161/2010. (V. 6.) Korm. rendelet

a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

A Kormány a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § *c)* pontjában,

a 11–12. §, a 15. §, a 18–21. § és a 29. § tekintetében a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § *b)* pontjában,

a 3. § (3) bekezdése, a 4. §, az 5. § (3) bekezdése, a 7. § (2) bekezdése, a 8. § (2) bekezdése, a 9. §, a 13. §, a 16. §, a 22. §, a 24–25. §, a 30–31. §, a 43–46. §, az 53–54. §, az 57–58. § és a 64. § tekintetében a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § *d)* pontjában

kapott felhatalmazás alapján,

az Alkotmány 35. § (1) bekezdés *b)* pontjában meghatározott feladatkörében eljárva

a következőket rendeli el:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. Értelmező rendelkezések

1. § E rendelet alkalmazásában:

1. *adathordozó:* az elektronikus adatkezelő rendszerhez (a továbbiakban: rendszer) csatlakoztatható, vagy abba beépített olyan eszköz, melynek segítségével az elektronikus minősített adatok tárolása megvalósítható,

2. *biztonsági dokumentáció:* a rendszerbiztonsági követelmények és az üzemeltetés-biztonsági szabályzat, továbbá – ha a minősített adatot elektronikus rendszeren kezelő szerv rejtjeltevékenységet folytat – a működtetési szabályzat és a kezelési utasítás,

3. *életciklus:* magában foglalja a rendszer létrehozására vonatkozó döntéstől a tervezést, a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást, a rendszer egyes elemeinek vagy egészének a kivonását és megsemmisítését,

4. *kezelési utasítás:* a rejtjelző eszköz működtetését leíró dokumentum,

5. *kezelői engedély:* a rejtjelző eszköz biztonságos üzemeltetéséhez szükséges elméleti és gyakorlati ismereteket nyújtó tanfolyam elvégzését és az azt követő sikeres vizsgát igazoló vizsgabizonyítvány alapján a rejtjelfelügyelő által kiállított felhatalmazás, amely rögzíti, hogy az engedély birtokosa milyen rejtjelző eszközöket üzemeltethet,

6. *kompromittáló kisugárzás:* olyan elektromos vagy elektromágneses jel, amelynek vétele és feldolgozása lehetővé teszi az arra illetéktelen személy vagy szerv számára az elektronikusan kezelt minősített adat kinyerését és megismerését,

7. *elektronikus biztonság:* a rendszerekben alkalmazott biztonsági intézkedések – a személyi-, a fizikai-, az adminisztratív-, valamint a rendszer-, a kommunikáció- és a rejtjelbiztonság – összessége, amelyek biztosítják az elektronikusan kezelt minősített adat bizalmasságát, sérthetetlenségét és rendelkezésre állását,

8. *működtetési szabályzat:* a rejtjelző eszközre vonatkozó eszköz-specifikus működtetési követelményeket és eljárásrendeket rögzítő dokumentum,

9. *rejtjelanyag:*
a) a rejtjelzés céljára szolgáló gépek, berendezések, számítástechnikai és egyéb eszközök,
b) rejtjelkulcsok,
c) rejtjelző eszközök speciális tartozékai és alkatrészei,
d) más rendeltetésű eszközök rejtjelzést megvalósító részegységei,
e) más rendeltetésű számítástechnikai eszközök, amennyiben rejtjelző programot működtetnek vagy a rejtjelzés folyamatát szolgáló adatokhoz hozzáférhetnek vagy ilyen adatot tartalmaznak,
f) a rejtjelző eszközökről, módszerekről, eljárásokról készített dokumentációk,
g) a rejtjelző eszközök biztonsági szabályzata, valamint
h) a rejtjelző eszközök biztonságával összefüggő egyéb dokumentumok,
10. *rejtjelfelügyelő:* a biztonsági vezető felügyelete mellett a rejtjeltevékenység alkalmazási területén a rejtjeltevékenység személyi, fizikai, adminisztratív, valamint a rejtjelbiztonsági követelményeinek érvényesüléséért felelős személy,
11.[1] *rejtjel-hozzáférési engedély:* az állami vagy közfeladat végrehajtása érdekében a biztonsági vezető által a megfelelő szintű személyi biztonsági tanúsítvány alapján adott írásbeli felhatalmazás, amely rögzíti, hogy az engedély birtokosa milyen rejtjelanyaghoz férhet hozzá,
12. *rejtjelszabályzat:* a minősített adatot kezelő szerv vezetője által kiadott belső rendelkezés, amely a rejtjeltevékenység általános szabályozására szolgál, valamint meghatározza a rejtjelanyag szállítására és tárolására vonatkozó követelményeket,
13. *rejtjeltevékenység:* a rejtjelzés, valamint az azzal összefüggő rejtjelző eszköz fejlesztése, gyártása, javítása, értékesítése, az ezekkel kapcsolatos kiképzés, a rejtjelkulcs gyártása, megsemmisítése, az ezekkel kapcsolatos ügyvitel, továbbá a felsoroltak biztonságához közvetlenül kötődő feladatok ellátása,
14. *rejtjelzés:* minden olyan tevékenység, eljárás, amelynek során valamely minősített adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon és ennek következtében a minősített adat minősítés nélküliként kezelhető legyen, valamint a rejtjelzett adat eredeti állapotba történő visszaállítása,
15. *rejtjelző:* a rejtjelfelügyelő irányítása mellett a rejtjeltevékenység végrehajtásáért felelős személy,
16. *rendszeradminisztrátor:* a rendszerbiztonsági felügyelő irányítása mellett a rendszer üzemeltetéséért, karbantartásáért felelős személy,
17. *rendszerbiztonsági felügyelő:* a rendszer alkalmazási területén a rendszer személyi, fizikai, adminisztratív, valamint rendszerbiztonsági feltételeinek érvényesüléséért felelős személy,
18. *rendszerbiztonsági követelmények:* a rendszer részletes leírását, valamint a rendszerre vonatkozó biztonsági követelményeket tartalmazó dokumentum,
19. *rendszerengedély:* a minősített adatot kezelő szerv által üzemeltetett rendszer üzemeltetésére, módosítására, valamint rendszerek összekapcsolására a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) által lefolytatott engedélyezési eljárást követően kiadott határozat, amely meghatározza a rendszer által kezelhető minősített adat legmagasabb minősítési szintjét, valamint a kérelmező szervezet számára meghatározott rendszerben és telepítési helyen engedélyezi a kérelemben azonosított rejtjelző eszköz működtetését,
20. *rendszeresítési engedély:* az NBF által lefolytatott engedélyezési eljárást követően kiadott határozat, amely rögzíti a kérelemben azonosított típusú és verziójú rejtjelző eszköz rendeltetését és meghatározza az azon rejtjelezhető minősített adat legmagasabb minősítési szintjét,

1 Megállapította: 436/2025. (XII. 23.) Korm. rendelet 19. §. Hatályos: 2026. I. 6-tól.

21.[1] *TEMPEST követelmények:* a „Bizalmas!” vagy magasabb minősítési szintű külföldi minősített adat, valamint az adminisztratív zóna határától legfeljebb 8 méterre elhelyezkedő rendszer által kezelt „Titkos!” és „Szigorúan titkos!” minősítési szintű nemzeti minősített adat bizalmasságának védelme érdekében alkalmazandó, a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentését célzó – e rendeletben és a 4. § (4) bekezdés *b)* pontja alapján kiadott TEMPEST biztonsági követelményekben meghatározott – biztonsági intézkedések,

22. *üzemeltetés-biztonsági szabályzat:* a rendszer egy meghatározott üzemeltetési helyén a biztonsági követelmények teljesítése érdekében követendő feladatok, eljárások, valamint az üzemeltetéshez szükséges munkakörök teljes körű leírása,

23.[2] *külföldi rejtjelző eszköz:* a NATO, az EU vagy ezek valamely tagállama által engedélyezett rejtjelző eszköz.

2. § (1) Minősített adat kizárólag olyan rendszeren kezelhető, amely rendelkezik az NBF által kiadott, legalább a kezelni kívánt minősített adat minősítési szintjével megegyező szintű rendszerengedéllyel.

(2) A „Bizalmas!”, valamint magasabb minősítési szintű adatot elektronikus rendszeren kezelő szerv rendelkezik a rendszeren kezelhető minősített adat legmagasabb minősítési szintjével legalább azonos szintű minősített adat kezelésére a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendeletben meghatározott engedéllyel, ennek hiányában a rendszerengedély nem adható ki.

(3) A nemzetbiztonsági és bűnügyi műveletekben külföldön folytatott rejtjeltevékenység különleges biztonsági követelményeit – a nemzetbiztonsági kockázatok alapján, a hatáskörrel rendelkező nemzetbiztonsági szolgálat egyetértésével – az NBF állapítja meg.

(4) A felhasználó rendszer használata nem minősül rejtjeltevékenységnek, ha a minősített adatok kezelése vagy továbbítása olyan informatikai rendszeren történik, amelyben a rejtjelző eszköz, rejtjelző szoftver vagy rejtjelző eljárás is telepítésre került és a rendszer biztonsági beállítása nem teszi a felhasználó számára lehetővé a rejtjelzés biztonsági beállításainak módosítását vagy a minősített adatok rendszerben történő kezelése vagy továbbítása során a rendszerben alkalmazott rejtjelzés kiiktatását.

(5) Nemzeti „Korlátozott terjesztésű!” minősítési szintű adatot – ha az elektronikus rendszer magasabb minősítési szintű adat kezelésére vonatkozó rendszerengedéllyel nem rendelkezik és a megvalósítási lehetőségek adottak – rejtjelzéssel védett virtuális magánhálózat útján kell továbbítani.

(6)[3] A közös biztonsági terület létrehozására jogosult szervek nemzeti minősített adatot kezelő, önálló, hálózat részét nem képező közös rendszert üzemeltethetnek. A közös rendszerben a minősített adatot kezelő szervek nem alkalmazhatnak közös adathordozót. Az adathordozón – a 25. § (3) bekezdésében foglaltakon túl – fel kell tüntetni a minősített adatot kezelő szerv nevét. Az adathordozót alkalmazását követően el kell távolítani a rendszerből. A minősített adatot kezelő szervek gondoskodnak az adathordozók elkülönített biztonsági tárolóban történő tárolásáról.

(7)[4] A közös biztonsági területen üzemeltetett rendszerrel kapcsolatos fenntartói, felügyeleti és rendszerbiztonsági követelményeket a központi államigazgatási szervek vezetői a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet szerinti együttes utasításban szabályozzák.

---

1 Megállapította: 137/2025. (VI. 16.) Korm. rendelet 1. §. Hatályos: 2025. VI. 17-től.
2 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 19. §. Hatályos: 2024. X. 25-től.
3 Beiktatta: 436/2025. (XII. 23.) Korm. rendelet 20. §. Hatályos: 2026. I. 6-tól.
4 Beiktatta: 436/2025. (XII. 23.) Korm. rendelet 20. §. Hatályos: 2026. I. 6-tól.

(8)[1] A (7) bekezdésben meghatározott együttes utasítás a közös rendszerbiztonsági felügyelő és a közös rendszeradminisztrátor feletti munkáltatói jogkör gyakorlására vonatkozó megállapodást is tartalmazza.

(9)[2] A közös biztonsági területen működtetett rendszer biztonsági dokumentációjában az e rendeletben meghatározottakon túl rendelkezni kell a felelősség megosztásáról.

II. FEJEZET

AZ ELEKTRONIKUS BIZTONSÁG SZERVEZETE

2. Az elektronikus biztonság központi szervezete

3. § Az NBF ellátja a biztonsági engedélyezési hatósági, a rejtjelbiztonsági hatósági, valamint a TEMPEST hatósági funkciókat.

4. § (1) Az NBF általános feladatkörében:

a) felügyeli a minősített adatot elektronikus rendszeren kezelő szervek elektronikus biztonsággal kapcsolatos tevékenységét,

b) az elektronikus biztonság veszélyeztetése esetén a rendszer működtetését korlátozhatja, megtilthatja, a rendszert üzemeltető szerv vezetőjét az elektronikus biztonság helyreállítása érdekében szükséges intézkedések megtételére kötelezheti, a kiadott engedélyeket visszavonhatja,

c) egyetértési jogot gyakorol a nemzeti rendszerek összekapcsolási megállapodásaira vonatkozóan, valamint a nemzeti rendszer és a külföldi rendszer összekapcsolása esetén aláírja az egyetértési megállapodást,

d) hatósági ellenőrzést hajt végre,

e)[3] ellátja az elektronikus biztonság tekintetében a nemzeti biztonsági hatóság feladatkörét Magyarország nemzetközi kötelezettségvállalásai terén,

f) szükség esetén kivizsgálja az elektronikus biztonsági eseményeket, intézkedéseket ír elő a biztonság helyreállítása érdekében és a biztonsági esemény megismétlődésének elkerülésére,

g) külföldi minősített elektronikus adat veszélyeztetése esetén a vonatkozó megállapodások és nemzetközi kötelezettségvállalások alapján tájékoztatja a külföldi szerveket,

h) meghatározza és a minősített adatkezelést végző szervek részére elérhetővé teszi az elektronikus biztonságra vonatkozó irányelveket, követelményeket és az engedélyezés szakmai követelményrendszerét,

i)[4]

(2) Az NBF a biztonsági engedélyezés feladatainak keretén belül:

a) lefolytatja a biztonsági engedélyezési eljárást,

b) kiadja a rendszerengedélyt a működési környezetben meghatározott minősítési szintig,

c) egyetértési jogot gyakorol a rendszer elektronikus biztonságát érintő módosításokra vonatkozóan,

d) útmutatást ad és konzultációt folytat a biztonsági kockázatelemzéssel, kockázatkezeléssel és az elfogadható kockázattal kapcsolatos kérdésekben.

(3) Az NBF a rejtjelbiztonsági hatósági feladatainak keretén belül:

a) ellátja a rejtjeltevékenység hatósági engedélyezését és felügyeletét,

b) ellenőrzi a szervek rejtjeltevékenységét,

---

1 Beiktatta: 436/2025. (XII. 23.) Korm. rendelet 20. §. Hatályos: 2026. I. 6-tól.
2 Beiktatta: 436/2025. (XII. 23.) Korm. rendelet 20. §. Hatályos: 2026. I. 6-tól.
3 Módosította: 221/2014. (IX. 4.) Korm. rendelet 471. § a).
4 Hatályon kívül helyezte: 323/2018. (XII. 28.) Korm. rendelet 22. § a). Hatálytalan: 2019. I. 1-től.

c) egyetértési jogot gyakorol a rejtjeltevékenységre vonatkozó biztonsági dokumentáció esetében,

d) rejtjelszakmai és rejtjelbiztonsági kérdésekben állást foglal,

e) engedélyezi a rejtjelző eszközök készítését, fejlesztését, gyártását, alkalmazásának, működtetésének, kezelésének, javításának és őrzésének általános biztonsági feltételeit, egyetértési jogot gyakorol az erre vonatkozó követelményekkel és szabályzatokkal kapcsolatban,

f) a rejtjelbiztonság veszélyeztetése esetén a rejtjelző eszköz használatát korlátozhatja, megtilthatja, a rejtjeltevékenységet folytató szerv vezetőjét a rejtjelbiztonság helyreállítása érdekében szükséges intézkedés megtételére kötelezheti, a kiadott engedélyeket visszavonhatja,

g) összehangolja a rejtjeltevékenységben együttműködő szervek munkáját, szükség szerint koordinál a rejtjelző eszközök fejlesztésével, gyártásával és az eszközellátással kapcsolatban.

(4) Az NBF a nemzeti TEMPEST hatóság feladatainak keretén belül:

a) a kompromittáló kisugárzás elleni védelem tekintetében felügyeletet és ellenőrzést gyakorol,

b) meghatározza és a minősített adatkezelést végző szervek részére elérhetővé teszi a TEMPEST biztonsági követelményeket,

c) ellenőrzi a rendszer és működési környezete TEMPEST megfelelőségét,

d)[1] TEMPEST vizsgálatokat, méréseket végez,

e)[2] a TEMPEST mérések alapján zónába sorolja a rendszer környezetét,

f) a TEMPEST biztonság veszélyeztetése esetén a rendszer használatát korlátozhatja, megtilthatja, a szerv vezetőjét a kompromittáló kisugárzás elleni védelem helyreállítása érdekében szükséges intézkedések megtételére kötelezheti, a kiadott rendszerengedélyt visszavonhatja.

5. § (1)[3] Magyarország nemzetközi kötelezettségvállalásainak teljesítése érdekében

a)[4] a honvédelemért felelős miniszter látja el a NATO Központi Rejtjel Elosztó Felügyelet feladatait,

b)[5] a külpolitikáért felelős miniszter látja el az EU Központi Rejtjel Elosztó Felügyelet feladatait.

(2) Az (1) bekezdésben meghatározott szervek, az ott megjelölt feladatkörükben felelősek

a) a rejtjelző eszközök és rejtjelanyagok átvételéért, nyilvántartásáért, kezeléséért,

b) a nyilvántartó szervek létrehozásához és megszüntetéséhez szükséges követelmények meghatározásáért,

c) a rejtjelző eszközök és rejtjelanyagok elosztásáért és a továbbosztás felügyeletéért,

d) a rejtjelző eszközök felhasználását végző szervezetek ellenőrzéséért,

e) a központi nyilvántartási és ellenőrzési feladatok végrehajtásáért,

f) a NATO, EU külföldi elosztó és felügyeleti szervekkel való kapcsolattartásért,

g) az igény elbírálása után a rejtjelanyagok biztosításáért.

3. A minősített adatot elektronikus rendszeren kezelő szerv vezetőjének feladatai

6. § (1) A minősített adatot elektronikus rendszeren kezelő szerv vezetője:

a) felelős a minősített adat védelmi feltételeinek kialakításáért,

b) kijelöli a szervnél üzemeltetett rendszer elektronikus biztonságáért felelős személyeket,

c) kiadja a rendszer biztonsági dokumentációit.

---

1 Módosította: 375/2020. (VII. 30.) Korm. rendelet 35. § a).
2 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 9. § (1). Hatályos: 2019. I. 1-től.
3 Módosította: 221/2014. (IX. 4.) Korm. rendelet 471. § b).
4 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 10. §. Hatályos: 2019. I. 1-től.
5 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 10. §. Hatályos: 2019. I. 1-től.

(2) Amennyiben a szerv rejtjeltevékenységet is folytat, a minősített adatot elektronikus rendszeren kezelő szerv vezetője:

a) megállapítja a szerv rejtjeltevékenységének szabályait, tartalmát, szervezeti rendjét, terjedelmét, rejtjeles kapcsolatait és kiadja a rejtjelszabályzatot,

b) biztosítja a rejtjeltevékenység szervezeti, személyi, tárgyi és biztonsági feltételeit,

c) kijelöli a rejtjeltevékenység biztonságáért felelős személyeket,

d) [1]

(3) Amennyiben a rejtjel-felügyeleti feladatok ellátása központilag biztosított, a minősített adatot elektronikus rendszeren kezelő szerv vezetője csak a (2) bekezdés *b)–d)* pontjában foglalt feladatoknak tesz eleget.

4. Az elektronikus biztonság helyi szervezete

7. § (1) A minősített adatot elektronikus rendszeren kezelő szerv vezetője kijelöli azokat a személyeket, akik felelősek a szervnél üzemeltetett rendszer elektronikus biztonságáért, így:

a) a rendszerbiztonsági felügyelőt vagy a rendszerbiztonsági felügyelet vezetőjét és munkatársait,

b) a rendszeradminisztrátort, valamint

helyettesítőiket.

(2) Amennyiben a szerv rejtjeltevékenységet is folytat, kijelöli azokat a személyeket, akik felelősek a rejtjeltevékenység biztonságáért, így:

a) a rejtjelfelügyelőt vagy a rejtjelfelügyelet vezetőjét és munkatársait,

b) a rejtjelzőt, valamint

helyettesítőiket.

(3) [2] A Kormány tagjainak feladat- és hatásköréről szóló kormányrendelet szerinti, a miniszterelnök

a) kormányzati igazgatási és

b) politikai

munkaszervezete esetében a rendszerbiztonsági felügyelő, valamint a rendszeradminisztrátor a jogszabályokban meghatározott feladatait mindkét minősített adatot kezelő szerv vonatkozásában elláthatja.

5. A biztonsági vezető

8. § A minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője

a) kezdeményezi az elektronikus biztonsághoz és a rejtjeltevékenységhez előírt engedélyek beszerzését és gondoskodik azok nyilvántartásáról,

b) irányítja a rendszerbiztonsági felügyelő vagy a rendszerbiztonsági felügyelet és a rendszeradminisztrátor tevékenységét, valamint ellenőrzi az elektronikus biztonsági előírások betartását,

c) gondoskodik a rendszerbiztonsági dokumentumok elkészítéséről,

d) minden év február 28-áig tájékoztatja az NBF-et a szervezet rejtjeltevékenységéről, az NBF által megadott szempontok alapján,

e) irányítja a rejtjelfelügyelő vagy a rejtjelfelügyelet tevékenységét,

f) gondoskodik arról, hogy a rejtjeltevékenységgel kapcsolatos, védelem alá eső információkat csak azok a személyek ismerhessék meg, akiknek a munkájához az feltétlenül szükséges, és arra a megfelelő engedélyekkel rendelkeznek,

g) [3] kiadja a rejtjeltevékenységre vonatkozó rejtjel-hozzáférési engedélyeket,

h) kivizsgálja a rendszerbiztonsági eseményeket.

---

1 Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 35. § b). Hatálytalan: 2020. VII. 31-től.
2 Beiktatta: 340/2019. (XII. 23.) Korm. rendelet 2. §. Hatályos: 2020. I. 1-től.
3 Megállapította: 375/2020. (VII. 30.) Korm. rendelet 32. §. Hatályos: 2020. VII. 31-től.

6. Rendszerbiztonsági felügyelet

9. § (1) A minősített adatot elektronikus rendszeren kezelő szerv vezetője rendszerbiztonsági felügyelőt jelöl ki vagy – amennyiben a minősített anyagok mennyisége indokolja –rendszerbiztonsági felügyeletet (a továbbiakban együtt: rendszerbiztonsági felügyelet) hoz létre.

(2) Több rendszerbiztonsági felügyelet létrehozása esetén a minősített adatot elektronikus rendszeren kezelő szerv központi rendszerbiztonsági felügyeletet működtet.

(3) Az országos vagy több szervre kiterjedő rendszerhez kapcsolódáskor a minősített adatot elektronikus rendszeren kezelő szerven belül nem hoznak létre rendszerbiztonsági felügyeletet, ha a rendszerbiztonsági feladatok ellátása központilag biztosított.

10. § A rendszerbiztonsági felügyelet feladatai:

a) érvényesíti az elektronikus biztonsági követelményeket a rendszer teljes életciklusában,

b) irányítja és ellenőrzi a rendszerbiztonsági feladatokat ellátó személyek tevékenységét és a rendszerbiztonsággal kapcsolatos feladatok végrehajtását,

c) felelős a biztonsági dokumentáció elkészítéséért,

d) felügyeli a rendszer biztonságos üzemeltetését,

e) végzi a rendszerbiztonsággal kapcsolatos továbbképzési feladatokat,

f) naprakész nyilvántartást vezet a felügyelete alá tartozó rendszerekről, tárolja ezek biztonsági dokumentációját és az ezt kiegészítő tanúsítványokat,

g) érvényesíti az üzemeltetés-biztonsági szabályzat előírásait, valamint megismerteti azt a felhasználókkal.

7. Rejtjelfelügyelet

11. § (1) Rejtjeltevékenységet folytató szerv vezetője rejtjelfelügyelőt jelöl ki vagy – amennyiben a minősített anyagok mennyisége indokolja – rejtjelfelügyeletet hoz létre (a továbbiakban együtt: rejtjelfelügyelet).

(2) Több rejtjelfelügyelet létrehozása esetén a rejtjeltevékenységet folytató szerv központi rejtjelfelügyeletet működtet.

(3) Az országos vagy több szervre kiterjedő rejtjelzéssel védett hírközlő hálózatba kapcsolódáskor a rejtjeltevékenységet folytató szerven belül nem hoznak létre rejtjelfelügyeletet, ha a rejtjel-felügyeleti feladatok ellátása központilag biztosított.

12. § A rejtjelfelügyelet feladatai:

a) irányítja a rejtjeltevékenységet,

b) elkészíti a rejtjeltevékenységre vonatkozó biztonsági dokumentációt,

c) gondoskodik az engedélyezett rejtjelző eszközök telepítéséről, rendeltetésszerű és biztonságos működtetéséről, szükség szerinti karbantartásáról és javíttatásáról,

d) gondoskodik a szükséges rejtjelkulcsok beszerzéséről, elosztásáról, nyilvántartásáról,

e) nyilvántartja és őrzi a rejtjeltevékenységgel kapcsolatos engedélyeket, szükség esetén kezdeményezi hosszabbításukat, visszavonásukat,

f) megszervezi a rejtjelző eszközök alkalmazásához előírt tanfolyamok és vizsgák lebonyolítását,

g) ellenőrzi a szervezet rejtjeltevékenységére vonatkozó szabályok betartását, annak eredményéről tájékoztatja a szervezet biztonsági vezetőjét,

h) a rejtjelbiztonság veszélyeztetése esetén – a szerv biztonsági vezetője és az NBF egyidejű értesítése mellett – intézkedik a biztonság helyreállítására,

i) részt vesz az alárendeltségébe tartozó rejtjelző szolgálatoknak az NBF általi ellenőrzésében,

j) felelős a rejtjelanyagoknak a központi rejtjelelosztó hatóságoktól történő átvételéért, nyilvántartásáért, tárolásáért, valamint az ehhez szükséges rendszer kiépítéséért, továbbá az arra vonatkozó biztonsági intézkedések betartásáért.

8. Rendszeradminisztrátor

13. § (1) A minősített adatot elektronikus rendszeren kezelő szerv vezetője rendszeradminisztrátort jelöl ki.

(2) Az országos vagy több szervre kiterjedő rendszerbe kapcsolódáskor a minősített adatot elektronikus rendszeren kezelő szerv nem jelöl ki rendszeradminisztrátort, amennyiben az üzemeltetési felügyeleti feladatok ellátása más szerv által központilag biztosított.

14. § A rendszeradminisztrátor feladatai:

a) a rendszer működtetése és működőképességének fenntartása,

b) részvétel a rendszerek tervezési, fejlesztési, módosítási folyamataiban, technikai megvalósításában,

c) részvétel az elektronikus biztonsági ellenőrzésekben és azok előkészítésében,

d) vírusvédelmi eljárásrend kidolgozása és betartása,

e) naprakész nyilvántartás vezetése a rendszer elemeiről, a rendszerre telepített szoftverekről,

f) a felhasználók nevéről és jogosultságairól naprakész nyilvántartás vezetése,

g) tanácsadás és segítségnyújtás a felhasználóknak.

9. A rejtjelző, a rejtjelző szolgálatok

15. § A rejtjelző, valamint a rejtjelző szolgálatok feladatai:

a) a szakmai és a biztonsági szabályok betartásával üzemelteti a rejtjelző eszközöket, végrehajtja a rejtjelzési feladatokat,

b) ellátja a rejtjeltevékenységgel kapcsolatban számára meghatározott adatkezelési, eszköz nyilvántartási feladatokat,

c) részt vesz a rejtjeltevékenységgel összefüggő képzéseken, továbbképzéseken, tájékoztatókon, teljesíti az előírt vizsgakötelezettségeket,

d) részt vesz a rejtjelzői munkahely kialakításában, a rejtjelző eszközök telepítésében,

e) közreműködik a rejtjelző eszközök üzemképességének biztosításában, értesíti a rejtjelfelügyelőt a rejtjelző eszközök meghibásodásáról és az időszakos karbantartások esedékességéről.

III. FEJEZET

A RENDSZERRE VONATKOZÓ SZEMÉLYI BIZTONSÁGI KÖVETELMÉNYEK

16. § A rendszerre, valamint a rendszer minősített adathordozóira vonatkozó személyi biztonsági követelményekre a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet előírásai az irányadóak az e fejezetben foglalt kiegészítésekkel.

17. §[1] A rendszerbiztonsági felügyelő nem lehet rendszeradminisztrátor.

10. Rejtjeltevékenységgel kapcsolatos személyi biztonsági követelmények

18. § (1) A rejtjelanyaghoz az a személy férhet hozzá, aki a rejtjelanyagokhoz történő hozzáféréshez rejtjel-hozzáférési engedéllyel rendelkezik.

(2) Rejtjel-hozzáférési engedélyt az kaphat, akinek munkaköri feladatai ellátásához a rejtjeltevékenységgel kapcsolatos ismeretek birtoklása feltétlenül szükséges.

1 Módosította: 303/2024. (X. 24.) Korm. rendelet 27. § b).

19. § A munkakörbe kinevezésre jogosult vezető a rejtjel-hozzáférési engedélyben feltünteti azokat a tárgyköröket, valamint meghatározott rejtjelanyagokat, amelyekre az engedély vonatkozik. Amennyiben a felhasználás feltételei megszűnnek, a kinevezésre jogosult vezető az engedélyt haladéktalanul visszavonja.

20. § A minősített adatot elektronikus rendszeren kezelő szerv vezetője, az általa kinevezett biztonsági vezető, valamint a minősített adat védelméről szóló 2009. évi CLV. törvény 13. § (3) bekezdésben meghatározott személyek a rejtjeltevékenységgel kapcsolatos adatokat rejtjel-hozzáférési engedély nélkül is megismerhetik.

21. § (1) Rejtjelző eszközt az üzemeltethet, aki

a) a feladat biztonságos ellátásához szükséges személyi biztonsági követelményeknek megfelel, és a rejtjelfelügyelet a megbízással egyetért,

b) a 18. §-ban meghatározott felhasználói jogosultsággal rendelkezik,

c) az általa üzemeltetendő rejtjelző eszköz biztonsági dokumentációjában előírt speciális követelményeknek megfelel,

d) az általa üzemeltetendő rejtjelző eszköz biztonságos üzemeltetéséhez szükséges elméleti és gyakorlati ismereteket nyújtó tanfolyamot elvégezte, a tanfolyam anyagából sikeres vizsgát tett, valamint számára a rejtjelfelügyelet kezelői engedélyt adott ki.

(2) A rejtjelfelügyelet a kezelői engedélyben megjelöli azokat a rejtjelző eszközöket, amelyeknek üzemeltetésére az engedély jogosít.

(3) Az (1) és (2) bekezdés vonatkozik a rejtjelző eszközök javítására vagy karbantartására vonatkozó kezelői engedélyek kiadására is. A kezelői engedély kezelői szintű karbantartásra is jogosít.

(4) A kezelői engedély szabályai vonatkoznak a szakértői tevékenységre is.

IV. FEJEZET

A RENDSZERRE VONATKOZÓ FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK

22. § (1) A rendszerre, valamint a rendszer minősített adathordozóira vonatkozó fizikai biztonsági követelményekre a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet előírásai az irányadóak az e fejezetben foglalt kiegészítésekkel.

(2) A rendszer védelmét a rendszeren a rendszerengedélyben meghatározott legmagasabb minősítési szintnek megfelelő fizikai biztonság kialakításával kell biztosítani.

(3) „Bizalmas!” és ennél magasabb minősítési szintű adatot kezelő rendszert I. vagy II. osztályú biztonsági területen kell telepíteni. „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszer adminisztratív zónában is telepíthető.

(4) A rendszert illetéktelen hozzáférést kizáró módon kell telepíteni és üzemeltetni.

(5)[1] Ha a legfeljebb „Bizalmas!” minősítési szintű nemzeti minősített adatokat kezelő rendszer és elemei II. osztályú biztonsági területen helyezkednek el, a rendszer minősített adathordozói tekintetében biztonsági tárolónak, illetve zárnak tekinthető, ha az adathordozóhoz való hozzáférést legalább 1. kategóriájú tárolóval azonos szintű védelmet nyújtó zárható burkolattal vagy az adathordozó eltávolítását legalább 1. kategóriájú zárszerkezet alkalmazásával akadályozzák meg.

(6)[2] Állami szervek esetében, ha a legfeljebb „Titkos!” minősítési szintű nemzeti minősített adatokat kezelő rendszer és elemei 1. kategóriájú biztonsági tároló használatával engedélyezett II. osztályú biztonsági területen helyezkednek el, a rendszer minősített adathordozói tekintetében biztonsági tárolónak, illetve zárnak tekinthető, ha az adathordozóhoz való hozzáférést legalább 1. kategóriájú tárolóval azonos szintű védelmet nyújtó zárható burkolattal vagy az adathordozó eltávolítását legalább hagyományos zárszerkezet alkalmazásával akadályozzák meg.

---

1 Beiktatta: 318/2015. (X. 30.) Korm. rendelet 2. §. Hatályos: 2015. XI. 7-től.
2 Beiktatta: 323/2018. (XII. 28.) Korm. rendelet 11. §. Hatályos: 2019. I. 1-től.

(7)[1] A nemzeti minősített adatot kezelő elektronikus rendszert biztonsági területen kívül, adminisztratív zónában, a biztonsági vezető által megjelölt helyszínen, kizárólag személyes felügyelet alatt lehet üzemeltetni. Nemzeti „Titkos!” vagy „Szigorúan titkos!” elektronikus rendszer esetén a rendszer elemeinek meg kell felelnie a TEMPEST követelményeknek.

11. Rejtjeltevékenységgel kapcsolatos fizikai biztonsági követelmények

23. § (1)[2]

(2) A rejtjeltevékenységet folytató szerv az állandó telepítésű rejtjelző eszköz áthelyezése előtt az NBF-et a tervezett változtatásról tájékoztatja. Amennyiben a rejtjelző eszköz biztonsága megköveteli vagy működtetési szabályzata és kezelési utasítása ezt előírja, a rejtjeltevékenységet folytató szerv új rendszerengedélyt kér.

24. § (1) A rejtjelző eszközök kezelésének, őrzésének, szállításának, javításának, az azokkal folytatott rejtjelző munka ellátásának biztonsági követelményeit a rejtjeltevékenységre vonatkozó biztonsági dokumentáció tartalmazza. A rejtjelző eszközhöz kiadott speciális biztonsági követelményeket az eszközhöz kiadott működtetési szabályzat tartalmazza.

(2) A rejtjeltevékenységet folytató szerv a rejtelző eszközök, módszerek üzemeltetésével, tárolásával, valamint fejlesztésével, gyártásával kapcsolatos helyiségek fizikai biztonságának kialakításakor biztosítja, hogy a rendszer rejtjelzéssel kapcsolatos elemeihez felügyelet nélkül kizárólag olyan személy férhessen hozzá, akinek a munkaköre ellátásához az feltétlenül szükséges, más személy hozzáférését korlátozza, még akkor is, ha rendelkezik a megfelelő szintű személy biztonsági tanúsítvánnyal.

V. FEJEZET

A RENDSZERRE VONATKOZÓ ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK

25. § (1) A rendszerre, valamint a rendszer minősített adathordozóira vonatkozó adminisztratív biztonsági követelményekre a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendelet előírásai az irányadóak az e fejezetben foglalt eltérésekkel.

(2) A minősített adatot elektronikus rendszeren kezelő szerv minden, a rendszerben alkalmazott adathordozót a rajta tárolható legmagasabb minősítéssel rendelkező adat minősítési szintjének megfelelően kezeli és nyilvántartja. A beépített adathordozóval ellátott rendszer önmagában is adathordozónak minősül.

(3) A minősített adat adathordozón akkor kezelhető, ha a tényleges használatba vétel előtt az adathordozó nyilvántartásba került. A minősített adatot elektronikus rendszeren kezelő szerv az adathordozón feltünteti az azon tárolható legmagasabb minősítési szintű adat minősítési szintjét, valamint a nyilvántartási számot. Amennyiben ez nem lehetséges, a minősített adatot elektronikus rendszeren kezelő szerv a fel nem tüntethető azonosítók dokumentálására külön kísérőlapot készít. Az ilyen módon jelölt adathordozót úgy kezeli és védi, mintha az ténylegesen az engedélyezett legmagasabb minősítésű adatot tartalmazná.

(4) Az adathordozóra a feltüntetett minősítési szintnél magasabb minősítési szintű minősített adat nem kerülhet, kivéve, ha az adathordozón feltüntetett minősítési szintet a magasabb minősítési szintnek megfelelően módosítják.

1 Beiktatta: 323/2018. (XII. 28.) Korm. rendelet 11. §. Hatályos: 2019. I. 1-től.
2 Hatályon kívül helyezte: 303/2024. (X. 24.) Korm. rendelet 28. § a). Hatálytalan: 2024. X. 25-től.

(5)[1] A minősített adatot elektronikus rendszeren kezelő szerv a rendszerhez kapcsolódó – adathordozónak nem minősülő – elektronikus eszközön feltünteti a rendszer által kezelhető legmagasabb minősítési szintet.

26. § (1) A „Bizalmas!” és a „Korlátozott terjesztésű!” minősítési szintű adatot tartalmazó adathordozón feltüntetett minősítési szint alacsonyabb szintre megváltoztatható vagy megszüntethető, ha az azon tárolt minősített adat olyan módszerek alkalmazásával lett törölve, hogy az a későbbiekben ne legyen helyreállítható.

(2) A „Titkos!” és a „Szigorúan titkos!” minősítési szintű adatot tartalmazó adathordozón feltüntetett minősítési szint nem változtatható meg alacsonyabb minősítési szintre.

27. § (1) Az olyan adathordozó, amelyet nem lehet engedélyezett módon újra felhasználni, alacsonyabb minősítési szintű jelzéssel ellátni vagy a minősítési jelzését megszüntetni, vagy amely a működőképességét elvesztette, a feltüntetett minősítési szintjének megfelelő engedélyezett eljárásokkal megsemmisíthető.

(2) A minősített adatot elektronikus rendszeren kezelő szerv az adathordozót – annak megsemmisítéséig – a feltüntetett minősítési szintnek megfelelően kezeli.

(3) Amennyiben valamely saját készítésű minősített adatról nem készült biztonsági másolat, és az adat megőrzésére jogszabályban foglalt kötelezettség, vagy üzemeltetési okok miatt szükség van, a minősített adatot tároló adathordozó a minősítés érvényességi idejének lejárati ideje előtt nem semmisíthető meg.

28. § (1)[2] A rendszer elemeit az adminisztratív zónából, valamint a biztonsági területről nem üzemeltetés céljából kivinni kizárólag az adathordozó – és minden más, adat visszanyerésére alkalmas részegység – eltávolítását és biztonsági területen hagyását követően szabad, kivéve a más adminisztratív zónába vagy biztonsági területre történő szállítást.

(2) A minősített adatot elektronikus rendszeren kezelő szerv naprakész nyilvántartást vezet a rendszerben alkalmazott hardverekről, szoftverekről.

(3) A katonai, nemzetbiztonsági és bűnügyi műveletekben a személyi biztonsági tanúsítvánnyal rendelkező személy folyamatos személyes felügyelete alatt álló rendszer, valamint annak eleme a biztonsági vezető által meghatározott biztonsági intézkedések betartása mellett biztonsági területen kívül is használható.

12. A rejtjeltevékenységgel kapcsolatos külön adminisztratív biztonsági követelmények

29. § (1) A rejtjeltevékenységet folytató szerv elkülönített rejtjelügyvitelt és rejtjelanyag-nyilvántartást vezet.

(2) A rejtjeltevékenységet folytató szerv a rejtjelanyagok és a rejtjeleszközök átadásának és átvételének tényét rögzíti.

(3) A rejtjelanyagok elektronikus nyilvántartó rendszerben történő kezelésének szabályait a minősített adatot elektronikus rendszeren kezelő szerv a rejtjelszabályzatban vagy a rendszerbiztonsági dokumentációjában határozza meg.

(4) A rejtjeltevékenységet folytató szerv a rejtjeltevékenységgel kapcsolatos iratkezelési okmányrendszerét és a rejtjelanyagot elkülönített tároló helyen őrzi.

VI. FEJEZET

RENDSZERBIZTONSÁG

30. § A rendszerbiztonsági követelmények célja a minősített adat bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása a rendszer hardver, szoftver és hálózati biztonságának megteremtése révén.

---

1 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 20. §. Hatályos: 2024. X. 25-től.
2 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 12. §. Hatályos: 2019. I. 1-től.

13. Hardverbiztonság

31. § (1) A minősített adatot elektronikus rendszeren kezelő szerv a rendszer által kezelhető minősített adat legmagasabb minősítési szintjét egyértelműen azonosítható módon feltünteti a rendszer főbb elemein.

(2) A rendszerbiztonsági felügyelet a rendszer illetéktelen módosításának, valamint a rendszerhez nem tartozó eszközök rendszerhez való csatlakoztatásának megakadályozása érdekében gondoskodik a rendszer megbontható hardver eszközeinek és csatlakozásainak a lezárásáról. Ezt a védelmet kizárólag a rendszerbiztonsági dokumentációban megnevezett és a rendszerbiztonsági felügyelet engedélyével rendelkező személy bonthatja meg.

(3) A hardver védelmét a rendszerbiztonsági felügyelet rendszeresen ellenőrzi, s amennyiben rendellenességet talál, azt azonnal kivizsgálja, és helyreállítja a biztonságot.

32. § (1) Minősített adatot tartalmazó rendszer karbantartását csak olyan, megfelelő szintű személyi biztonsági tanúsítvánnyal rendelkező személy végezheti, aki rendelkezik a rendszerbiztonsági felügyelet engedélyével. Ez alól kivételt képez, ha minden olyan hardver elemet eltávolítottak, amely minősített adatokat tartalmazhat vagy ezen hardver elemek minősítési szintjét engedélyezett eljárással megszüntették.

(2) A TEMPEST tanúsítvánnyal rendelkező készülék, berendezés, eszköz elveszíti TEMPEST tanúsítványát a megbontást igénylő javítását követően, kivéve, ha az eszköz TEMPEST tanúsítványa ettől eltérő rendelkezést határoz meg.

(3) A felhasználó a rendszer semmilyen elemét nem bonthatja meg, ahhoz eszközöket nem csatlakoztathat, kivéve, ha a rendszerbiztonsági felügyelet a felhasználó részére erre engedélyt ad.

14. Szoftverbiztonság

33. § (1) Szoftverek telepítését a rendszerbiztonsági felügyelet, vagy annak engedélyével a rendszeradminisztrátor végezheti.

(2) A rendszerbiztonsági felügyelet, vagy annak engedélyével a rendszeradminisztrátor minden szoftvert és frissítését, amelyet a rendszerre telepíteni kíván, biztonsági ellenőrzés alá vet a telepítést megelőzően, elsősorban vírus vagy más rosszindulatú szoftver kiszűrése érdekében.

34. § (1) A minősített adatot elektronikus rendszeren kezelő szerv az NBF által jóváhagyott biztonsági konfigurációt alkalmazza.

(2) A minősített adatot elektronikus rendszeren kezelő szerv a felhasználók számára technikai eszközökkel megakadályozza, hogy külső adathordozóról való rendszerindítást követően a rendszer szolgáltatásai, valamint a rendszeren tárolt minősített adatok elérhetőek legyenek.

(3) A felhasználók részére a rendszerhez történő hozzáférést a biztonsági konfigurálást követően lehet biztosítani.

(4) A rendszer működését szabályozó konfigurációs beállításokhoz és a biztonsági célból naplózott adatokhoz csak a rendszerbiztonsági felügyelet, valamint a rendszerbiztonsági felügyelet engedélyével a rendszeradminisztrátor férhet hozzá.

34/A. §[1] (1) A minősített adatot elektronikus rendszeren kezelő szerv az NBF által jóváhagyott operációs rendszert alkalmaz.

(2)[2] Az operációs rendszert az operációs rendszerrel kapcsolatosan Magyarország kiberbiztonságáról szóló törvény szerinti kiberbiztonsági incidenskezelő központ által kiadott riasztást követően azonnal, de legalább havonta frissíteni kell.

---

1 Beiktatta: 323/2018. (XII. 28.) Korm. rendelet 13. §. Hatályos: 2019. I. 1-től.
2 Módosította: 418/2024. (XII. 23.) Korm. rendelet 122. §.

35. § (1) A rendszer biztonsági konfigurációja tartalmazza azokat a naplózási funkciókat, amelyek lehetővé teszik, hogy biztonsági ellenőrzéskor, valamint biztonságot sértő esemény gyanújának felmerülésekor a biztonságot sértő események kivizsgálhatóak legyenek.

(2) A rendszerbiztonsági felügyelet a naplófájlokat a biztonsági dokumentációban meghatározott időszakonként ellenőrzi, az ellenőrzés végrehajtását és eredményét dokumentálja.

(3)[1] A rendszeradminisztrátor a hat hónapnál régebbi naplófájlokról biztonsági mentéseket készít. A naplófájlokról készült biztonsági mentéseket 8 évig kell megőrizni.

15. Hozzáférési jogosultságok

36. § (1) A rendszerhez való hozzáférést a felhasználó megbízható azonosítása előzi meg. Ez történhet személyes használatra kiadott egyedi felhasználói névvel és ehhez tartozó, kizárólag a felhasználó által ismert jelszóval vagy ennél nagyobb biztonságot jelentő technológiával.

(2) A minősített adatot elektronikus rendszeren kezelő szerv a jelszavak illetéktelen megismerésének lehetőségét kizárja, illetéktelen megismerés esetén a megismert jelszót azonnal cseréli.

(3) Több felhasználóra azonos felhasználónév nem engedélyezhető.

(4)[2] A jelszóval történő azonosítás esetén alkalmazandó jelszóházirend minimumkövetelményeit az NBF határozza meg.

(5) A sikertelen és jogosulatlan rendszer-hozzáférési kísérleteket a minősített adatot elektronikus rendszeren kezelő szerv a jogosulatlan hozzáférési kísérletek és a felhasználói hibák elkülönítése érdekében naplózza és ellenőrzi.

(6) A minősített adatot elektronikus rendszeren kezelő szerv a rendszeradminisztrátor jelszavait lepecsételt borítékban, a rendszerre vonatkozó rendszerengedély által meghatározott minősített adat legmagasabb minősítési szintjének megfelelő biztonsági körülmények között tárolja.

37. § (1) A minősített adatot elektronikus rendszeren kezelő szerv a rendszer felhasználóihoz írási, olvasási vagy törlési hozzáférési jogokat rendel.

(2) A rendszer alkalmas a hozzáférési jogok egyedi vagy csoportszinten való megkülönböztetésére és szabályozására.

16.[3]

38. §[4]

17. Vírusvédelem

39. § (1)[5] A minősített adatot elektronikus rendszeren kezelő szerv a vírusok és más rosszindulatú szoftverek azonosítására és eltávolítására az NBF által jóváhagyott vírusvédelmi szoftvert alkalmaz.

(2) A minősített adatot elektronikus rendszeren kezelő szerv a védelmet úgy konfigurálja, hogy az állandóan üzemeljen és automatikus ellenőrzést hajtson végre rendszerindításkor, valamint külső adathordozó használatakor.

(3) A minősített adatot elektronikus rendszeren kezelő szerv a vírusvédelem adatbázisát rendszeresen frissíti.

---

1 Megállapította: 303/2024. (X. 24.) Korm. rendelet 21. §. Hatályos: 2024. X. 25-től.
2 Megállapította: 303/2024. (X. 24.) Korm. rendelet 22. §. Hatályos: 2024. X. 25-től.
3 Hatályon kívül helyezte: 323/2018. (XII. 28.) Korm. rendelet 22. § c). Hatálytalan: 2019. I. 1-től.
4 Hatályon kívül helyezte: 323/2018. (XII. 28.) Korm. rendelet 22. § c). Hatálytalan: 2019. I. 1-től.
5 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 14. §. Hatályos: 2019. I. 1-től.

18. Hálózatbiztonság

40. § (1) A rendszerek összekapcsolását az NBF engedélyezi.

(2) Az összekapcsolás csak a rendszerek közötti adatforgalom felügyeletét lehetővé tevő és biztonságát garantáló rendszer közbeiktatásával engedélyezhető.

(3) A rendszerek összekapcsolásánál a rendszerre a rendszerengedélyben meghatározottnál magasabb minősítési szintű adat nem kerülhet át.

(4)[1] A rendszerek összekapcsolása során kizárólag az NBF, illetve a NATO vagy az EU által engedélyezett technikai megoldás, eszköz alkalmazható.

(5)[2] Az NBF a – NATO vagy EU által engedélyezetteken kívüli – technikai megoldás, eszköz minősített adatot kezelő rendszerekben történő alkalmazhatóságát érintően elektronikus információbiztonsági szempontból kikéri a Nemzetbiztonsági Szakszolgálat szakvéleményét.

VII. FEJEZET

REJTJELBIZTONSÁG

41. § (1) A rejtjeltevékenységet folytató szerv a minősített adatot rejtjelzéssel védi, ha vezetékes vagy vezeték nélküli adatátviteli rendszerben történő továbbítás során az adat a minősített adatot elektronikus rendszeren kezelő szerv által ellenőrzött területen kívülre kerül vagy amennyiben egy adott rendszeren belül a szükséges ismeret elvének betartása rejtjelzéssel oldható meg.

(2) A minősített adat rejtjelzett formája minősítés nélküliként kezelhető és nyílt csatornán is továbbítható, amennyiben rendszerengedéllyel rendelkező rejtjelző eszköz alkalmazásával történt a rejtjelzés és a rejtjeltevékenységre vonatkozó szabályokat és előírásokat maradéktalanul betartották.

(3) A rejtjeltevékenységet folytató szerv rejtjeltevékenysége során csak olyan rejtjelző eszközt alkalmazhat, amelyre vonatkozóan az NBF rendszerengedélyt adott ki.

(4)[3] Nemzeti minősített adat rejtjelzésére az NBF által rendszeresített

a) a 44/A. § szerinti nemzeti fejlesztésű rejtjelző eszköz alkalmazható, amelynek fejlesztője esetében az NBF a rejtjelző eszközre vonatkozóan – a létrehozására vonatkozó döntéstől a tervezést, a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást is érintően, a rendszer egyes elemeinek vagy egészének a kivonásáig és megsemmisítéséig – megbízhatóan meggyőződött arról, hogy nem áll fenn a bizalmasság elve sérülésének veszélye, vagy

b) külföldi rejtjelző eszköz alkalmazható.

(5)[4] Külföldi rejtjelző eszköz nemzeti minősített adat rejtjelzésére történő alkalmazása esetén

a) a rejtjeltevékenységet folytató szerv beszerzi a rejtjelző eszközt és az ahhoz tartozó kulcsgyártó eszközt, és ellátja azok üzemeltetését,

b) a rejtjelző eszközhöz tartozó rejtjelkulcsok váltása és kezelése a rejtjeltevékenységet folytató szerv feladata,

c) az eszköz által igénybe vett kommunikációs csatornát

ca) a rejtjeltevékenységet folytató szerv tulajdonában lévő hálózaton,

cb) bérelt – a rejtjelzéssel érintett minősített adatot elektronikusan kezelő szerveken kívül más által nem használt – hálózaton,

cc) kormányzati célú elkülönült hírközlő hálózaton kell biztosítani,

---

1 Beiktatta: 243/2016. (VIII. 17.) Korm. rendelet 36. §. Hatályos: 2016. VIII. 25-től.
2 Beiktatta: 243/2016. (VIII. 17.) Korm. rendelet 36. §. Hatályos: 2016. VIII. 25-től.
3 Megállapította: 303/2024. (X. 24.) Korm. rendelet 23. § (1). Hatályos: 2024. X. 25-től.
4 Megállapította: 303/2024. (X. 24.) Korm. rendelet 23. § (1). Hatályos: 2024. X. 25-től.

d) a rejtjeltevékenységet folytató szerv a *c)* pont *ca)* és *cb)* alpontja szerinti hálózaton hálózati kommunikációt, forgalmat figyelő eszközt alkalmaz, és ellátja a hálózati kommunikációt, forgalmat figyelő eszköz működtetéséhez kapcsolódó feladatokat,

e) a rejtjeltevékenységet folytató szerv ellátja a rejtjelző eszköz telepítésével, üzembe helyezésével kapcsolatos feladatokat.

(6)[1] Az (5) bekezdés *a)* pontjában meghatározott, a kulcsgyártó eszköz beszerzéséhez, üzemeltetéséhez kapcsolódó feladat alól kivételt képez, ha a rejtjelző eszközhöz tartozó kulcsgyártó eszköz más rejtjeltevékenységet folytató szervnél rendelkezésre áll és e szerv az üzemeltetéssel kapcsolatos feladatok ellátását vállalja.

42. § (1) Külföldi minősített adat rejtjelzése esetén a vonatkozó nemzetközi és nemzeti előírások az irányadóak a rejtjeltevékenységre vonatkozóan.

(2)[2] Külföldi minősítésű adat „Bizalmas!” minősítési szintig a 41. § (4) bekezdés *a)* pontjában meghatározott rejtjelző eszközön is továbbítható, amennyiben az NBF által kiadott rendszerengedély ezt lehetővé teszi.

(3)[3] A NATO által engedélyezett eszközök a NATO által meghatározott minősítési szintig alkalmazhatóak NATO minősített adatok rejtjelzésére.

(4)[4] A NATO tagállamai által engedélyezett eszközök az engedélyben meghatározott, de legfeljebb „Bizalmas!” minősítési szintig alkalmazhatóak NATO minősített adatok rejtjelzésére.

(5)[5] Az EU által engedélyezett eszközök az EU által meghatározott minősítési szintig alkalmazhatóak EU minősített adatok rejtjelzésére.

(6)[6] Az EU tagállamai által engedélyezett eszközök az engedélyben meghatározott, de legfeljebb „Bizalmas!” minősítési szintig alkalmazhatóak EU minősített adatok rejtjelzésére.

(7)[7] A (3)–(6) bekezdésben meghatározott esetekben nincs szükség rendszeresítési engedély kiadására.

VIII. FEJEZET

ENGEDÉLYEZÉSI ELJÁRÁSOK

19. Rendszerengedély kiadása

43. § (1) Rendszert létesíteni, üzemeltetni, működését meghosszabbítani, rendszereket összekapcsolni, megszüntetni, engedélyezett rendszeren az elektronikus biztonságot érintő módosítást végrehajtani az NBF által kiadott rendszerengedéllyel lehet.

(2)[8] A rendszerengedély iránti kérelmet a minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője írásban, az NBF honlapján közzétett nyomtatvány kitöltésével nyújtja be az NBF-nek.

(3)[9]

(4) Az NBF hatósági eljárás keretében ellenőrzi a rendszerre vonatkozó elektronikus biztonsági követelmények teljesülését és annak megfelelőssége esetén kiadja a rendszerengedélyt.

(5) A rendszerengedély érvényességi ideje legfeljebb 3 év.

---

1 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 23. § (2). Hatályos: 2024. X. 25-től.
2 Módosította: 303/2024. (X. 24.) Korm. rendelet 27. § c).
3 Megállapította: 303/2024. (X. 24.) Korm. rendelet 24. § (1). Hatályos: 2024. X. 25-től.
4 Megállapította: 303/2024. (X. 24.) Korm. rendelet 24. § (1). Hatályos: 2024. X. 25-től.
5 Megállapította: 303/2024. (X. 24.) Korm. rendelet 24. § (1). Hatályos: 2024. X. 25-től.
6 Megállapította: 303/2024. (X. 24.) Korm. rendelet 24. § (1). Hatályos: 2024. X. 25-től.
7 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 24. § (2). Hatályos: 2024. X. 25-től.
8 Módosította: 457/2017. (XII. 28.) Korm. rendelet 301. §, 303/2024. (X. 24.) Korm. rendelet 28. § b).
9 Hatályon kívül helyezte: 303/2024. (X. 24.) Korm. rendelet 28. § c). Hatálytalan: 2024. X. 25-től.

(6)[1] A rendszer működésének meghosszabbítására irányuló kérelmet a rendszerengedély érvényességi idejének lejárta előtt legalább 30 nappal kell kezdeményezni.

(7)[2] A soron kívül elrendelt katonai műveletek, gyakorlatok, bemutatók, valamint a honvédelmi szervezetek soron kívüli feladatainak végrehajtásához szükséges rendszer működésének meghosszabbítására irányuló kérelem kezdeményezésének határideje a (6) bekezdésben meghatározottnál rövidebb is lehet.

44. § (1) A biztonsági vezető vagy a rendszerbiztonsági felügyelet a „Bizalmas!” vagy magasabb minősítési szintű adatot kezelő rendszer biztonsági követelményeinek kialakításával kapcsolatban előzetes egyeztetést kezdeményezhet, valamint helyszínbejárást kérhet az NBF-től.

(2) A „Szigorúan titkos!” minősítési szintű adatot kezelő rendszer esetén az NBF a helyszínbejárási kérelem teljesítését nem tagadhatja meg.

19/A.[3] Rejtjelző eszköz fejlesztése, gyártása

44/A. §[4] (1) Rejtjelző eszköz fejlesztését, illetve gyártását állami szerv vagy telephely biztonsági tanúsítvánnyal rendelkező, kizárólagos belföldi tulajdonban álló gazdálkodó szervezet végezheti.

(2) Rejtjelző eszköz fejlesztését, illetve gyártását végző szervezetnek rendelkeznie kell a fejlesztéshez kapcsolódó dokumentumok minősítési szintjének megfelelő, az NBF működésének, valamint a minősített adat kezelésének rendjéről szóló kormányrendeletben meghatározott engedéllyel, rendszerengedéllyel és rejtjelszabályzattal.

(3) A rejtjelző eszközzel kapcsolatos fejlesztési tevékenység, illetve a rejtjelző eszköz gyártásának engedélyezésére irányuló kérelmet az érintett minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője vagy a rejtjelző eszközt fejlesztő, illetve gyártó szerv vezetője nyújtja be írásban az NBF-nek.

(4) A rejtjelző eszközzel kapcsolatos fejlesztési tevékenység engedélyezésére irányuló kérelemnek tartalmaznia kell a tervezett eszköz megnevezését, jellegét, a védeni tervezett adat minősítési szintjét, valamint a fejlesztés befejezésének tervezett időpontját.

20. Rejtjelző eszköz rendszeresítése

45. § (1) Rejtjelző eszköz rendszeresítési engedélye iránti kérelmet az érintett minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője vagy a rejtjelző eszközt fejlesztő és gyártó szerv vezetője nyújtja be írásban az NBF-nek.

(2)[5] A rejtjeltevékenységet folytató szerv a rendszeresítési engedély iránti kérelemhez mellékelve az eszköz jellegétől függően benyújtja

a) minden, a rejtjelző eszköz rendeltetésszerű működéséhez és működtetéséhez szükséges eszközt,

b) a rejtjelezhető minősített adat javasolt legmagasabb minősítési szintjének megjelölését,

c) a rejtjelző eszköz teljes körű funkcionális és biztonsági leírását tartalmazó dokumentációt,

d) a rejtjelző eszköz gyártási és tesztelési dokumentációját,

e) a rejtjelző eszköz rendeltetésszerű működtetéséhez szükséges biztonsági feltételrendszerre vonatkozó ajánlásokat,

f) a rejtjelző eszköz működtetési szabályzatát, kezelési utasítását és a rejtjelző eszköz alkalmazásához szükséges egyéb dokumentumokat.

---

1 Beiktatta: 318/2015. (X. 30.) Korm. rendelet 3. §. Hatályos: 2015. XI. 7-től.
2 Beiktatta: 318/2015. (X. 30.) Korm. rendelet 3. §. Hatályos: 2015. XI. 7-től.
3 Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 33. §. Hatályos: 2020. VII. 31-től.
4 Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 33. §. Hatályos: 2020. VII. 31-től.
5 Megállapította: 375/2020. (VII. 30.) Korm. rendelet 34. §. Hatályos: 2020. VII. 31-től.

(3) A nemzeti minősített adatok védelmére alkalmazott külföldi rejtjelző eszközök esetében a rejtjeltevékenységet folytató szerv – a (2) bekezdésben foglaltaktól eltérően – a rendszeresítési engedély iránti kérelemben [1]
a) a jóváhagyó hatóság tanúsítványát,
b) az eszközre vonatkozó biztonsági dokumentációt
nyújtja be.
(4) Új vagy kiegészítő engedélyezési eljárásra van szükség, ha a rendszeresítési engedéllyel már rendelkező rejtjelző eszközt továbbfejlesztették, módosították.
(5) [2]
46. § (1) Rejtjelzésre olyan eszközök alkalmazhatók, amelyek biztosítják a rejtjelzési kötelezettség alá eső minősített adatok védelmét.
(2) A nemzeti minősített adatok védelmére alkalmazott rejtjelző eszköz (1) bekezdésben meghatározott alkalmasságát az NBF rendszeresítési engedély kiadásával állapítja meg, amely tartalmazza
a) a rejtjelző eszköz típusát és verzióját,
b) azt a legmagasabb minősítési szintet, amely minősítési szintű adatok védelmére a rejtjelző eszköz alkalmazható,
c) a rejtjelző eszköz, a működtetéséhez szükséges tartozékok, rejtjelkulcsok és dokumentációk minősítési szintjét,
d) a rejtjelző eszköz eszköz-specifikus biztonsági követelményeit.
(3) [3]
(4) Nemzeti minősített adat rejtjelzésére csak az NBF által kiadott rendszeresítési engedéllyel rendelkező rejtjelző eszköz alkalmazható.
(5) [4]

21. Rejtjeltevékenység engedélyezése

47. § (1) [5] Rejtjelző eszköz telepítése esetén a rejtjeltevékenységet folytató szerv a telepítést követő 15 napon belül megküldi az NBF részére a telepítési jegyzőkönyvet, amely tartalmazza különösen:
a) a rejtjelző eszköz nevét, típusát, verzióját és mennyiségét,
b) a rejtjelző eszköz telepítési helyének pontos meghatározását,
c) a rejtjelző eszköz használatával kapcsolatos szervezeti, személyi és adminisztratív feltételek teljesülésére vonatkozó adatokat, nyilatkozatokat.
(2) Telefon, mobil vagy tábori rejtjelző eszközök esetén az (1) bekezdésben meghatározottak közül csak az adott eszköz esetében értelmezhető adatokat szükséges megadni.
(3) [6] Amennyiben a rendszerengedély iránti kérelem rejtjeltevékenységgel kapcsolatos engedélyezést is magában foglal, a rejtjeltevékenységet folytató szerv a rendszerengedély iránti kérelemben – telepített rejtjelző eszköz esetén – megjelöli a telepítési jegyzőkönyv iktatószámát.
48. § (1) Az NBF engedélye szükséges továbbá:
a) a rejtjelző eszköznek az ország területéről történő kiviteléhez, külföldi használatához,
b) [7] a rejtjelző eszközzel kapcsolatos fejlesztési, gyártási, beszerzési tevékenységhez,
c) a rejtjelző eszközzel kapcsolatos karbantartó, javító tevékenységhez,
d) rejtjelző eszköz kiállításához vagy bemutatásához,
e) [8]

---

1 Módosította: 303/2024. (X. 24.) Korm. rendelet 27. § d).
2 Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 35. § c). Hatálytalan: 2020. VII. 31-től.
3 Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 35. § d). Hatálytalan: 2020. VII. 31-től.
4 Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 35. § d). Hatálytalan: 2020. VII. 31-től.
5 Megállapította: 303/2024. (X. 24.) Korm. rendelet 25. § (1). Hatályos: 2024. X. 25-től.
6 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 25. § (2). Hatályos: 2024. X. 25-től.
7 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 17. §. Hatályos: 2019. I. 1-től.
8 Hatályon kívül helyezte: 323/2018. (XII. 28.) Korm. rendelet 22. § d). Hatálytalan: 2019. I. 1-től.

(2) Az Országgyűlés, a Honvédelmi Tanács, vagy a Kormány döntése alapján a Magyar Honvédségnek a többnemzetiségű összfegyvernemi alkalmi harci kötelékben és gyakorlatokon résztvevő szervezetei számára a szervezetnél rendszeresített rejtjelző eszközök külföldre, valamint haza szállítására vonatkozóan az NBF engedélye nem szükséges. Az ilyen eszközökről a honvédelemért felelős miniszter nyilvántartást vezet.

48/A. §[1] (1) A felhasználó a birtokában lévő minősített adatot kezelő mobilkommunikációs eszközt a minősített adatot kezelő szerv vezetője vagy a biztonsági vezető által, a mobilkommunikációs eszközre vonatkozó biztonsági dokumentáció alapján meghatározott biztonsági intézkedések betartásával biztonsági területen kívül is használhatja, amely során köteles gondoskodni arról, hogy a minősített adat jogosulatlan személy részére ne váljon hozzáférhetővé.

(2) A 43. § (1) bekezdésétől eltérően a minősített adatot kezelő mobilkommunikációs eszközök – az üzemeltetéshez szükséges központi rendszerelemek kivételével – rendszerengedély nélkül használhatóak.

(3) A 49. § (1) bekezdésétől eltérően a minősített adatot kezelő mobilkommunikációs eszközöknek – az üzemeltetéshez szükséges központi rendszerelemek kivételével – nem kell megfelelnie a TEMPEST követelményeknek.

(4) A 48. § (1) bekezdés *b)* pontjától eltérően a minősített adatot kezelő mobilkommunikációs eszközök beszerzéséhez elegendő az NBF tájékoztatása.

22. A TEMPEST követelmények érvényesítése

49. §[2] (1) A „Bizalmas!” és magasabb minősítési szintű külföldi minősített adatot kezelő rendszer, valamint az adminisztratív zóna határától legfeljebb 8 méterre elhelyezkedő „Titkos!” és „Szigorúan titkos!” minősítési szintű nemzeti minősített adatot kezelő rendszer esetén a minősített adatot kezelő szerv gondoskodik a TEMPEST követelmények teljesítéséről.

(2) Az adminisztratív zóna határától legfeljebb 8 méterre elhelyezkedő „Titkos!” és „Szigorúan titkos!” minősítési szintű nemzeti minősített adatot kezelő rendszer esetén a legmagasabb TEMPEST védelmet biztosító rendszerelemek alkalmazása szükséges.

(3) Ha a (2) bekezdés szerinti TEMPEST védelmet biztosító rendszerelemek alkalmazása nem lehetséges, az NBF helyszíni szemle keretében, a TEMPEST biztonsági követelményekben meghatározottak szerint állapítja meg a TEMPEST védelem biztosítása érdekében alkalmazandó intézkedéseket.

50. § (1) A TEMPEST követelményeket kielégítő eszközök bevizsgálását az NBF végzi. A bevizsgálás alapján kiadott dokumentum tartalmazza:[3]

a) az eszköz konkrét típusát,

b) az eszköz TEMPEST besorolását,

c) az eszköz üzemeltetésére vonatkozó biztonsági követelményeket.

(2)[4] Az (1) bekezdésben foglaltakon túl az NBF által kijelölt szerv, a NATO, az EU vagy tagországaik TEMPEST hatósága által elfogadott vagy kiadott dokumentum további vizsgálatok nélkül is elfogadható.

51. § (1)[5] A „Bizalmas!” és magasabb minősítési szintű külföldi minősített adatot kezelő rendszer esetén az NBF meghatározza a rendszer telepítési helyének TEMPEST zóna besorolását.

(2) A TEMPEST zóna mérés és besorolás elvégzés érdekében a minősített adatot elektronikus rendszeren kezelő szerv az NBF részére az alábbi adatok megismerését biztosítja:

---

1 Beiktatta: 303/2024. (X. 24.) Korm. rendelet 26. §. Hatályos: 2024. X. 25-től.
2 Megállapította: 137/2025. (VI. 16.) Korm. rendelet 2. §. Hatályos: 2025. VI. 17-től.
3 Módosította: 323/2018. (XII. 28.) Korm. rendelet 21. §.
4 Módosította: 323/2018. (XII. 28.) Korm. rendelet 21. §.
5 Megállapította: 318/2015. (X. 30.) Korm. rendelet 5. §. Módosította: 137/2025. (VI. 16.) Korm. rendelet 4. §.

a) helyszínrajz és szöveges leírása, amely a telep teljes területét, határait és a szomszédos, nem saját ellenőrzés alá tartozó létesítmények elhelyezkedését mutatja,

b) alaprajz és szöveges leírása, amely a rendszer telepítési helyét magába foglaló épület, épületrész részletes rajzát tartalmazza oly módon, hogy a rendszer elemeinek telepítési helye egyértelműen meghatározható legyen,

c) telepítési alaprajz és szöveges leírása, amely a rendszer telepítési helyét magába foglaló helyiség részletes rajzát tartalmazza oly módon, hogy a rendszer elemeinek, a biztonságtechnikai eszközök és beléptető rendszer elemeinek, a helyiségekben levő eszközöknek és berendezéseknek, a hálózati áramellátásnak, biztonságtechnika és telefon kábeleknek és csatlakozóknak, a telepített rádiófrekvenciás szűrőknek, valamint a berendezési tárgyaknak a telepítési helye egyértelműen meghatározható legyen.

(3) A TEMPEST zóna mérését és TEMPEST besorolást az NBF végzi.

(4) A (3) bekezdésben foglaltakon túl az NBF által kijelölt szerv, a NATO, az EU vagy tagországaik TEMPEST hatósága által elfogadott vagy kiadott zóna besorolás további vizsgálatok nélkül is elfogadható.

IX. FEJEZET

ELLENŐRZÉS

52. § (1) Az NBF a rendszerengedélyek kiadását követően az elektronikus biztonság követelményeinek érvényesülését ellenőrzi.

(2) Internethez kapcsolódó rendszerek esetén az NBF – az NHBK folyamatos szakmai tájékoztatását is felhasználva – ellenőrizheti az elektronikus biztonság követelményeinek érvényesülését az internetről jelentkező fenyegetések ellen.

(3) Az NBF a rendszer, valamint a rendszeren kezelt minősített adatok védelme érdekében intézkedéseket határozhat meg. Amennyiben a minősített adatok védelme súlyosan veszélyeztetett, az NBF a kiadott engedélyeket visszavonhatja, intézkedések megtételére hívhatja fel a biztonsági vezetőt.

53. § Aki az elektronikus biztonsággal kapcsolatban szabálytalanságot vagy rendellenességet észlel, jelenti azt a biztonsági vezetőnek. A biztonsági vezető a bejelentést kivizsgálja, értesíti a NBF-et és intézkedést tesz a biztonság helyreállítására.

23. A rejtjeltevékenység ellenőrzésével kapcsolatos szabályok

54. § (1) A rejtjeltevékenység hatósági ellenőrzését az NBF végzi.

(2)[1] A rejtjeltevékenységgel kapcsolatos belső ellenőrzésre a minősített adatot elektronikus rendszeren kezelő szerv vezetője, a biztonsági vezető, rejtjelfelügyelő vagy a rejtjelfelügyelet vezetője és a szerv rejtjelszabályzatában meghatározott további személyek jogosultak.

55. § (1) Aki a rejtjeltevékenységgel kapcsolatban szabálytalanságot, rendellenességet észlel, jelenti azt a rejtjelfelügyeletnek.

(2) A rejtjelbiztonságot veszélyeztető eseményről a rejtjeltevékenységet folytató szerv az NBF-et haladéktalanul értesíti.

X. FEJEZET

ELEKTRONIKUS BIZTONSÁGI KÉPZÉS

1 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 18. §. Hatályos: 2019. I. 1-től.

56. § (1)[1] Az NBF a rendszerbiztonsági felügyeletek és rejtjelfelügyeletek részére évenként képzést tart az elektronikus és a rejtjelbiztonsággal kapcsolatban.

(2)[2] A rendszerbiztonsági felügyelő vagy a rendszerbiztonsági felügyelet vezetője és a rejtjelfelügyelő vagy a rejtjelfelügyelet vezetője, valamint az általa kijelölt személy a képzésen részt vesz.

57. §[3] A rendszer felhasználói részére a képzést a rendszerbiztonsági felügyelet és a rejtjelfelügyelet legalább kétévente megtartja.

XI. FEJEZET

BIZTONSÁGI DOKUMENTÁCIÓ, REJTJELSZABÁLYZAT

58. § (1) A biztonsági dokumentáció betartása kötelező a rendszert működtető vagy felhasználó szervekre, valamint személyekre.

(2) A biztonsági vezető a rendszer életciklusának kezdeti szakaszában megkezdi a biztonsági dokumentáció kidolgozását, és a rendszer megvalósítása során, valamint a rendszer életciklusának további szakaszaiban, kockázatelemzés és kockázatértékelés alapján a szükséges mértékben kiegészíti vagy módosítja.

59. § (1) A minősített adatot elektronikus rendszeren kezelő szerv a rendszerbiztonsági követelményeket minden „Bizalmas!” és magasabb minősítési szintű adatot kezelő rendszer esetében elkészíti.

(2) A minősített adatot elektronikus rendszeren kezelő szerv az üzemeltetési biztonsági szabályzatot minden minősített adatot kezelő rendszer esetében elkészíti.

(3) A minősített adatot elektronikus rendszeren kezelő szerv a rendszerbiztonsági követelményeket az internetre vagy más nyilvános hálózathoz kapcsolódó „Korlátozott terjesztésű!” minősítési szintű adatot kezelő rendszer esetében elkészíti.

60. § A rendszer felhasználói írásban nyilatkoznak az üzemeltetési biztonsági szabályzat tudomásulvételéről azelőtt, hogy a rendszerhez hozzáférési jogosultságot kapnának.

24. Rejtjeltevékenységgel kapcsolatos biztonsági dokumentáció

61. § (1) A rejtjeltevékenységet folytató szerv rejtjelszabályzatában részletezi a rejtjelfelügyelet hatáskörét, szervezeti és működési rendjét, feladatait, valamint a szervezet rejtjelanyagaira vonatkozó biztonsági követelményeket.

(2) A szervezet rejtjelszabályzatának kiadásához az NBF előzetes egyetértése szükséges.

XII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

62. § E rendelet a kihirdetését követő nyolcadik napon lép hatályba.

63. §[4] Ez a rendelet

a) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2013. szeptember 23-i 2013/488/EU tanácsi határozat,

b) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról szóló, 2015. március 13-i 2015/444/EU bizottsági határozat

végrehajtásához szükséges rendelkezéseket határoz meg.

---

1 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 19. §. Hatályos: 2019. I. 1-től.
2 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 19. §. Hatályos: 2019. I. 1-től.
3 Megállapította: 323/2018. (XII. 28.) Korm. rendelet 20. §. Hatályos: 2019. I. 1-től.
4 Megállapította: 137/2025. (VI. 16.) Korm. rendelet 3. §. Hatályos: 2025. VI. 17-től.

64. § [1]

---

1 Hatályon kívül helyezte: ugyene rendelet 64. § (2). Hatálytalan: 2010. V. 15-től.

TARTALOMJEGYZÉK

161/2010. (V. 6.) Korm. rendelet ---- 1
a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól ---- 1
I. FEJEZET ---- 1
ÁLTALÁNOS RENDELKEZÉSEK ---- 1
1. Értelmező rendelkezések ---- 1
II. FEJEZET ---- 4
AZ ELEKTRONIKUS BIZTONSÁG SZERVEZETE ---- 4
2. Az elektronikus biztonság központi szervezete ---- 4
3. A minősített adatot elektronikus rendszeren kezelő szerv vezetőjének feladatai ---- 5
4. Az elektronikus biztonság helyi szervezete ---- 6
5. A biztonsági vezető ---- 6
6. Rendszerbiztonsági felügyelet ---- 7
7. Rejtjelfelügyelet ---- 7
8. Rendszeradminisztrátor ---- 8
9. A rejtjelző, a rejtjelző szolgálatok ---- 8
III. FEJEZET ---- 8
A RENDSZERRE VONATKOZÓ SZEMÉLYI BIZTONSÁGI KÖVETELMÉNYEK ---- 8
10. Rejtjeltevékenységgel kapcsolatos személyi biztonsági követelmények ---- 8
IV. FEJEZET ---- 9
A RENDSZERRE VONATKOZÓ FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK ---- 9
11. Rejtjeltevékenységgel kapcsolatos fizikai biztonsági követelmények ---- 10
V. FEJEZET ---- 10
A RENDSZERRE VONATKOZÓ ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK ---- 10
12. A rejtjeltevékenységgel kapcsolatos külön adminisztratív biztonsági követelmények ---- 11
VI. FEJEZET ---- 11
RENDSZERBIZTONSÁG ---- 11
13. Hardverbiztonság ---- 12
14. Szoftverbiztonság ---- 12
15. Hozzáférési jogosultságok ---- 13
16. ---- 13
17. Vírusvédelem ---- 13
18. Hálózatbiztonság ---- 14
VII. FEJEZET ---- 14
REJTJELBIZTONSÁG ---- 14
VIII. FEJEZET ---- 15

ENGEDÉLYEZÉSI ELJÁRÁSOK ---- 15
19. Rendszerengedély kiadása ---- 15
19/A. Rejtjelző eszköz fejlesztése, gyártása ---- 16
20. Rejtjelző eszköz rendszeresítése ---- 16
21. Rejtjeltevékenység engedélyezése ---- 17
22. A TEMPEST követelmények érvényesítése ---- 18
IX. FEJEZET ---- 19
ELLENŐRZÉS ---- 19
23. A rejtjeltevékenység ellenőrzésével kapcsolatos szabályok ---- 19
X. FEJEZET ---- 19
ELEKTRONIKUS BIZTONSÁGI KÉPZÉS ---- 19
XI. FEJEZET ---- 20
BIZTONSÁGI DOKUMENTÁCIÓ, REJTJELSZABÁLYZAT ---- 20
24. Rejtjeltevékenységgel kapcsolatos biztonsági dokumentáció ---- 20
XII. FEJEZET ---- 20
ZÁRÓ RENDELKEZÉSEK ---- 20