezni, hogy annak tartalma illetéktelen személy számára (pl. ablakon keresztül rálátással) ne legyen érzékelhető.

ADMINISZTRATÍV BIZTONSÁG

2. Biztonsági dokumentáció

- 2.1. A minősített adatot elektronikus rendszeren kezelő szerv köteles biztonsági dokumentációt készíteni.
- 2.2. Az üzemeltetés-biztonsági szabályzat (a továbbiakban ÜBSZ) kötelező tartalmi elemei:
- a) a rendszer jellegének meghatározása (a rendszer által kezelhető minősített adat legmagasabb minősítési szintje, a rendszer rendeltetése, a rendszer felhasználói);
 - b) a rendszer felügyeletéért és üzemeltetéséért felelős szervezeti egységek és személyek meghatározása, kötelezettségeik rögzítése;
 - c) a rendszer biztonságához kapcsolódó adminisztrációval összefüggő rendelkezések meghatározása (a rendszerhez történő hozzáférés feltételei és annak megszűnése, kötelező képzések);
 - d) a telepítési helyet érintően az alábbiak meghatározása szükséges:
 - a telepítési helyszín környezetének leírása,
 - a rendszerelemek (munkaállomások, szerverek, nyomtatók, fődarabok) üzemeltetésének a helyszíne,
 - amennyiben a fenti rendszerelemek tárolása eltérő helyszínen történik, annak meghatározása,
 - a munkaidő befejezésekor a munkaállomással és a kivehető merevlemezzel kapcsolatos feladatok meghatározása;
 - a biztonságtechnikai eszközökkel kapcsolatos feladatok meghatározása;
 - e) a dokumentumbiztonságot érintő rendelkezések meghatározása:

- a minősített adatot tartalmazó elektronikus adathordozók kezelésére vonatkozó speciális szabályok rögzítése,
 - a rendszer főbb elemein a rendszer által kezelhető minősített adat legmagasabb minősítési szintjének feltüntetésére vonatkozó rendelkezések rögzítése,
 - a külső adathordozó használatára vonatkozó speciális előírások,
 - a rendszeren végzett nyomtatás speciális szabályai;
- f) kép és hang rögzítésére vonatkozó előírások rögzítése;
- g) hardverkonfiguráció és szoftverkonfiguráció részletes szabályainak meghatározása:
- üzembe helyezés,
 - karbantartás,
 - telepítésre és frissítésre vonatkozó előírások,
 - biztonsági és naplózási beállítások;
- h) vírusvédelemre vonatkozó előírások meghatározása;
- i) biztonsági incidensek kezelésére vonatkozó rendelkezések meghatározása;
- j) vészhelyzetben alkalmazandó előírások meghatározása és a helyreállítás folyamatára vonatkozó rendelkezések rögzítése;
- k) kockázatelemzés;
- l) konfigurációmenedzsment;
- m) a biztonsági oktatás rendjének meghatározása;
- n) alkalmazott segédletek listája.
- 2.3. „Bizalmas!” vagy magasabb minősítési szintű adatot kezelő rendszer esetében, vagy az internetre vagy más nyilvános hálózathoz kapcsolódó „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszer esetében a kockázatelemzést, a konfigurációmenedzsmentet, a biztonsági oktatás rendjének meghatározását és az alkalmazott segédletek listáját a rendszerbiztonsági követelményekben (a továbbiakban: RBK) kell rögzíteni.
- 2.4. Az ÜBSZ tudomásul vételéről és az abban foglaltak betartásáról szóló felhasználói nyilatkozatokat a felhasználói engedély selejtezéséig kell megőrizni.
- 2.5. A rendszerbiztonsági követelmények kötelező tartalmi elemei:
- a) a rendszer jellegének meghatározása (rendeltetése, a rendszeren kezelhető minősített adat legmagasabb minősítési szintje, felhasználói);
 - b) a rendszer hardver- és szoftverkörnyezetéért felelős szervek és személyek meghatározása;

- c) az adatok ki- és bevitelére vonatkozó előírások rögzítése;
- d) a rendszer felhasználóinak meghatározása;
- e) a rendszer biztonságáért felelős személyek meghatározása nevük és elérhetőségük megjelölésével;
- f) a telepítés helyszínének ismertetése;
- g) a hozzáférésre vonatkozó előírások meghatározása (felhasználó-azonosítás, hozzáférés felügyelete);
- h) az ellenőrzési metodika rögzítése;
- i) a biztonsági jellegű események kezelésére vonatkozó előírások rögzítése;
- j) a biztonsági oktatás rendjének meghatározása;
- k) az újraakkreditálás szabályainak rögzítése;
- l) a kockázatelemzés;
- m) a konfigurációmenedzsment leírása;
- n) alkalmazott segédletek listája.

3. Biztonsági segédletek

- 3.1. A minősített adatot kezelő elektronikus rendszer üzemeltetésével kapcsolatos tevékenységet olyan biztonsági segédletekben kell rögzíteni, amelyek visszakereshetően tartalmazzák a biztonságos üzemeltetéshez kapcsolódó adatokat.
- 3.2. E célból papír alapú, vagy elektronikus nyilvántartás hozható létre, amelynek az alábbi követelményeket kell teljesítenie:
 - a) a rendszerelemek átadását és visszavételét úgy kell végrehajtani, hogy abból egyértelműen megállapítható legyen az adott rendszerelemért felelős személy;
 - b) a nyomtatásra vonatkozó adatokat úgy kell rögzíteni, hogy a kinyomtatott adatok nyomon követése folyamatosan biztosított legyen;
 - c) biztosítani kell, hogy a végrehajtott ellenőrzések, karbantartások, frissítések, illetve a biztonságot befolyásoló események (pl. vírusfertőzés, szabálytalan használat) rögzítésre kerüljenek.

4. Adathordozók kezelése

- 4.1. A minősített adatot tartalmazó adathordozók védelme érdekében szoftveres titkosítás alkalmazható, azonban ez nem helyettesíti a minősítésének megfelelő védelmet.
- 4.2. I. osztályú biztonsági területen telepített minősített adatot kezelő elektronikus rendszerben beépített merevlemez is alkalmazható.
- 4.3. A minősített adatokat kezelő elektronikus rendszeren egy adathordozón több forrásból (nemzeti, NATO, EU) származó adat kezelhető, a minősített adatok logikai úton történő elkülönítését azonban biztosítani kell.

- 4.4. A minősített adatot kezelő elektronikus rendszert tartalmazó elsődleges adathordozó cseréjéről az NBF tájékoztatása szükséges. A bejelentés során az eszköz típusát és gyári azonosító számát is meg kell küldeni a hatóság részére.
- 4.5. Az adathordozókat életciklusuk végén ki kell vonni a használatból. A „Korlátozott terjesztésű!” és a „Bizalmas!” minősítési szintű adatot tartalmazó adathordozót – annak érdekében, hogy a rajta tárolt minősített adat ne legyen helyreállítható – biztonságos adattörlési eljárást alkalmazó szoftverrel kell törölni. „Korlátozott terjesztésű!” minősítési szintű adathordozót háromszoros, „Bizalmas!” minősítési szintű adathordozót hétszeres törlési-felülírási módszerrel kell törölni. Az SSD meghajtókat ATA Secure Erase eljárással kell törölni. A biztonságos eljárással törölt adathordozó újra felhasználható.

5. Ellenőrzések rendje

A minősített adatot kezelő rendszerek ellenőrzését az alábbi táblázatban szereplő személyek, az abban meghatározott időközönként kötelesek végrehajtani. A biztonsági vezető, a rendszerbiztonsági felügyelő, valamint a rendszeradminisztrátor az ellenőrzést dokumentált módon köteles végrehajtani.

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

HARDVERBIZTONSÁG

6. Kompromittáló kisugárzás elleni védelem

- 6.1. A TEMPEST követelményeknek való megfelelést tanúsítványokkal, illetve a Nemzeti Biztonsági Felügyeletet (a továbbiakban: NBF) vagy a NATO illetékes szervezete által elvégzett zóna méréssel és zóna besorolással kell igazolni.
- 6.2. Az eszközök elhelyezésénél figyelembe kell venni az egyéb elektronikus eszközöktől, berendezésektől való távolságot.

7. Eszközök karbantartása

- 7.1. A rendszer elemeinek karbantartása során figyelembe kell venni az 1. sz. mellékletben foglalt változásokkal, módosításokkal kapcsolatos bejelentési, engedélyezési és intézkedési kötelezettséget.
- 7.2. A TEMPEST tanúsítvánnyal rendelkező eszköz gyártója a tanúsítványban érvényességi időt határozhat meg. Ha lejárt az érvényességi idő, az arra engedélyezett laboratóriumban az eszköz kisugárzási paramétereinek ismételt megállapítása után új TEMPEST tanúsítvány állítható ki.
- 7.3. 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

8. BIOS beállítások

- 8.1. A minősített adatot kezelő rendszerben kizárólag a rendszeradminisztrátor rendelkezhet rendszergazdai jogosultságokkal.
- 8.2. A minősített adatot kezelő rendszer alaplapi biztonsági beállításait (BIOS/UEFI) adminisztrátori hozzáférést biztosító jelszóval kell védeni.
- 8.3. A BIOS-ban a következő biztonsági beállításokat kell elvégezni:
 - a) használaton kívüli kimeneti portok letiltása,
 - b) használaton kívüli vezetékes és vezeték nélküli hálózati kapcsolat hardveres tiltása,
 - c) rendszerindítás korlátozása az elsődleges adathordozóra.

9. Operációs rendszer és biztonsági konfiguráció

- 9.1. A minősített adatot kezelő rendszert csak engedélyezett, jogtiszt licensszel, illetve gyártói támogatással rendelkező, naprakész operációs rendszerrel lehet üzemeltetni. A minősített adatot kezelő rendszeren kizárólag a Microsoft Windows 10, illetve a támogatással rendelkező Linux operációs rendszerek használata engedélyezett. A

korábban engedélyezett, működő rendszerek esetében a Microsoft Windows 7 operációs rendszer 2022. december 31-ig alkalmazható. Az operációs rendszer változtatása az NBF előzetes engedélyéhez kötött.

- 9.2. A 9.1. ponttól eltérően a Microsoft Windows 7 operációs rendszerről Microsoft Windows 10 operációs rendszerre történő frissítés – az ingyenes gyártói támogatás megszűnésére figyelemmel – nem engedélyköteles, a frissítésről azonban szükséges az NBF-et tájékoztatni.
- 9.3. 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) a bejelentkezéshez a Ctrl + Alt + Del billentyűkombináció alkalmazása;
 - b) a bejelentkezési képernyőn az előző felhasználó neve nem jelenhet meg;
 - c) a Ctrl + Alt + Del billentyűkombináció alkalmazását követően meg kell jeleníteni a rendszeren kezelt minősített adat minősítési szintjét és forrását, valamint az illetéktelen használatra vonatkozó büntetőjogi következményeket tartalmazó figyelmeztető üzenet;
 - d) a jelszavas képernyővédelem biztosítása;
 - e) a lomtár tiltása;
 - f) a vendég fiók tiltása;
 - g) az események 14. pont szerinti naplózása;
 - h) a fiók- és jelszóházi rend beállítása.

10. Adatfájl csere

A letiltott portok feloldásával és a külső adathordozó csatlakoztatásával járó adatfájl cserét, majd ezt követően a port tiltását a jóváhagyott biztonsági szabályzatban foglaltak szerint a rendszeradminisztrátor által ellenőrzött módon szükséges végrehajtani.

11. Felhasználói szoftverek

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

12. Vírusvédelem

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

12.2. A vírusvédelmi szoftver vírusdefiníciós adatbázisát

- a) legfeljebb „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszeren legalább 4 hetente,
- b) legfeljebb „Bizalmas!” minősítési szintű adatot kezelő rendszeren legalább 3 hetente,
- c) legfeljebb „Titkos!”, vagy „Szigorúan titkos!” minősítési szintű adatot kezelő rendszeren legalább 2 hetente
kell offline frissíteni.

12.3. Vírus jelenlétére utaló jelenség észlelése esetén a felhasználónak fel kell függesztenie a munkát és értesítenie kell a rendszerbiztonsági felügyelőt.

13. Fiók- és jelszóházi rend

13.1. A felhasználó azonosítása egyedi felhasználónév és jelszó alkalmazásával, vagy biometrikus azonosító alkalmazása esetén kétfaktoros hitelesítéssel történik. A minősített adatot kezelő rendszerhez való hozzáférést biztosító jelszónak a kis- és nagybetű, szám és speciális karakter négyes kombinációból legalább hármat kell tartalmaznia.

13.2. A jelszó hossza:

- a) legfeljebb „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszer esetén legalább 12 karakter;
- b) „Bizalmas!” vagy annál magasabb minősítési szintű adatot kezelő rendszer esetén legalább 14 karakter.

13.3. 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.

13.4. A minősített adatot kezelő rendszeren a fiókjárolási küszöbérték beállítását úgy kell elvégezni, hogy a rendszer a harmadik sikertelen bejelentkezési kísérletet követően a felhasználót egy órára kizárja a rendszerből.

13.5. A minősített adatot kezelő rendszer rendszerszintű jelszavai közé a rendszeradminisztrátor felhasználói fiókjához tartozó jelszó és a BIOS jelszó tartozik, amelyeket a rendszeren kezelhető minősített adat legmagasabb minősítési szintjének megfelelően kell tárolni, a biztonsági vezető által meghatározott biztonsági tárolóban.

13.6. A rendszeradminisztrátor akadályoztatása esetén a rendszerszintű jelszavakat tartalmazó borítékok felbontására a biztonsági vezető jogosult. Ha a rendszerszintű jelszavakat tartalmazó borítékot illetéktelen személy bontotta fel, a jelszavakat haladéktalanul le kell cserélni.

13.7. A rendszerszintű jelszavakat tartalmazó borítékok felbontása esetén a rendszerszintű jelszavakat új, azonos iktatási számmal megjelölt, lepecsételt lezárt borítékokban kell elhelyezni és a 13.5. pont szerint tárolni.

13.8. A felhasználó hozzáférését engedélyező formanyomtatványt iktatásba kell venni és a felhasználói engedély selejtezéséig meg kell őrizni. A felhasználó részére beállításra kerülő jogosultságoknak összhangban kell állnia a felhasználói engedélyben rögzített rendelkezési jogosultságokkal. A felhasználó számára a felhasználói jogosultságok módosítása, illetve a saját tulajdonba vétel joga nem kerülhet beállításra.

14. Naplóműködés

14.1. A minősített adatot kezelő rendszeren naplófájlban kell rögzíteni a következő, rendszeren végzett 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 dátum és idő módosítása;
- h) a rendszer erőforrásokhoz történő hozzáférési kísérletek;
- i) az automatikus riasztási funkciók működésének leállítása;
- j) új felhasználó létrehozása;
- k) valamely felhasználó törlése vagy hozzáféréseinek letiltása.

14.2. A naplófájl a 14.1. pontban felsorolt események vonatkozásában tartalmazza:

- a) az esemény típusát,
- b) a felhasználó azonosítóját,
- c) az események dátumát és
- d) az események sikeres, vagy sikertelen kimenetelét.

14.3. A rendszerbiztonsági felügyelő az ÜBSZ-ben meghatározott időközönként ellenőrzi a naplófájlok bejegyzéseit.

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

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

15. Biztonsági mentés

- 15.1. A rendszeren tárolt minősített adatokról biztonsági mentés készíthető. A biztonsági mentés végrehajtásának módját, gyakoriságát és a rendszertől való elkülönített tárolását az ÜBSZ-ben kell meghatározni.
- 15.2. 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.

16. Hatályba léptető és záró rendelkezések

Jelen dokumentum a kiadása napján lép hatályba, egyidejűleg hatályát veszti a 30710-1/884/2020. iktató számú, 2.0 verziószámú Elektronikus Biztonsági Követelmények az állami szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez megnevezésű dokumentum.

Készült: 1 pld. elektronikusan NBF honlap

1. SZ. MELLÉKLET: MINŐSÍTETT ADATOT KEZELŐ RENDSZER MÓDOSÍTÁSÁVAL KAPCSOLATOS BEJELENTÉSI, ENGEDÉLYEZÉSI ÉS INTÉZKEDÉSI KÖTELEZETTSÉGEK.

	NBF engedélye	NBF tájékoztatása	Biztonsági vezető engedélye	Rögzítés a rendszer dokumentációban.
Változás:				
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
Helyiség berendezése TEMPEST eszközök alkalmazása esetén		X	X	X
Helyiségben más rendszerek		X	X	
Helyiségben bútorzat			X	
Helyiségben bútorzat TEMPEST eszközök alkalmazása esetén		X	X	
ÜBSZ átdolgozása		X		
RBK átdolgozása		X		
Felhasználók hozzáadása, törlése			X	
Munkaállomások, szerverek, nyomtatók száma	X			X
Rendszer kapcsolat (külső vagy más rendszer, létesítés, megszüntetés)	X			X
Fődarab (monitor, alaplap, számítógépház, szkennel, rendszert tartalmazó elsődleges adathordozó)		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
Operációs rendszer frissítése Microsoft Windows 7-ről Microsoft Windows 10-re		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
Operációs rendszer és szoftver frissítés, karbantartás				X