NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
NEMZETI BIZTONSÁGI FELÜGYELET

ELEKTRONIKUS BIZTONSÁGI KÖVETELMÉNYEK

az állami szervek és a gazdálkodó szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez

2025

Iktatószám: 30710-3/400-1/2025
Dátum: 2025. november 28.

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 –meghatározza és a minősített adatkezelést végző szervek részére elérhetővé tegye az elektronikus biztonságra vonatkozó irányelveket, követelményeket és az engedélyezés szakmai követelményrendszerét.

TARTALOMJEGYZÉK

I. FIZIKAI BIZTONSÁG

1. Fizikai biztonsági követelmények

1.1 A 90/2010. Korm. rendeletben és az Er.-ben foglaltakon túl a minősített adatot kezelő rendszer (a továbbiakban: rendszer) telepítési helyszínén tilos a rendszerre vonatkozó rendszerengedély-kérelemhez csatolt helyszínrajzon nem jelölt informatikai eszközöket tárolni vagy üzemeltetni.

II. ADMINISZTRATÍV BIZTONSÁG

2. Biztonsági dokumentáció

2.1 Az Er. szerinti üzemeltetés-biztonsági szabályzatot (a továbbiakban: ÜBSZ) és rendszerbiztonsági követelményeket (a továbbiakban: RBK) készítő minősített adatot kezelő szerv köteles gondoskodni ezen biztonsági dokumentáció naprakészen tartásáról. Amennyiben az Er. alapján ÜBSZ és RBK kiadása is szükséges, akkor azokat – az azonos tartalmi elemek szükségtelen duplikálásának elkerülése érdekében – a minősített adatot kezelő szerv vezetőjének döntése alapján egységes szerkezetbe lehet foglalni.

2.2 Az ÜBSZ kötelező tartalmi elemei:

a) a rendszer jellegének meghatározása (a rendszer által kezelhető minősített adat legmagasabb minősítési szintje, a rendszer rendeltetése, a rendszer felhasználói köre);

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 (telepítési alaprajz és annak szöveges leírása, amely a rendszer telepítési helyét magába foglaló helyiség részletes rajzát tartalmazza),
- 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,
- 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;

e) a kép és hang rögzítésére vonatkozó előírások rögzítése;

f) a hardverkonfiguráció és szoftverkonfiguráció részletes szabályainak meghatározása:
- üzembe helyezés,
- karbantartás,
- telepítésre és frissítésre vonatkozó előírások,
- biztonsági és naplózási beállítások;

g) a vírusvédelemre vonatkozó előírások meghatározása;

h) a jelszóházirend rögzítése;

i) a biztonsági incidensek kezelésére vonatkozó rendelkezések meghatározása;

j) a vészhelyzetben alkalmazandó előírások meghatározása és a helyreállítás folyamatára vonatkozó rendelkezések rögzítése;

k) a kockázatelemzés;

l) a konfigurációmenedzsment;

m) a rendszerbiztonsági nyilvántartások felsorolása;

n) az ellenőrzési metodika rögzítése;

o) a rendszerelemek és az alkalmazott szoftverek felsorolása;

p) a rendszer felhasználói részére az Er-ben előírt elektronikus biztonsági képzés tematikájának és rendjének meghatározása.

2.3 Az ÜBSZ tudomásul vételéről és az abban foglaltak betartásáról szóló felhasználói nyilatkozatokat a rendszer megszüntetését követő 8 évig kell megőrizni.

2.4 Az RBK 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) a rendszer biztonságáért felelős személyek meghatározása nevük és elérhetőségük megjelölésével;

d) a hozzáférésre vonatkozó előírások meghatározása (felhasználó-azonosítás, hozzáférés felügyelete);

e) az adatfájl cserére vonatkozó előírások rögzítése;

f) a kockázatelemzés;

g) a konfigurációmenedzsment leírása;

h) TEMPEST eszközök alkalmazása esetén az elektromágneses kompromittáló

kisugárzás elleni védelemre vonatkozó előírások meghatározása;

i) rejtjelző eszköz használata esetén hálózatbiztonsági szabályok meghatározása.

2.5 Az RBK-t a rendszer megszüntetését követő 8 évig kell megőrizni.

3. Rendszerbiztonsági nyilvántartások

3.1 A rendszer üzemeltetésével kapcsolatos tevékenységet az alábbi rendszerbiztonsági nyilvántartásokban – a biztonságos üzemeltetéshez kapcsolódó adatok ellenőrzése és visszakeresése céljából – kell dokumentálni:

a) az adathordozók nyilvántartása, amelyben az adathordozók egyedi azonosító számát, az eszköz típusát, a márka és modell megnevezését, a kapacitását és ha van, a sorozatszámát, illetve virtuális adathordozó esetén az eszköz típusát kell nyilvántartani;

b) a rendszerfrissítések és ellenőrzések nyilvántartása, amelyben a végrehajtott rendszerfrissítéseket, szoftveres módosításokat, az IT infrastruktúra felújítását, karbantartását, a merevlemezek kiadását és az ellenőrzéseket kell dokumentálni;

c) a biztonsági események nyilvántartása, amelyben a rendszer biztonságát érintő eseményeket szükséges rögzíteni.

3.2 A rendszerbiztonsági nyilvántartásokat a lezárásukat követő 8 évig kell megőrizni.

4. Adathordozók kezelése

4.1 A minősített adatokat kezelő elektronikus rendszeren egy adathordozón több forrásból (nemzeti, NATO, EU) származó adat is kezelhető, a minősített adatok logikai úton történő elkülönítését azonban biztosítani kell.

4.2 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 metódussal kell törölni. Az előzőekben foglaltakkal szemben az SSD és SSHD meghajtókat ATA Secure Erase eljárással kell törölni. A biztonságos eljárással törölt adathordozó újra felhasználható. A „Titkos!” és „Szigorúan titkos!” minősítési szintű adatot tartalmazó adathordozót szoftveres eljárással nem lehet törölni, életciklusa végén kizárólag fizikai megsemmisítés engedélyezett.

5. Ellenőrzések rendje

5.1 A rendszer 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
1. munkaállomás, csatlakozások állapota, sértetlensége	felhasználó	minden használat előtt
	rendszerbiztonsági felügyelő	12 havonta
2. a rendszer részét képező adathordozók	rendszeradminisztrátor, rendszerbiztonsági felügyelő	12 havonta
3. letiltott portok feloldásával és a külső adathordozó csatlakoztatásával járó adatfájl csere	rendszeradminisztrátor	végrehajtás előtt
4. naplófájlok, biztonsági mentések	rendszerbiztonsági felügyelő	4 hetente
5. engedélyezett telepített szoftverek	rendszeradminisztrátor	12 havonta
6. BIOS beállítások	rendszeradminisztrátor	3 havonta
7. rendszerfrissítések és ellenőrzések nyilvántartása	biztonsági vezető	6 havonta
8. TEMPEST matricák sértetlensége	rendszerbiztonsági felügyelő és a felhasználók	3 havonta a rendszerbiztonsági felügyelő, továbbá a felhasználók minden használat előtt

III. HARDVERBIZTONSÁG

6. Kompromittáló kisugárzás elleni védelem

6.1 A TEMPEST követelményeket az NBF által kiadott TEMPEST Biztonsági Követelmények megnevezésű dokumentum tartalmazza.

6.2 A TEMPEST követelmények teljesítésére vonatkozó kötelezettségtől függetlenül, csak olyan, CE jelöléssel ellátott hardvereszközök használhatóak, amelyek megfelelnek az elektromágneses összeférhetőségre vonatkozó szabályozás előírásainak.

7. Engedélyköteles rendszerelem

7.1. Engedélyköteles rendszerelem minden olyan fizikai komponens, amely az elektronikus adatkezelő rendszer részeként annak működésében és/vagy az elektronikusan kezelt minősített adat bizalmasságának, sérthetetlenségének és rendelkezésre állásának megőrzésében nélkülözhetetlen.

IV. SZOFTVERBIZTONSÁG

8. BIOS beállítások

8.1 A rendszerben kizárólag a rendszeradminisztrátor rendelkezhet rendszergazdai jogosultságokkal.

8.2 A 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 rendszert csak engedélyezett, jogtiszta licensszel, és gyártói támogatással rendelkező, naprakész Microsoft Windows vagy Linux operációs rendszerrel lehet üzemeltetni.

9.2 A 9.1. pontban meghatározottaktól egyéni elbírálás alapján – az alkalmazni tervezett rendszer, valamint szoftverek figyelembevételével – az NBF engedhet eltérést.

9.3 A rendszeren alkalmazott operációs rendszert az Er. 34/A. §-ban meghatározott időközönként kell frissíteni.

9.4 Online módon frissíteni részletes kockázatelemzés alapján, a 2. számú mellékletben foglaltak betartásával lehet.

9.5 A 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 üzenetet;

d) a jelszavas képernyővédelem biztosítása;

e) a lomtár tiltása;

f) a vendég fiók tiltása;

g) az események 15. pont szerinti naplózása;

h) a fiók- és jelszóházirend beállítása.

10. Adatfájl csere

10.1 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.

10.2 Az Er. 2.§ (5) bekezdésben meghatározott esetben, minősített adat továbbítására szolgáló rejtjelzéssel védett virtuális magánhálózatot (VPN) kialakítani, kizárólag az NBF által engedélyezett szoftverekkel lehetséges.

11. Felhasználói szoftverek

11.1 A rendszerre kizárólag a munkavégzéshez feltétlenül szükséges, jogtiszta licensszel és gyártói támogatással rendelkező, naprakész – a 9.1. pontnak megfelelő operációs rendszer által támogatott – szoftverek telepítése megengedett.

11.2 A 11.1. pontban foglaltaktól eltérni egyéni kockázatelemzés alapján, az NBF jóváhagyásával lehet.

12. Vírusvédelem

12.1 Az Er.-ben előírt vírusvédelemhez jogtiszta licensszel, illetve gyártói támogatással rendelkező szoftvert kell alkalmazni. Erre a célra a Microsoft operációs rendszerek részét képező Windows Defender is alkalmazható.

12.2 Online módon frissíteni részletes kockázatelemzés alapján, a 2. számú mellékletben foglaltak betartásával lehet.

12.3 Az egyes vírusvédelmi szoftvereket az NBF az adott szoftver sérülékenységét érintő riasztások figyelembevételével hagyja jóvá, vagy tagadja meg a jóváhagyását.

12.4 A vírusvédelmi szoftver vírusdefiníciós adatbázisát:

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

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

c) „Titkos!”, vagy „Szigorúan titkos!” minősítési szintű adatot kezelő rendszeren legalább 2 hetente

kell frissíteni.

12.5 Vírus jelenlétére utaló jelenség észlelése esetén a felhasználó köteles felfüggeszteni a munkát és haladéktalanul értesíteni a rendszerbiztonsági felügyelőt.

13. Fiók- és jelszóházirend

13.1 A felhasználó azonosítása egyedi felhasználónév és jelszó alkalmazásával, vagy biometrikus azonosító alkalmazása esetén kétfaktoros vagy multifaktoros hitelesítéssel történik.

13.2 A rendszerhez való hozzáférést biztosító jelszónak a kis- és nagybetű, szám és speciális karakter négyes kombinációból legalább hármat kell tartalmaznia.

A jelszó hossza:

a) „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 rendszeren a fiókzárolási küszöbérték beállítását úgy kell elvégezni, hogy a rendszer három sikertelen bejelentkezési kísérletet követően egy órára kitiltja a felhasználót. A kitiltás feloldására egy órán belül kizárólag a rendszeradminisztrátor jogosult.

13.5 A felhasználó hozzáférését engedélyező formanyomtatványt iktatásba kell venni és a felhasználói fiók törlését követő 8 évig meg kell őrizni. A felhasználó számára a felhasználói jogosultságok módosítása, illetve a saját tulajdonba vétel joga nem kerülhet beállításra.

14. Rendszerszintű jelszavak

14.1 A 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, iktatószámmal ellátott, lepecsételt, lezárt borítékokban elhelyezve, egymástól elkülönítve kell tárolni, a biztonsági vezető által meghatározott biztonsági tárolóban.

14.2 A rendszeradminisztrátor akadályoztatása esetén a rendszerszintű jelszavakat tartalmazó borítékok felbontására a biztonsági vezető és a rendszerbiztonsági felügyelő jogosult. Ha a rendszerszintű jelszavakat tartalmazó borítékokat illetéktelen személy bontotta fel, a jelszavakat haladéktalanul le kell cserélni.

14.3 A rendszerszintű jelszavakat tartalmazó borítékok felbontása esetén a rendszerszintű jelszavakat új, azonos iktatószámmal megjelölt, lepecsételt lezárt borítékokban kell elhelyezni és a 14.1. pont szerint tárolni.

15. Naplóházirend

15.1 A 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 hozzáférésének letiltása.

15.2 A naplófájl a 15.1. pontban felsorolt események vonatkozásában tartalmazza:

a) az esemény típusát,

b) az eszköz azonosítóját,

c) a felhasználó azonosítóját,

d) az események dátumát,

e) az érintett szolgáltatást, parancsot, alkalmazást

f) az események sikeres, vagy sikertelen kimenetelét.

15.3 A rendszerbiztonsági felügyelő az 5. pontban meghatározott időközönként ellenőrzi a naplófájlok bejegyzéseit.

15.4 A rendszeren biztosítani kell az utolsó 6 hónapban készült naplófájlok elérhetőségét.

15.5 A rendszeradminisztrátor a 6 hónapnál régebbi naplófájlokról biztonsági mentést készít, amelyet nyilvántartásba vett adathordozón kell tárolni, a biztonsági vezető által meghatározott biztonsági tárolóban.

16. **Biztonsági mentés**

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

V. HATÁLYBA LÉPTETŐ ÉS ZÁRÓ RENDELKEZÉSEK

Jelen dokumentum a kiadása napján lép hatályba, egyidejűleg hatályát veszti a 30710-3/475-6/2023 iktatószámú, 4.2. verziószámú „Elektronikus Biztonsági Követelmények gazdálkodó szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez” megnevezésű dokumentum, valamint a 30710-3/475-7/2023 iktatószámú, 4.2. verziószámú „Elektronikus Biztonsági Követelmények az állami szervezetek minősített adatot kezelő rendszereinek engedélyezéséhez és üzemeltetéséhez” megnevezésű dokumentum.

1. sz. melléklet: A minősített adatot kezelő rendszer módosításával kapcsolatos bejelentési, engedélyezési és intézkedési kötelezettségek

A minősített adatot kezelő rendszeren végrehajtani tervezett változások engedélyezéséhez az NBF honlapján elérhető „Rendszerengedély-kérelem" megnevezésű nyomtatvány kitöltése szükséges, amelyet a „Kérdőív a rendszerengedély kérelemhez" megnevezésű dokumentummal együtt kell benyújtani az NBF-hez.

Változás:	NBF rendszer-engedélye	NBF tájékoztatása	Biztonsági vezető	Rögzítés a rendszer dokumentációban
Minősítési szint és adatforrás	X			
Adatkezelési engedély (rendszerengedélyt érintő)	X			
Rendszerbiztonsági felügyelő személye			X	X
Rendszeradminisztrátor személye			X	X
Telepítési helyszín	X			X
Rendszer rendezvényre történő szállítása és üzemeltetése		X	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	
Rendszerengedélyben szereplő fődarabok számának változása esetén	X			X
Rendszerengedélyben szereplő fődarabok cseréje esetén		X	X	X
Rendszer kapcsolat (bármely más rendszer, létesítés, megszüntetés)	X			X
Részegység (monitor, videokártya, optikai meghajtó, egér, billentyűzet stb.)			X	X
Rejtjelző eszköz típusának változása esetén	X			
Alapvető szoftver (Operációs rendszer, biztonsági szoftver, Vírusvédelem, virtuális szerver)	X		X	X
Microsoft Windows 11, Microsoft IoT telepítése		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

2. sz. melléklet: Az operációs rendszer, valamint a vírusvédelmi szoftver online frissítésére vonatkozó szabályok

Az operációs rendszer, valamint a vírusvédelmi szoftver online frissítése az alábbiak szerint lehetséges:

1. Köztes update infrastruktúrán keresztül történő frissítés:

a) A frissítések kizárólag a gyártó/forgalmazó hivatalos szerveréről tölthetők le.

b) Kötelező a digitális aláírás ellenőrzése minden frissítésnél (pl. Microsoft Code Signing, PGP/GPG, gyártói tanúsítvány).

c) A kommunikációhoz TLS 1.3 vagy magasabb verzió alkalmazása, lehetőség szerint kétoldalú tanúsítványhitelesítéssel.

d) Kijelölt frissítőszerver kerül kialakításra egy védett köztes hálózati zónában (DMZ), amely a gyártói szerverektől letölti a frissítéseket.

e) A minősített rendszerek csak a belső frissítőszerverhez kapcsolódnak, amely validált és jóváhagyott csomagokat biztosít.

f) Az adatáramlás egyirányú átjárón (adatdióda vagy hasonló technológia) történik, amely kizárja a külső behatolást.

2. Kötelező naplózás, ellenőrzés, hash-validáció és rollback lehetőség:

a) A frissítések telepítése előtt tesztkörnyezetben validálni kell azok működését és kompatibilitását.

b) Automatikus és manuális ellenőrzési lépések: hash-ellenőrzés, sandbox futtatás, kompatibilitási tesztek.

c) Csak az ellenőrzött és jóváhagyott csomagok kerülhetnek át a minősített környezetbe.

d) Frissítési forgalom szigorúan szabályozott időablakban történhet.

e) Tűzfalak, IDS/IPS rendszerek és alkalmazásszintű proxyk monitorozzák a teljes frissítési kommunikációt.

f) Kizárólag a frissítéshez szükséges portok és protokollok engedélyezhetők.

g) Minden frissítési művelet részletes naplózásra kerül: időpont, forrás, cél, csomagazonosító, érvényességi vizsgálat eredménye.

h) A naplókat manipuláció ellen védett módon kell tárolni.

i) Rendszeres független audit szükséges a folyamat megfelelőségének ellenőrzésére.

j) Biztosítani kell a lehetőséget az online frissítés azonnali leállítására kompromittálódás gyanúja esetén.

k) Hibás frissítés esetén előre definiált visszaállítási (rollback) mechanizmust kell alkalmazni.

l) Offline frissítés továbbra is kötelezően rendelkezésre álljon, mint biztonsági tartalék eljárásrend.