A Kormány 161/2010. (V. 6.) Korm. Rendelete 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 meg valósítható,
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 meg valósító 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. ***rejtjel-hozzáférési engedély****:* az állami vagy közfeladat végrehajtása érdekében a rejtjeltevékenységgel összefüggő munkakörbe történő kinevezésre jogosult vezető által az előírt szintű nemzetbiztonsági ellenőrzés eredményeként kockázatmentességet igazoló biztonsági szakvélemény 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 köve tően 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,
21. ***TEMPEST követelmények****:* a „Bizalmas!” vagy magasabb minősítési szintű adat bizalmasságának védelme érdekében kialakított biztonsági intézkedések – amelyek kiterjednek az elektromos és adatkábelek vonalvezetésére, a rendszer környezetében alkalmazható berendezésekre, árnyékolástechnikai megoldásokra, valamint csökkentett kisugárzású eszközökre – együttese, amelyet a rendszer valamennyi eleme vezetett és elektromágneses kompromittáló kisugárzásának csökkentése érdekében alakítottak ki,
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.

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 meg valósítási lehetőségek adottak – rejtjelzéssel védett virtuális magánhálózat útján kell továbbítani.

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) ellátja az elektronikus biztonság tekintetében a nemzeti biztonsági hatóság feladatkörét a Magyar Köztársaság 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) együttműködik a Nemzeti Hálózatbiztonsági Központtal (a továbbiakban: NHBK), amelynek keretén belül

ia) ellátja az NHBK-tól kapott hálózatbiztonsági információk terjesztését a minősített adatot elektronikus rendszeren kezelő szervek felé,

ib) tájékoztatja az NHBK-t a minősített adatot elektronikus rendszeren kezelő szervektől kapott, az NHBK feladatkörébe tartozó információkról.

(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,

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) TEMPEST vizsgálatokat, méréseket végez vagy végeztet,

e) a TEMPEST mérések alapján határozatot ad ki az eszközök besorolására, valamint a rendszer környezetének zónabesorolására vonatkozóan,

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) A Magyar Köztársaság nemzetközi kötelezettségvállalásainak teljesítése érdekében

a) a honvédelemért felelős miniszter látja el a NATO, valamint NYEU Központi Rejtjel Elosztó Hatóság feladatait,

b) a külpolitikáért felelős miniszter látja el az EU Központi Rejtjel Elosztó Hatóság 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.

(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) kiadja a rejtjeltevékenységre vonatkozó rejtjel-hozzáférési engedélyeket.

(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.

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 elő írások 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) folyamatos kapcsolatot tart az NHBK-val a használt rendszerek hálózati biztonsága vonatkozásában,

h) kivizsgálja a rendszerbiztonsági eseményeket.

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 továb biak ban 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 elő írásait, 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 meg valósításában,

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 elő írásai az irányadóak az e fejezetben foglalt kiegészítésekkel.

17. §

A rendszerbiztonsági felügyelő nem lehet a 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.

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 elő írásai 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.

11. Rejtjeltevékenységgel kapcsolatos fizikai biztonsági követelmények

23. §

(1) Rejtjelző eszköz csak a rendszerengedélyben meghatározott módon telepíthető.

(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 rejtjelző 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 elő írásai 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 meg fele lően 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 meg fele lően módosítják.

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 meg felelően 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.

i. 28. § (1) A rendszer elemeit az adminisztratív zónából, valamint a biztonsági területről 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.

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

(4) 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.

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 aló 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 köve tően, 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 köve tően a rendszer szolgáltatásai, valamint a rendszeren tárolt minősített adatok elérhetőek legyenek.

(3) A felhasználók részére a rendszerhez történő hozzáférést a biztonsági konfigurálást köve tően 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.

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) A rendszeradminisztrátor a naplózási eseményeket tartalmazó adatokról a rendszer biztonsági dokumentációja szerinti időközönként biztonsági mentéseket készít, és azt a rendszer biztonsági dokumentációban meghatározott ideig megőrzi.

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) Jelszóval történő azonosítás esetén a jelszóházirendet az NBF hagyja jóvá.

(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. Biztonsági mentés, helyreállítás

38. §

(1) A minősített adatot elektronikus rendszeren kezelő szerv biztonsági mentésekkel biztosítja a rendszer és a rajta kezelt adatok rendelkezésre állását.

(2) A rendszer biztonsági dokumentációiban meghatározott időszakonként a minősített adatokról a minősített adatot elektronikus rendszeren kezelő szerv biztonsági másolatokat készít.

(3) A minősített adatot elektronikus rendszeren kezelő szerv a biztonsági másolatot a rendszeren kezelhető minősített adatok legmagasabb minősítési szintjének megfelelő biztonsági körülmények között, a rendszertől elkülönített módon tárolja.

17. Vírusvédelem

39. §

(1) A minősített adatot elektronikus rendszeren kezelő szerv a vírusok és más rosszindulatú szoftverek azonosítására és eltávolítására megfelelő védelmet 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.

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.

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 elő írásokat maradéktalanul betartották.

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

(4) Nemzeti minősített adat rejtjelzésére csak olyan rejtjelző eszköz alkalmazható, amelynek fejlesztője, illetve gyártója rendelkezik a minősített adat kezeléséhez szükséges, jogszabályban meghatározott személyi és tárgyi feltételekkel, és amely szerv 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.

(5) Nemzeti minősített adat rejtjelzésére külföldi eszköz csak akkor alkalmazható, amennyiben a (4) bekezdésben meghatározott rejtjelző eszköz nem áll rendelkezésre, vagy a katonai műszaki követelmények nem teszik lehetővé külön nemzeti és külföldi rejtjelző eszköz együttes alkalmazását katonai műveletekben.

42. §

(1) Külföldi minősített adat rejtjelzése esetén a vonatkozó nemzetközi és nemzeti elő írások az irányadóak a rejtjeltevékenységre vonatkozóan.

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

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

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

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

(6) A (3)–(5) 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) A rendszerengedély iránti kérelmet a minősített adatot elektronikus rendszeren kezelő szerv biztonsági vezetője írásban nyújtja be az NBF-nek.

(3) A rendszerengedély kiadására irányuló kérelemhez a minősített adatot elektronikus rendszeren kezelő szerv csatolja a rendszerre vonatkozó biztonsági dokumentációt.

(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.

44. §

(1) A biztonsági vezető vagy a rendszerbiztonsági felügyelet a „Bizalmas!” vagy magasabb minősítési szintű adatot kezelő

(1) rendszer biztonsági követelményeinek kialakításával kapcsolatban elő ze tes egyeztetést kezdeményezhet, valamint

(2) helyszínbejárást kérhet az NBF-től.

(3) A „Szigorúan titkos!” minősítési szintű adatot kezelő rendszer esetén az NBF a helyszínbejárási kérelem teljesítését

(4) nem tagadhatja meg.

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) A rejtjeltevékenységet folytató szerv a rendszeresítési engedély iránti kérelemben benyújtja:

a) a rejtjelző eszköz két működőképes példányát,

b) a rejtjelző eszköz tervezett rendeltetésére vonatkozó információkat, beleértve a rejtjelezhető minősített adat javasolt legmagasabb minősítési szintjét,

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

e) a rejtjelző eszköz gyártási és tesztelési dokumentációját,

f) a fejlesztő és gyártó nyilatkozatát a teljességről, megfelelőségről és azonosságról,

g) a rejtjelző eszköz rendeltetésszerű működtetéséhez szükséges biztonsági feltételrendszerre vonatkozó ajánlásokat.

(3) A nemzeti minősített adatok védelmére alkalmazott, a NATO, az EU vagy az EU valamely tagállama által engedélyezett rejtjelző eszközök esetében rejtjeltevékenységet folytató szerv – a (2) bekezdésben foglaltaktól eltérően – a rendszeresítési engedély iránti kérelemben

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) Az NBF a rejtjelző eszközre vonatkozó – (2) bekezdés szerinti – rendszeresítési engedély kiadása során a rejtjelző eszköz mechanikai felépítése és bontásvédelme értékelésében kikéri az Információs Hivatal szakértői véleményét.

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) Az NBF a rendszeresítési engedély mellékleteként kiadja a rejtjelző eszköz működtetési szabályzatát, kezelési utasítását és a rejtjelző eszköz alkalmazásához szükséges egyéb dokumentumokat. Az NBF a rendszeresítési engedély kiadásába szakértőként bevonja az Információs Hivatalt a nemzetbiztonsági szolgálatokról szóló tör vényben foglalt feladatai végrehajtása érdekében.

(4) Nemzeti minősített adat rejtjelzésére csak az NBF által kiadott rendszeresítési engedéllyel rendelkező rejtjelző eszköz alkalmazható.

(5) Az NBF kriptográfiai és bontásvédelmi szempontból, valamint a mechanikai felépítést érintően kikéri az Információs Hivatal szakértői véleményét a kifejlesztendő rejtjelző eszközre vonatkozóan.

21. Rejtjeltevékenység engedélyezése

47. §

(1) Amennyiben a rendszerengedély iránti kérelem rejtjeltevékenységgel kapcsolatos engedélyezést is magában foglal, a rendszerengedély iránti kérelem a következőket tartalmazza:

a) a rejtjelző eszköz nevét, típusát, verzióját és mennyiségét,

b) a rendszer elvi vázát, elemeit,

c) a rejtjelző eszköz tervezett telepítési helyének pontos meghatározását,

d) a rejtjelző eszköz használatával kapcsolatos szervezeti, személyi és adminisztratív feltételek teljesülésére vonatkozó adatokat, nyilatkozatokat,

e) a rejtjelző eszköz alkalmazásához előírt biztonsági feltételek meglétének igazolására szolgáló dokumentációt, a rejtjelzésre szolgáló helyiség alaprajzát, a helyiséget védő biztonsági rendszer leírását,

f) amennyiben a rejtjelző eszköz telepítéséhez külső segítséget kívánnak igénybe venni, a közreműködő természetes személyazonosító adatait.

(2) Telefon, mobil vagy tábori rejtjelző eszközök esetén az (1) bekezdésben meghatározottak közül csak az adott eszköz esetében értelmezhető adatokat szükséges megadni.

48. §

(1) Az NBF engedélye szükséges továbbá:

a) a rejtjelző eszköznek az ország területéről történő kiviteléhez, külföldi használatához,

b) a rejtjelző eszközzel kapcsolatos fejlesztési, gyártási tevékenységhez,

c) a rejtjelző eszközzel kapcsolatos karbantartó, javító tevékenységhez,

d) rejtjelző eszköz kiállításához vagy bemutatásához,

e) rejtjelző eszközhöz kötődő értékesítési, piackutató és reklámtevékenységhez.

(3) 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.

22. A TEMPEST követelmények érvényesítése

49. §

(1) „Bizalmas!” és magasabb minősítési szintű adatot kezelő rendszer védelme megfelel a TEMPEST követelményeknek.

(2) A TEMPEST követelmények kiterjednek a rendszer környezetében alkalmazható berendezésekre, elektromos árnyékolástechnikai megoldásokra, csökkentett kisugárzású hardver eszközök alkalmazására, az építészeti, épületgépészeti, épületvillamossági, valamint a rendszerhez tartozó vagy a rendszer környezetében található fém berendezések földelésére.

50. §

(1) A TEMPEST követelményeket kielégítő eszközök bevizsgálását az NBF végzi. A bevizsgálás alapján kiadott határozat tartalmazza:

a) az eszköz konkrét típusát,

b) az eszköz TEMPEST besorolását,

c) az eszköz üzemeltetésére vonatkozó biztonsági követelményeket.

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

51. §

(1) A „Bizalmas!” és magasabb minősítési szintű 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:

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 köve tően 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) A rejtjeltevékenységgel kapcsolatos belső ellenőrzésre a minősített adatot elektronikus rendszeren kezelő szerv vezetője, a biztonsági vezető, a rejtjelfelügyelet, a rejtjeltevékenységet végző szervezeti egység közvetlen 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

56. §

(1) Az NBF a rendszerbiztonsági felügyeletek részére rendszeres időközönként képzést tart az elektronikus biztonsággal kapcsolatban.

(2) A rendszerbiztonsági felügyelet vezetője, valamint az általa kijelölt személy a képzésen részt vesz.

57. §

(1) A rendszer felhasználói részére a képzést a rendszerbiztonsági felügyelet legalább kétévente megtartja.

(2) A képzés végén a felhasználók aláírásukkal igazolják a képzésen való részvételüket.

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 meg valósítása 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 elő ze tes egyetértése szükséges.

XII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

62. §

E rendelet a kihirdetését követő nyolcadik napon lép hatályba.

63. §

Ez a rendelet

a) az 1. § 7., 13., 14., 19., 21. és 22. pontjában, a 2–4. §-ban, a 9. §-ban, a 10. § c) pontjában, a 22. § (1)–(3) bekezdésében, a 25. § (2)–(4) bekezdésében, a 26. § (1) és (2) bekezdésében, a 27. § (1) és (2) bekezdésében, a 28. § (1) bekezdésében, a 31–33. §-ban, a 35. § (1) és (2) bekezdésében, a 39. § (1)–(3) bekezdésében, a 41. § (1) és (3) bekezdésében, a 42. § (1) és (6) bekezdésében, a 43. § (1), (3) és (4) bekezdésében, a 49. § (1) bekezdésében, az 57. § (1) és (2) bekezdésében a Tanács biztonsági szabályzatának elfogadásáról szóló 2001. március 19-i 264/2001/EK tanácsi határozat Melléklet XI. szakaszának,

b) az 1. § 7. pontjában, a 3–4. §-ban, a 8. § c) pontjában, a 22. § (3) bekezdésében, a 25. § (2)–(3) bekezdésében, a 26. § (1)–(2) bekezdésében, a 27. § (1)–(4) bekezdésében, a 32. § (1) bekezdésében, a 33. § (1)–(2) bekezdésében, a 41. §-ban, a 45. §-ban, a 49. §-ban, az 50–51. §-ban, az 56. § (1)–(2) bekezdésében, az 57. § (1)–(2) bekezdésében, az 59. § (1)–(2) bekezdésében – a 2001/844/EK, ESZAK, Euratom határozat módosításáról szóló, 2005. február 3-i 2005/94/EK, Euratom bizottsági határozattal és a 2001/844/EK, ESZAK, Euratom határozat módosításáról szóló, 2006. január 31-i 2006/70/EK,Euratom bizottsági határozattal módosított – az eljárási szabályzatának módosításáról szóló 2001. november 29-i 844//2001/EK, ESZAK, EURATOM bizottsági határozat 3. cikk b) pontjának, 8. cikkének, valamint a Melléklet 25.1.4., 25.1.5., 25.3.2., 25.3.7., 25.4.2., 25.5.3., 25.5.4., 25.5.5., 25.5.6., 25.6.1., 25.6.2., 25.6.3., 25.6.4. és 25.7.2. pontjainak

a végrehajtásához szükséges rendelkezéseket állapít meg.

64. §

(1) Hatályát veszti a rejtjeltevékenységről szóló 43/1994. (III. 29.) Korm. rendelet, valamint a rejtjeltevékenységről szóló 43/1994. (III. 29.) Korm. rendelet módosításáról szóló 220/2005. (X. 13.) Korm. rendelet.

(2) Ez a § hatályát veszti a rendelet hatályba lépését követő napon.

Bajnai Gordon s. k.,
Miniszterelnök

TARTALOMJEGYZÉK