179/2003. (XI. 5.) Korm. rendelet

a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól

Az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény módosításáról szóló 1998. évi LXXX. törvény 5. §-ában kapott felhatalmazás alapján a külföldi minősítéssel és jelöléssel ellátott adatok védelmének szabályairól a Kormány a következőket rendeli el:

I. Fejezet

ÁLTALÁNOS RENDELKEZÉSEK

1. § E rendelet hatálya az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény (a továbbiakban: Ttv.) 5/C. §-ában meghatározott magyar kibocsátóra, felhasználóra és címzettre, továbbá a Ttv. 5/B. §-ának (2)-(6) bekezdésében meghatározott külföldi minősítéssel és jelöléssel ellátott adat védelmére terjed ki. A Ttv. 5/B. § (7) bekezdésében meghatározott adatokra és az ilyen adatokat kezelő szervekre a rendelet hatálya akkor terjed ki, ha a nemzetközi szerződést kihirdető törvény biztonsági hatóságként a Nemzeti Biztonsági Felügyeletet (a továbbiakban: Felügyelet) jelöli ki.

Értelmező rendelkezések

2. § E rendelet alkalmazásában:

1. *Külföldi minősítéssel és jelöléssel ellátott adat:* nemzetközi kötelezettségvállalás alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült, a Ttv. 5/B. § (2)-(7) bekezdésében meghatározott külföldi minősítéssel és jelöléssel ellátott adat.
2. *NATO, illetve NYEU Központi Nyilvántartó:* a Honvédelmi Minisztérium a NATO, illetve NYEU minősített adatok országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége.
3. *EU Központi Nyilvántartó:* a Külügyminisztériumnak az EU minősített adatok országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége.
4. *Nyilvántartó:* a Felügyelet által a külföldi minősítéssel és jelöléssel ellátott adat kezelésére feljogosított szervezeti egység, amely felett a NATO, illetve NYEU, továbbá az EU Központi Nyilvántartó szakmai felügyeletet gyakorol.
5. *Ellenőrző pont:* a külföldi minősítéssel és jelöléssel ellátott adat kezelésére feljogosított szervezeti egység, amely felett a Nyilvántartó szakmai felügyeletet gyakorol.
6. *Illetékes biztonsági felügyelet:* a külföldi minősítéssel és jelöléssel ellátott adatot kezelő szervnél, a vonatkozó jogszabályokban előírt biztonsági feladatokat ellátó szervezeti egység vagy szervezetrendszer központi egysége. Az illetékes biztonsági felügyelet feladatait a szerv által kijelölt biztonsági megbízott is elláthatja.
7. *Biztonsági megbízott:* a külföldi minősítéssel és jelöléssel ellátott adat védelmével kapcsolatos biztonsági feladatok végrehajtására és koordinálására a titokbirtokos szerv vezetője által - a Felügyelet elnökének egyetértésével - kinevezett személy.
8. *Reagáló erők:* a fizikai biztonság érdekében elrendelt intézkedések végrehajtására kötelezett személyzet, így az őrök, a biztonsági rendszert működtető személyek.
9. *Elektronikus adatkezelés:* adat elektronikus, elektromagnetikus vagy optikai úton történő feldolgozása (készítése, megjelenítése, tárolása, módosítása, törlése), illetve továbbítása.
10. *Elektronikus biztonság:* a kommunikációs, informatikai és más elektronikus rendszerekben alkalmazott biztonsági intézkedések összessége, amelyek biztosítják az elektronikusan kezelt külföldi minősítéssel és jelöléssel ellátott adat bizalmasságát, sértetlenségét és rendelkezésre állását. Összetevői a számítógép- és hálózatbiztonság (hardver, szoftver és firmver biztonság), kommunikációs biztonság (rejtjel-, átvitel- és kompromittáló kisugárzás biztonság), valamint a személyi-, fizikai- és dokumentum biztonságnak a rendszerre vonatkozó különös szabályai.

11. *Rendszer:* külföldi minősítéssel és jelöléssel ellátott adat elektronikus kezelésére alkalmas berendezés - a rejtjelző eszköz kivételével -, módszer és eljárás együttese. A rendszer lehet nemzeti, NATO, NYEU, illetve EU és összekapcsolt.

12. *Nemzeti hatáskörű rendszer:* külföldi minősítéssel és jelöléssel ellátott adatok elektronikus kezelésére szolgáló, a tagállamok által létrehozott és elektronikus biztonsági felügyeleti szempontból nemzeti hatáskörbe tartozó rendszer.

13. *NATO, NYEU, illetve EU rendszer:* külföldi minősítéssel és jelöléssel ellátott adat elektronikus kezelésére szolgáló, a NATO, a NYEU, illetve az EU által létrehozott, de a tagállamok területén elektronikus biztonsági felügyeleti szempontból nemzeti hatáskörbe utalt rendszer.

14. *Összekapcsolt rendszer:* a nemzeti hatáskörű és a NATO, NYEU, illetve EU rendszerek - hatályos nemzetközi szerződés által engedélyezett - összekapcsolása révén létrejövő rendszer.

15. *Rendszer Biztonsági Utasítás:* a NATO, a NYEU, illetve az EU elektronikus biztonsági követelményeire, a tagállamok elektronikus biztonsági előírásaira, valamint a helyszíni kockázat értékelésére alapozva teljes és részletes leírását adja azon elektronikus biztonsági követelményeknek, amelyek betartása a rendszerre vonatkozóan kötelező.

16. *Üzemeltetés Biztonsági Szabályzat:* a rendszer egy meghatározott üzemeltetési helyén alkalmazott biztonsági előírások, a működtetés során követendő eljárások, valamint a rendszerrel kapcsolatban álló személyek és felelősségi köreik teljes körű leírása.

17. *Rendszerbiztonsági felelős:* a biztonsági megbízott felügyelete mellett a rendszer alkalmazási területén felelős a rendszer személyi, fizikai, dokumentum, hardver, szoftver biztonsági feltételek érvényesüléséért, a biztonsági beállítások és hozzáférési jogosultságok beállításáért.

18. *Rendszerüzemeltetési biztonsági felelős:* a rendszerbiztonsági felelős irányítása mellett a rendszer alkalmazási területén felelős a rendszer üzemeltetéséért, a hardver és szoftver konfiguráció folyamatos karbantartásáért.

19. *Életciklus:* a rendszer életciklusa 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.

20. *Veszélyeztetés:* ha fennáll annak a lehetősége, hogy a külföldi minősítéssel és jelöléssel ellátott adat részben vagy egészben illetéktelen személy részére hozzáférhetővé válik, vagy megsemmisül, továbbá veszélyeztetettnek tekintendő minden ideiglenesen eltűnt külföldi minősítéssel és jelöléssel ellátott adat beleértve az időszaki ellenőrzés során fel nem lelt iratokat is, mindaddig, amíg a vizsgálat mást nem állapít meg.

21. *Fenyegetés:* a biztonság véletlen vagy szándékos megsértésének lehetősége, az elektronikus biztonság három biztonsági célkitűzése, a bizalmasság, a sértetlenség és a rendelkezésre állás közül egy vagy több elem elvesztése.

3. § A biztonsági megbízott hatáskörében - amennyiben a titokbirtokos szerv vezetője másként nem rendelkezik - a Ttv. 2. §-a (1) bekezdésének 10. pontjában meghatározott titokvédelmi felügyelő jár el.

II. Fejezet

FIZIKAI BIZTONSÁGI ALAPELVEK ÉS KÖVETELMÉNYEK

4. § (1) Minden olyan helyiséget, épületet, építményt, ahol külföldi minősítéssel és jelöléssel ellátott adatot kezelnek, illetve tárolnak, fizikai biztonsági intézkedésekkel védeni kell illetéktelen személyek által az adatokhoz történő hozzáférés ellen.

(2) A fizikai biztonsági intézkedések bevezetése során figyelembe kell venni:

a) a kezelt vagy tárolt külföldi minősítéssel és jelöléssel ellátott adat minősítési szintjét,

b) a külföldi minősítéssel és jelöléssel ellátott adatok mennyiségét és megjelenési formáját,

c) a helyszín veszélyeztetettségi szintjét.

(3) A fizikai biztonsági rendszert több egymásra épülő elemből kell kialakítani. A fizikai biztonság külső elemeinek a védendő terület határait kell biztosítaniuk. A fizikai biztonság közbenső elemeinek észlelnie kell az illetéktelen behatolást, és riasztania kell a reagáló erőket. A belső fizikai biztonsági intézkedéseknek a reagáló erők megérkezéséig késleltetni kell a behatolókat a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő hozzáférésben.

(4) A fizikai biztonsági rendszerben csak garantált minőségű technikai elemek használhatók. Ennek igazolására a Felügyelet külön vizsgálat nélkül elfogadja a Magyar Biztosítók Szövetsége (a továbbiakban: MABISZ) által kiállított Biztosítói Minősítési Tanúsítványt vagy a nemzetközi gyakorlatban azzal egyenértékű okiratot (a továbbiakban együtt: Tanúsítvány).

5. § (1) A 4. § (1) bekezdésben foglaltak alapján I., illetve II. osztályú biztonsági területet (a továbbiakban együtt: biztonsági terület), szükség esetén adminisztratív zónát kell kialakítani minden szervnél, ahol külföldi minősítéssel és jelöléssel ellátott adatot kívánnak kezelni, illetve tárolni.

(2) I. osztályú biztonsági területnek minősül, ahol "Bizalmas!" vagy annál magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatot dolgoznak fel vagy tárolnak olyan módon, hogy a területre való belépés egyben a külföldi minősítéssel és jelöléssel ellátott adatokhoz való hozzáférést is jelenti. A terület fizikailag körülhatárolt és védett, valamint a ki- és belépés ellenőrzött. A belépés csak beléptető rendszeren keresztül azon személyek számára engedélyezhető, akik erre külön felhatalmazással és személyi biztonsági tanúsítvánnyal rendelkeznek.

(3) II. osztályú biztonsági területnek minősül, ahol "Bizalmas!" vagy annál magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatot dolgoznak fel vagy tárolnak olyan módon, hogy a illetéktelen hozzáférést belső intézkedésekkel meg lehet akadályozni. A terület fizikailag körülhatárolt és védett, valamint a ki- és belépés ellenőrzött. A belépés csak beléptető rendszeren keresztül azon személyek számára engedélyezhető, akik erre külön felhatalmazással és személyi biztonsági tanúsítvánnyal rendelkeznek. A külföldi minősítéssel és jelöléssel ellátott adatokhoz történő illetéktelen hozzáférés megakadályozása érdekében más személy csak kísérettel, vagy ezzel egyenértékű ellenőrzés mellett léphet be a területre.

(4) Adminisztratív zónának minősül a terület, ahol a belépés ellenőrzött. Szükség esetén adminisztratív zónát lehet kiépíteni az I., illetve a II. osztályú biztonsági területek körül.

(5) "Korlátozott terjesztésű!" külföldi minősítéssel és jelöléssel ellátott adatok I., illetve II. osztályú biztonsági területen kívül adminisztratív zónában is feldolgozhatóak és az adminisztratív zónán belül zárható irodabútorban tárolhatók. "Bizalmas!" és ennél magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatok I., illetve II. osztályú biztonsági területen tárolhatóak, illetve dolgozhatóak fel.

(6) NATO, illetve NYEU és EU minősítéssel és jelöléssel ellátott adatok tárolhatóak egy biztonsági területen, azonban dokumentum biztonsági szempontból elkülönítésüket biztosítani kell.

Egyedi fizikai biztonsági intézkedések

6. § (1) A "Szigorúan titkos!", "Titkos!", "Bizalmas!" külföldi minősítéssel és jelöléssel ellátott adatok esetén a 19-20. §-ban vagy a 21-22. §-ban meghatározott, ezen kívül a 23-24. §-ban és a 26-27. §-ban foglalt biztonsági intézkedések alkalmazása kötelező. A "Korlátozott terjesztésű!" külföldi minősítéssel és jelöléssel ellátott adatok esetén a 19-20. §-ban vagy a 21-22. §-ban meghatározott, ezen kívül a 23. §-ban foglalt biztonsági intézkedések alkalmazása kötelező.

(2) Az (1) bekezdésben kötelezően előírt biztonsági intézkedéseken túlmenően a fejezetben meghatározott egyéb biztonsági intézkedések is alkalmazhatóak.

Épület, objektumhatároló falak és kerítések

7. § A biztonsági területet magába foglaló épület, objektumhatároló falak és kerítések fizikai akadályt képeznek, és meghatározzák a védelem alá eső terület külső határait. Az általuk nyújtott védelem szintje függ magasságuktól, szerkezetüktől, a felhasznált anyagoktól, és bármely, a védelem növelésére szolgáló további biztonsági elemtől (pl. a megvilágítástól vagy a zárt láncú kamerarendszertől). A belépési pontokat az épület, objektumhatároló falak és kerítések által nyújtott védelemmel egyező biztonsági intézkedésekkel kell ellátni.

Biztonsági megvilágítás

8. § A biztonsági világítást elsősorban az épület, objektumhatároló falak és kerítések védelmét megerősítő, zárt láncú kamerarendszer működtetésének támogatására célszerű alkalmazni.

Zárt láncú kamerarendszer

9. § A zárt láncú kamerarendszer az őrség munkáját segíti, elsősorban a riasztások ellenőrzésében. Telepíthető az épület, objektumhatároló falak és kerítések, épületet övező területek vagy folyosók megfigyelésére.

Behatolásjelző rendszer

10. § Behatolásjelző rendszert az I. vagy II. osztályú biztonsági területen célszerű alkalmazni. A kiépítés során figyelembe kell venni, hogy a reagáló erőknek a riasztást követően még az előtt a területre kell érnie, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő hozzáférés megtörténne. Behatolásjelző rendszerek telepíthetőek az épület, objektumhatároló falak és kerítések biztonságának a növelésére, amelyet hamis riasztások kiszűrése érdekében célszerű kombináltan használni zárt láncú kamerarendszerrel.

A belépés ellenőrzése

11. § Az I., illetve a II. osztályú biztonsági területre történő belépés csak technikai úton vagy az őrség által megvalósított beléptető rendszeren keresztül történhet. A belépések ellenőrzése történhet az épületek bejáratainál, folyosóknál vagy irodáknál is.

Őrség és reagáló erők

12. § (1) Az őrök feladatait, valamint az őrjáratok szükségességét és gyakoriságát a további biztonsági eszközök meglétének figyelembevételével kell meghatározni.

(2) Az őrség számára írásban kell meghatározni a külföldi minősítéssel és jelöléssel ellátott adatok védelmével kapcsolatos feladatokat.

(3) Az őrségnek vagy a legalább két főből álló reagáló erőnek a külföldi minősítéssel és jelöléssel ellátott adat veszélyeztetettségének jelzésekor - a telepített fizikai biztonsági rendszerre figyelemmel - úgy kell a jelzés helyére érnie, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz illetéktelen hozzáférést megakadályozhassa.

(4) Munkaidő után a külföldi minősítéssel és jelöléssel ellátott adatok tárolási helyét az őrség lehetőség szerint járőrözéssel biztosítja, a biztonsági igényekhez igazított rendszerességgel.

(5) Azokon a biztonsági területeken, ahol nincsen 24 órás folyamatos őrzés, illetve felügyelet, munkaidő befejezése után belső ellenőrzéssel kell biztosítani a külföldi minősítéssel és jelöléssel ellátott adatok biztonságba helyezését.

Látogatók ellenőrzése

13. § A látogatók ellenőrzése során figyelembe kell venni, hogy rendelkeznek-e személyi biztonsági tanúsítvánnyal és engedéllyel, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz hozzáférjenek. Amennyiben ezekkel a látogatók nem rendelkeznek, az ellenőrzésük történhet folyamatos kísérettel, vagy egyéb ezzel egyenértékű megoldással. Azoknak a látogatóknak, akik önállóan mozoghatnak a biztonsági területeken, azonosító kártyát kell viselniük.

A külföldi minősítéssel és jelöléssel ellátott adatok tárolásának minimális szabályai

14. § "Szigorúan titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok I. vagy II. osztályú biztonsági területen biztonsági tárolóban és az alábbi intézkedések közül egy vagy több alkalmazása mellett tárolhatóak:

a) folyamatos védelem biztosítása személyi biztonsági tanúsítvánnyal rendelkező őrök, vagy más erre felhatalmazott személyek által;

b) a biztonsági tároló legalább kétóránkénti ellenőrzésének biztosítása személyi biztonsági tanúsítvánnyal rendelkező őrök, vagy más erre felhatalmazott személyek által;

c) behatolásjelző rendszer telepítése oly módon, hogy a reagáló erők még az előtt a riasztás helyére érkezzenek, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő illetéktelen hozzáférés megtörténne;

d) behatolásjelző rendszerrel ellátott biztonsági tároló telepítése oly módon, hogy a reagáló erők még az előtt a riasztás helyére érkezzenek, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő illetéktelen hozzáférés megtörténne;

e) a 18. §-ban meghatározott nyílt tárolási lehetőség esetén behatolásjelző rendszer telepítése oly módon, hogy a reagáló erők még az előtt a riasztás helyére érkezzenek, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő illetéktelen hozzáférés megtörténne.

15. § "Titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok I. vagy II. osztályú biztonsági területen az alábbi intézkedések közül egy vagy több alkalmazása mellett tárolhatóak:

a) a 14. §-ban meghatározott intézkedések közül bármelyik alkalmazása;

b) biztonsági tárolóban történő tárolás a 14. § *b), d)* pontjában előírt kiegészítő ellenőrzés nélkül;

c) a 18. §-ban meghatározott nyílt tárolási lehetőség esetén az alábbi kiegészítő intézkedések valamelyikének alkalmazása mellett:

ca) a helyszín folyamatos őrzése személyi biztonsági tanúsítvánnyal rendelkező őrök, vagy más erre felhatalmazott személyek által,

cb) nyílt tároló helyiség 4 óránkénti ellenőrzése személyi biztonsági tanúsítvánnyal rendelkező őrök, vagy más erre felhatalmazott személyek által,

cc) behatolás jelző rendszer telepítése, oly módon, hogy a reagáló erők még az előtt a riasztás helyére érkezzenek, mielőtt a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő illetéktelen hozzáférés megtörténne.

16. § (1) "Bizalmas!" minősítéssel és jelöléssel ellátott adatok a 14-15. §-okban meghatározottak szerint tárolhatóak azzal a kivétellel, hogy kiegészítő ellenőrzés nem szükséges.

(2) "Korlátozott terjesztésű" minősítéssel és jelöléssel ellátott adatok adminisztratív zónában zárható irodabútorban tárolhatóak.

Kulcsok és zárkombinációk

17. § (1) A biztonsági tárolóeszközök kulcsait az épületből kivinni nem lehet. Ezek tartalékpéldányát és a kódokat a biztonsági megbízott őrzi a - a tárolt adatok minősítési szintjének megfelelő - tárolóeszközben. A kulcsok és - szükség esetén - a számkombinációt tartalmazó boríték felvétele, illetve leadása dokumentált módon, az erre a célra felfektetett nyilvántartásban történhet.

(2) Minden tartalék kulcsot, számkombinációt külön borítékba kell elhelyezni.

(3) A számkombinációt meg kell változtatni

a) a berendezés használójának változásakor,

b) használatbavételkor és javítás után,

c) a számkombináció felfedése (illetéktelen tudomásra jutása) vagy annak veszélye esetén,

d) de legalább minden hat hónap elteltével.

Nyílt tárolási lehetőség

18. § (1) Ahol nyílt tárolási lehetőséget alkalmaznak a helyiség falazatának, födémének és padozatának meg kell felelnie a 30 cm vastagságú falazóblokk szilárdsági mutatójának.

(2) A helyiség ajtajának Tanúsítvánnyal rendelkező, "Bizalmas!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén minimum 5 perces, "Titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén minimum 10 perces, "Szigorúan titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén minimum 15 perces áthatolási, áttörési ellenállásra képes biztonsági ajtónak kell lennie. A biztonsági ajtót minden esetben nyitásérzékelővel kell ellátni.

(3) A helyiségbe mozgásérzékelőt és füstérzékelőt kell felszerelni. Csak olyan elektronikai jelzőrendszer telepíthető, melynek alkotóelemei Tanúsítvánnyal rendelkeznek.

(4) Amennyiben a helyiség falazatán ablakok, nyílások, áttörések találhatóak, azokat az alábbi méretű fix, illetve nyitható belső ráccsal kell ellátni:

a) "Bizalmas!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén 140 x 140 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján körbehegesztett rácsszerkezet;

b) "Titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén 90 x 90 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján körbehegesztett rácsszerkezet;

c) "Szigorúan titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén 70 x 70 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján körbehegesztett rácsszerkezet.

(5) Nyitható rácsszerkezet esetén mechanikus számkombinációs zárat és nyitásérzékelőt kell felszerelni.

AZ EGYEDI FIZIKAI BIZTONSÁGI INTÉZKEDÉSEK BESOROLÁSA

Biztonsági tárolók és zárak

19. § (1) 4. osztályú tároló Tanúsítványa szerint "E" vagy azzal egyenértékű fokozatba sorolt biztonsági tároló.

(2) 3. osztályú tároló Tanúsítványa szerint "C" vagy azzal egyenértékű fokozatba sorolt biztonsági tároló.
(3) 2. osztályú tároló Tanúsítványa szerint "A" vagy azzal egyenértékű fokozatba sorolt biztonsági tároló.
(4) 1. osztályú tároló zárható irodabútor, amely korlátozott mechanikai védelemmel rendelkezik.

Biztonsági tárolókhoz tartozó zárak

20. § (1) 4. osztályú zár Tanúsítványa szerint "E" vagy azzal egyenértékű fokozatba sorolt biztonsági tárolóhoz rendszeresített zár.
(2) 3. osztályú zár Tanúsítványa szerint "C" vagy azzal egyenértékű fokozatba sorolt biztonsági tárolóhoz rendszeresített zár.
(3) 2. osztályú zár Tanúsítványa szerint "A" vagy azzal egyenértékű fokozatba sorolt biztonsági tárolóhoz rendszeresített zár.
(4) 1. osztályú zár bármilyen hagyományos zár.

Helyiségek és zárak

21. § (1) 4. osztályú helyiség falazata, födéme és padozata nagyfokú mechanikai ellenállásra képes. Amennyiben ablakai vannak a falazattal azonos szintű ellenállásra képesek. Tanúsítványa alapján ajtaja 15 perces áthatolási, áttörési ellenállásra képes biztonsági ajtó.
(2) 3. osztályú helyiség falazata, födéme és padozata nagyfokú mechanikai ellenállásra képes. Amennyiben ablakai vannak a falazattal azonos szintű ellenállásra képesek. Tanúsítványa alapján ajtaja 10 perces áthatolási, áttörési ellenállásra képes biztonsági ajtó.
(3) 2. osztályú helyiség falazata, födéme és padozata nagyfokú mechanikai ellenállásra képes. Amennyiben ablakai vannak a falazattal azonos szintű ellenállásra képesek. Tanúsítványa alapján ajtaja 5 perces áthatolási, áttörési ellenállásra képes biztonsági ajtó.
(4) 1. osztályú helyiség hagyományos zárható ajtóval rendelkezik. Falazata, födéme és padozata korlátozott mechanikai ellenállásra képes.

Helyiségekhez tartozó zárak

22. § (1) 4. osztályú zár Tanúsítványa alapján 15 perces áthatolási, áttörési ellenállásra képes biztonsági ajtóhoz rendszeresített zár.
(2) 3. osztályú zár Tanúsítványa alapján 10 perces áthatolási, áttörési ellenállásra képes biztonsági ajtóhoz rendszeresített zár.
(3) 2. osztályú zár Tanúsítványa alapján 5 perces áthatolási, áttörési ellenállásra képes biztonsági ajtóhoz rendszeresített zár.
(4) 1. osztályú zár bármilyen hagyományos zár lehet.

Épületek

23. § (1) 4. osztályú épület falazata, födéme és padozata nagyfokú mechanikai ellenállásra képes. Ajtaja és ablakai (ha vannak) a falazattal egyenértékű ellenállást biztosítanak.
(2) 3. osztályú épület falazata, födéme és padozata jelentős mechanikai ellenállásra képes. Ajtaja és ablakai (ha vannak) a falazattal egyenértékű ellenállást biztosítanak.
(3) 2. osztályú épület falazata lehet könnyűszerkezetes is, de mechanikai ellenállásra kell képesnek lennie hagyományos kézi szerszámok igénybevétele esetén. Ajtaja és ablakai (ha vannak) a falazattal egyenértékű ellenállást biztosítanak.
(4) 1. osztályú épület könnyűszerkezetes elemekből készült, mechanikai ellenállásra korlátozottan képes.

Beléptető rendszer

24. § (1) 4. osztályú beléptető rendszer teljesen automatikus, elektronikus kártyával vagy más ezzel egyenértékű eszközzel és PIN kód vagy biometrikus azonosító használatával működik. Mechanikus sorompóval rendelkezik, mely egyszerre egy személy áthaladását teszi lehetővé.

(2) 3. osztályú beléptető rendszer elektronikus kártyával vagy más ezzel egyenértékű eszközzel vagy PIN kód használatával működik. Az áthaladás fizikai sorompó vagy őrség által ellenőrzött.

(3) 2. osztályú beléptető rendszer őrség, illetve recepciósok alkalmazása által valósul meg. A belépés igazolvány felmutatása mellett történhet.

(4) 1. osztályú beléptető rendszer egyszerű, zárható ajtó. Az arra jogosultak belépése kulcs használatával, vagy más mechanikus megoldás alkalmazásával történhet.

Látogatók ellenőrzése

25. § A személyi biztonsági tanúsítvány megléte és a belépés engedélyezése meghatározza, hogy a látogatók kísérettel vagy kíséret nélkül léphetnek be a biztonsági területre.

Őrség és a behatolás jelző rendszerek

26. § (1) 5. osztályú őrség legalább kétóránként rendszeresen járőrözik, esetileg meghatározott útvonalon. Személyi biztonsági tanúsítvánnyal rendelkeznek.

(2) 4. osztályú őrség legalább hatóránként rendszeresen járőrözik, esetileg meghatározott útvonalon. Munkaidőn túl 2-3 alkalommal biztonsági ellenőrzést tartanak. Személyi biztonsági tanúsítvánnyal rendelkeznek.

(3) 3. osztályú őrség csak a biztonsági területen kívül járőrözik. Az őrök a biztonsági területre nem léphetnek be. A járőrözés gyakoriságát a helyi környezet biztonsága határozza meg. Személyi biztonsági tanúsítvánnyal nem rendelkeznek.

(4) 2. osztályú őrség az épületen belül, ügyeleti helyiségben a biztonsági rendszer felügyeletét látja el. A járőrözés nem kötelezettségük. Riasztás esetén, annak eredetét meg kell vizsgálniuk, szükség esetén a kijelölt reagáló erőket, vagy az arra illetékest értesítik. Személyi biztonsági tanúsítvánnyal nem rendelkeznek.

(5) 1. osztályú őrség kizárólag munkaidőn túl, az épület külső részén hajtanak végre járőrözést. A biztonsági területre nem léphetnek be, riasztás esetén az arra illetékest értesítik. Személyi biztonsági tanúsítvánnyal nem rendelkeznek.

Behatolás jelző rendszer

27. § (1) 4. osztályú behatolás jelző rendszer Tanúsítványa alapján, elemei a teljes körű elektronikai jelzőrendszer alkotóelemeként alkalmasak a védelem kialakítására.

(2) 3. osztályú behatolás jelző rendszer Tanúsítványa alapján, elemei a teljes körű elektronikai jelzőrendszer alkotóelemeként alkalmasak a védelem kialakítására. A behatolás jelző rendszert egyéb fizikai biztonsági intézkedésekkel kell kiegészíteni.

(3) 2. osztályú behatolás jelző rendszer elemei Tanúsítványa alapján a részleges elektronikai jelzőrendszer alkotóelemeként alkalmasak a védelem kialakítására. Olyan helyeken alkalmazható, ahol a behatolás valószínűsége csekély.

(4) 1. osztályú behatolásjelző rendszer elemei Tanúsítványa alapján a részleges elektronikai jelzőrendszer alkotóelemeként alkalmasak a védelem kialakítására. A riasztás a helyszínen - a környezetet riasztva - történik.

Kerítések

28. § (1) 4. osztályú kerítés nagyfokú védelmet nyújt nagyszámú, speciális eszközökkel felszerelt behatolóval szemben. Behatolásjelző rendszerrel van kiegészítve.

(2) 3. osztályú kerítés védelmet nyújt átlagos eszközökkel felszerelt behatolóval szemben.

(3) 2. osztályú kerítés védelmet nyújt a helyszínen található eszközökkel felszerelt behatolóval szemben.

(4) 1. osztályú kerítés célja, hogy jelölje a védett terület határait. Nincs felszerelve külön fizikai védelemmel.

(5) A kerítések védelmének növelésére alkalmazható behatolásjelző rendszer. Ezeket a hamis riasztások kiszűrése érdekében célszerű zárt láncú kamerarendszerrel és biztonsági világítással együttesen alkalmazni.

29. § (1) Az I., illetve a II. osztályú biztonsági terület alkalmas külföldi minősítéssel és jelöléssel ellátott adatok tárolására, illetve feldolgozására, amennyiben az 1. számú mellékletben meghatározott pontszámot eléri és a külföldi minősítéssel és jelöléssel ellátott adatok kezelésére a Felügyelet a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól szóló 180/2003.

(XI. 5.) Korm. rendeletben (a továbbiakban: R.) meghatározott Engedélyt megadta. Az *1. számú mellékletben* meghatározott pontszámoktól eltérni kizárólag pozitív irányban, a fizikai biztonság növelésével lehet.

(2) Az (1) bekezdésben említett pontszámot a *2. számú mellékletben* meghatározott táblázat alapján kell kiszámolni.

III. Fejezet

DOKUMENTUM BIZTONSÁG

A külföldi minősítéssel és jelöléssel ellátott adatok nyilvántartására kijelölt szervezeti egység

30. § (1) A minősített adatkezelő helyekre érkezett, valamint az ott készített külföldi minősítéssel és jelöléssel ellátott adatokat nyilvántartásba kell venni. A Nyilvántartóknak, illetve az Ellenőrző pontoknak a feladat- és hatáskörükbe tartozó külföldi minősítéssel és jelöléssel ellátott adatok hollétéről számot kell adniuk.

(2) A NATO, illetve NYEU Központi Nyilvántartó és az EU Központi Nyilvántartó, a Felügyelet tájékoztatása alapján jegyzéket vezetnek a hatáskörükbe tartozó külföldi minősítéssel és jelöléssel ellátott adatokat kezelő szerveknél működő Nyilvántartókról és Ellenőrző pontokról. A Nyilvántartók jelentései alapján összesített nyilvántartást vezetnek valamennyi, a Magyar Köztársaság mint tagállam részére megküldött, vagy ott készített "Szigorúan titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatról.

(3) A NATO, illetve NYEU Központi Nyilvántartó és az EU Központi Nyilvántartó egy időben Nyilvántartóként is működhet.

A Nyilvántartó és az Ellenőrző pont

31. § (1) A Nyilvántartó felelős azon külföldi minősítéssel és jelöléssel ellátott adat kezeléséért, mely adatkezelési szempontból a felügyelete alá tartozó szervnél keletkezik, illetve ide érkezik.

(2) A Nyilvántartót üzemeltető szervezeti egység létrehozhat Ellenőrző pontot, amelynek jogai és kötelezettségei megegyeznek a felügyeletét ellátó Nyilvántartóéval.

(3) A Ttv. 3. §-a (1) bekezdésének, valamint a 4. §-a (1) bekezdésének hatálya alá tartozó minősített adatok kezelő személyzete kezelheti a külföldi minősítéssel és jelöléssel ellátott adatokat is, amennyiben a megfelelő szintű Személyi Biztonsági Tanúsítvánnyal rendelkezik, továbbá külön jogszabályban meghatározott oktatáson részt vett, és erre a feladatra a titokbirtokos szerv vezetője kijelölte.

A külföldi minősítéssel és jelöléssel ellátott adat megismerése

32. § (1) A külföldi minősítéssel és jelöléssel ellátott adat megismerését a titokbirtokos jogosult engedélyezni a betekintési engedély megadásával.

(2) A betekintési jogosultság megadása előtt meg kell győződni arról, hogy a személy rendelkezik-e a megfelelő szintű nemzetbiztonsági ellenőrzés alapján kiadott személyi biztonsági tanúsítvánnyal, és a hozzáférés állami vagy közfeladat végrehajtása érdekében szükséges.

(3) Külföldi minősítéssel és jelöléssel ellátott adathoz történő hozzáférés engedélyezésekor az érintett személynek titoktartási nyilatkozatot kell aláírnia.

(4) A külföldi minősítéssel és jelöléssel ellátott adatokat csak olyan személyek kezelhetik, készíthetik, fordíthatják, sokszorosíthatják, másolhatják vagy semmisíthetik meg, akik legalább ugyanolyan szintű külföldi minősítéssel és jelöléssel ellátott adatba való betekintési joggal rendelkeznek.

A biztonsági megbízott feladatai

33. § A biztonsági megbízott a titokbirtokos szerv vezetőjének átruházott hatáskörében eljárva utasítási joggal gyakorolja az őt megbízó vezető titokvédelmi jogosítványait, ellátja az e rendeletben meghatározott szabályok alkalmazásának felügyeletét. Ennek keretében gondoskodik a külföldi minősítéssel és jelöléssel ellátott adat védelmére meghatározott feladatok végrehajtásáról, így:

a) gondoskodik a külföldi minősítéssel és jelöléssel ellátott adat védelmére vonatkozó jogszabályok végrehajtásáról, a külföldi minősítéssel és jelöléssel ellátott adatok személyi, fizikai, dokumentum és elektronikus biztonságának kiépítéséről és működtetéséről;

b) gondoskodik a Biztonsági Szabályzat és az Intézkedési Terv elkészítéséről és naprakész állapotban tartásáról;

c) felelős azért, hogy akinek a feladata ellátásához ez szükséges, betekintési engedéllyel rendelkezzen, és a külföldi minősítéssel és jelöléssel ellátott adat védelmére vonatkozó szabályokat megismerje;

d) gondoskodik a külföldi minősítéssel és jelöléssel ellátott adat nyomon követhetőségét biztosító rendszer kiépítéséről;

e) gondoskodik a betekintők névjegyzékének összeállításáról, naprakész állapotban tartásáról;

f) gondoskodik a titokvédelmi jogszabályok megismeréséről szóló titoktartási nyilatkozatok őrzéséről;

g) évente jegyzőkönyv felvétele mellett gondoskodik a titokvédelmi rendelkezések megtartásának ellenőrzéséről;

h) gondoskodik a megfelelő kódok, számkombinációk cseréjéről;

i) évente február 28-áig tájékoztatja a NATO, illetve NYEU, továbbá az EU Központi Nyilvántartót a lefolytatott belső ellenőrzés eredményéről.

A titkos ügykezelő feladatai

34. § A titkos ügykezelő feladata:

a) a készült vagy más titokbirtokostól érkezett külföldi minősítéssel és jelöléssel ellátott adat átvétele, nyilvántartása, megfelelő tárolása, selejtezése;

b) a külföldi minősítéssel és jelöléssel ellátott adat kiadása és visszavétele;

c) a betekintési jogosultság megszűnése esetén a külföldi minősítéssel és jelöléssel ellátott adat visszavétele;

d) a külföldi minősítéssel és jelöléssel ellátott adat felhasználásával és kezelésével kapcsolatos betekintési engedélyek nyilvántartása, a külföldi minősítéssel és jelöléssel ellátott adat nyilvántartására szolgáló segédletek hitelesítése, nyilvántartásba vétele;

e) a külföldi minősítéssel és jelöléssel ellátott adat belföldre, illetve külföldre történő továbbításához szükséges feladatok végrehajtása.

Eljárás a titkos ügykezelő megbízásának megszűnése esetén

35. § (1) A titkos ügykezelő megbízásának megszűnése esetén a birtokában lévő, megőrzésére rendelt külföldi minősítéssel és jelöléssel ellátott adatokat, valamint a tárolására szolgáló eszközök kulcsait, kódszámait, a rendszeresített nyilvántartási segédleteket, bélyegzőket a helyettese, távollétében a biztonsági megbízott vagy az erre kijelölt személy részére jegyzőkönyvvel átadja.

(2) Az (1) bekezdésben foglaltak végrehajtása során az átvételre kijelölt személynek meg kell győződnie arról, hogy a külföldi minősítéssel és jelöléssel ellátott adatok kezelésére szolgáló segédletek, kulcsok, kódszámok hiánytalanul megvannak. A kezelt külföldi minősítéssel és jelöléssel ellátott adatok meglétét tételesen - jegyzőkönyv felvétele mellett - ellenőrizni kell.

A külföldi minősítéssel és jelöléssel ellátott adat kezeléséhez szükséges nyilvántartási segédletek

36. § (1) A főnyilvántartó könyvbe kell beiktatni a Nyilvántartónál, illetve az Ellenőrző pontnál használt valamennyi iktatási segédletet.

(2) Az iktatási segédletek borítóján fel kell tüntetni a főnyilvántartó könyvből kapott sorszámot.

(3) A főnyilvántartó könyv és az iktatási segédletek nem selejtezhetőek.

A külföldi minősítéssel és jelöléssel ellátott adat átvétele

37. § (1) Más szervtől érkezett külföldi minősítéssel és jelöléssel ellátott adatot a címzett, illetve a titkos ügykezelő vehet át.

(2) A külföldi minősítéssel és jelöléssel ellátott adatot átvevő személy az alábbiakat köteles ellenőrizni:

a) a címzés alapján jogosult-e a külföldi minősítéssel és jelöléssel ellátott adat átvételére;

b) az átadási okmányon szereplő nyilvántartási szám és a külföldi minősítéssel és jelöléssel ellátott adatot tartalmazó zárt küldemény csomagolásán szereplő nyilvántartási szám megegyezik-e;

c) ha a küldemény nem "sk. felbontásra" jelzéssel érkezett, a külföldi minősítéssel és jelöléssel ellátott adat terjedelmét és mellékleteinek számát;

d) a zártan érkezett küldemény csomagolásának sértetlenségét.

(3) Az átvevő az átadási okmányon nevének, beosztásának és az átvétel idejének feltüntetése mellett aláírásával, valamint bélyegzőlenyomattal igazolja a küldemény átvételét.

(4) Téves címzés vagy helytelen kézbesítés esetén a küldeményt - két példányban készült jegyzőkönyv felvétele mellett - a jegyzőkönyv 1. számú példányával együtt azonnal vissza kell juttatni a feladónak.

(5) Ha a küldemény csomagolása sérült, a külföldi minősítéssel és jelöléssel ellátott adatot átadó jelenlétében az átvevő a küldeményt felbontja és ellenőrzi a küldemény tartalmát. Az intézkedésről két példányban jegyzőkönyvet kell felvenni. A jegyzőkönyvet az átadó, illetve az átvevő is aláírja. A jegyzőkönyv 1. számú példányát - aláírás ellenében - az átadónak át kell adni, aki intézkedik a sérülés körülményeinek tisztázására. A sérülés tényét az átadási okmányon szerepeltetni kell.

(6) Ha a küldeményt az átvevő tévedésből bontja fel, akkor erről két példányban jegyzőkönyvet készít. A küldeményt szabályszerűen lezárja és a jegyzőkönyv 1. számú példányával együtt a címzettnek továbbítja.

A külföldi minősítéssel és jelöléssel ellátott adatot tartalmazó küldemények felbontása

38. § (1) A küldemény felbontása előtt a címzett, illetve a titkos ügykezelő a küldemény sértetlenségéről köteles meggyőződni. A küldemény felbontásakor ellenőrizni kell a külföldi minősítéssel és jelöléssel ellátott adat hiánytalan meglétét a csomagoláson feltüntetett adatokkal, illetve az iratkezelési záradékban található adatokkal.

(2) A titkos ügykezelő bontja fel a más szervtől érkezett külföldi minősítéssel és jelöléssel ellátott adatokat tartalmazó küldeményeket, kivéve azokat, amelyeken az "sk. felbontásra" jelzés szerepel. Ez esetben zárt küldeményként veszi nyilvántartásba a külföldi minősítéssel és jelöléssel ellátott adatot az iktatókönyv megfelelő rovatainak kitöltésével. A küldemény átadásánál fel kell tüntetni, hogy az adatot "sk. felbontásra" jelzés miatt felbontás nélkül adták át. Amennyiben a külföldi minősítéssel és jelöléssel ellátott adatot a titkos ügykezelő nem ismerheti meg, a felbontásra jogosult személy a feldolgozást követően az iratot újra hitelesen lezárva a titkos ügykezelőnek dokumentált módon átadja őrzés, illetve tárolás céljából.

(3) Az "sk. felbontásra" jelzéssel ellátott küldemények esetén a felbontásra jogosult köteles a titkos ügykezelővel közölni az adat nyilvántartásba vételéhez szükséges valamennyi adatot.

(4) A külföldi minősítéssel és jelöléssel ellátott adat hiánya esetén két példányban jegyzőkönyvet kell felvenni. A jegyzőkönyv 1. számú példányát a küldő szervnek kell eljuttatni, és soron kívül tisztázni kell a hiány okát.

A külföldi minősítéssel és jelöléssel ellátott adat nyilvántartásba vétele

39. § (1) A külföldi minősítéssel és jelöléssel ellátott adatok iktatása - lehetőség szerint alszámos iktatási rendszerben - manuálisan vagy számítástechnikai eszközön történhet.

(2) Az alszámos iktatási rendszer alkalmazása esetén minden önálló ügyben keletkezett első adat 1-től növekvő főszámot kap az iktatókönyvben. A titkos ügykezelő az azonos tárgyban, egy ügyben keletkezett újabb adatot az illető főszám alszámain veszi nyilvántartásba, azaz 1-től növekvő alszámot kap. Amennyiben más tárgyban keletkezett az újabb adat, az iktatókönyv következő főszámát kapja.

(3) Az iktatás minden év január 1-jén 1-es főszámmal kezdődik és a naptári év végéig emelkedő számmal folytatódik. A naptári év végén az iktatókönyvet le kell zárni oly módon, hogy az iktatásra használt utolsó lapon az üresen maradt rovatokat a titkos ügykezelő áthúzza és feltünteti az iktatókönyv lezárásának pontos dátumát, aláírásával és a Nyilvántartó hivatalos bélyegzőlenyomatával látja el. Számítástechnikai eszközön történő nyilvántartás esetén az év végén történő lezárásról szintén gondoskodni kell.

(4) A külföldi minősítéssel és jelöléssel ellátott adatot úgy kell nyilvántartásba venni, hogy az érkezett, a készített, a továbbított, illetve az irattárba helyezett adatok iktatószáma, példányszáma, terjedelme, példányának sorszáma, a tárgya és az egyes példányok őrzési helye megállapítható legyen.

(5) Az egy ügyben keletkezett, önálló részként kezelhető adatokat, ideértve a nem minősítettet is - a legmagasabb minősítésű adat iktatószámán - együtt lehet kezelni és nyilvántartani.

(6) Az iktatáskor a külföldi minősítéssel és jelöléssel ellátott adaton - papíralapú adathordozó esetén - el kell helyezni a iktatóbélyegző lenyomatát.

(7) Az iktatóbélyegző lenyomatának a következőket kell tartalmaznia:
a) a szerv nevét,
b) iktatás pontos dátumát (év, hónap, nap),
c) az iktatószámot,
d) a külföldi minősítéssel és jelöléssel ellátott adat terjedelmét és a mellékleteinek számát.

A külföldi minősítéssel és jelöléssel ellátott adat - szerven belül történő - átadása, visszavétele

40. § (1) A külföldi minősítéssel és jelöléssel ellátott adat átadása, visszavétele csak a titkos ügykezelő útján, belső átadókönyvben vagy más átadó okmányon dokumentált módon történhet.
(2) Külföldi minősítéssel és jelöléssel ellátott adat szerven belül történő átadására és visszavételére szolgáló, az (1) bekezdés szerinti kezelési segédlet tartalmazza:
a) a külföldi minősítéssel és jelöléssel ellátott adat nyilvántartási számát,
b) a minősítési jelölést,
c) a példánysorszámot,
d) a példányonkénti lapterjedelmet,
e) a címzettet,
f) az átadás keltét,
g) az átadás tényének igazolását az átvevő nevének és olvasható aláírásának feltüntetésével,
h) a visszavétel keltét,
i) a visszavétel tényének igazolását a visszavevő nevének és olvasható aláírásának feltüntetésével.

Külföldi minősítéssel és jelöléssel ellátott adat készítése

41. § (1) A Ttv. 5/C. §-ának (1) bekezdése alapján a külföldi minősítés és jelölés alkalmazására a kibocsátó és a felhasználó jogosult.
(2) Amennyiben a Ttv. 3. §-ának és 4. §-ának hatálya alá tartozó minősített adatok átadása szükséges a Ttv. 5/B. § (2)-(7) bekezdésében meghatározott szervek részére, a külföldi minősítéssel és jelöléssel ellátott adaton a Ttv. 5/B. §-ának (2)-(6) bekezdésében, illetve a Ttv. 5/B. §-a (7) bekezdésének hatálya alá tartozó adatok esetén a nemzetközi szerződést kihirdető törvényben meghatározott megfelelő szintű minősítést kell feltüntetni.
(3) Amennyiben a készítő szervnél készült adatba belefoglalják a szerv részére átadott külföldi minősítéssel és jelöléssel ellátott adatot, az így készített adat minősítése nem lehet alacsonyabb az átvett külföldi minősítéssel és jelöléssel ellátott adat minősítésénél.
(4) Az iraton a címzésen, a dátumon kívül fel kell tüntetni:
a) a külföldi minősítést minden oldal alján és tetején középen,
b) a készítő szerv megnevezését,
c) a példány sorszámát,
d) a nyilvántartási számot az első oldalon,
e) az irat tárgyát, hivatkozási számát és az ügy előadóját,
f) a kiadmányozó aláírását,
g) mellékletek esetén azok példányszámát, nyilvántartási számát, lapjainak számát és minősítését,
h) az iratkezelési záradékot, amely tartalmazza
ha) a készített irat példányszámát,
hb) az irat lapszámát,
hc) az irattári kezelési jelzést,
hd) az irat készítőjét és telefonszámát, valamint
he) az egyes példányok címzettjeit.

Felülvizsgálat, a minősítés megszüntetése

42. § (1) A külföldi minősítéssel és jelöléssel ellátott adat minősítésének megszüntetéséről vagy megváltoztatásáról kizárólag a kibocsátó dönthet.

(2) Az a szerv, amely külföldi minősítéssel és jelöléssel ellátott adatot bocsát ki, köteles megvizsgálni - a Ttv. 10. §-ának (1) bekezdésében meghatározott időközönként - a minősítés további fenntartásának szükségességét.

(3) Amikor a kibocsátó az adat minősítését megváltoztatja vagy megszünteti, az adathordozó mindazon oldalán, ahol a minősítési jelölés megváltozik vagy megszűnik, az eredeti minősítést egy vonallal át kell húzni, és közvetlenül alá vagy fölé kell az új minősítést vagy a "Törölve", illetve szükség szerint a "Nem minősített" jelölést elhelyezni, amelyet a minősítő neve, a módosítást végrehajtó személy aláírása és a felülvizsgálat dátuma követ. A változtatásokról mindazokat értesíteni kell, akiknek az adatot megküldték.

(4) A minősítés megváltoztatásáról, illetve megszüntetéséről érkező értesítésben elrendelteket a címzettnek haladéktalanul végre kell hajtania.

A külföldi minősítéssel és jelöléssel ellátott adat másolása, sokszorosítása, fordítása, kivonatolása

43. § (1) Amennyiben a címzettnek szüksége van a "Szigorúan titkos!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatok további példányaira, azokat a kibocsátótól kell kérnie.

(2) Az (1) bekezdésben foglaltak kivételével külföldi minősítéssel és jelöléssel ellátott adat fordítását és másolását a címzett engedélyezheti. Az eredeti adatban jelzett biztonsági előírásokat az elkészített fordításokra, illetve másolatokra is alkalmazni kell.

(3) A másolatra, illetve fordításra rá kell vezetni az eredeti példány iktatószámát, példánysorszámát, valamint a másolatot készítő szervezeti egység megjelölését, a másolatot, fordítást készítő szervezeti egység nyilvántartó könyve szerinti iktatószámát és példányszámát, továbbá a 41. § (4) bekezdésében meghatározott valamennyi alaki kelléket. A másolatot készítő szervezeti egység hitelesített Sokszorosítási naplót vezet.

(4) A sokszorosított példányokat a külföldi minősítéssel és jelöléssel ellátott adat nyilvántartási számán - lehetőség szerint alszámon - kell nyilvántartásba venni. A sokszorosítás során keletkezett felesleges példányokat és selejtes lapokat megsemmisítésre a titkos ügykezelőnek kell átadni, aki köteles e tényt a Sokszorosítási naplóban is dokumentálni.

(5) A külföldi minősítéssel és jelöléssel ellátott adatok másolására csak a biztonsági területen elhelyezett másológépen kerülhet sor.

(6) Annak érdekében, hogy a kivonatok megfelelő védelmét biztosítsák, ezeknek az adatoknak a megfelelő minősítést kell adni. A külföldi minősítéssel és jelöléssel ellátott adat kivonatának tartalmaznia kell az adat vagy alkotórésze - amelyből azt kiemelték - eredeti minősítését (amennyiben egyedileg minősítették), kivéve, ha nyilvánvaló, hogy az más minősítést igényel. A kivonatot záradékolni kell, amely tartalmazza a kivonat készítőjének, engedélyezőjének nevét, beosztását.

Külföldi minősítéssel és jelöléssel ellátott adat továbbítása

44. § (1) Külföldi minősítéssel és jelöléssel ellátott adathordozó más szerv részére történő továbbítása csak titkos ügykezelő útján történhet. Az átadást, illetve az átvételt kézbesítő vagy átadókönyvben, átadókartonon, illetve futárjegyzéken dokumentálni kell. A titkos ügykezelő a továbbítás tényét nyilvántartókönyvben rögzíti.

(2) Külföldi minősítéssel és jelöléssel ellátott adathordozó belföldön az Állami Futárszolgálat útján továbbítható a futárszolgálat igénybevételére vonatkozó szabályok szerint.

(3) Sürgős esetben - vagy ha az nem futárszolgálat útján történik - a külföldi minősítéssel és jelöléssel ellátott adat személyes kézbesítő útján is továbbítható. Ilyen esetben az ügykezelő kézbesítőkönyvvel, illetve futárjegyzékkel átadja a külföldi minősítéssel és jelöléssel ellátott adatot, és felhívja a figyelmet a fokozott biztonsági előírások betartására. A személyes kézbesítő kézbesítőkönyvvel, illetve futárjegyzékkel adja át az adatot az átvételre jogosult személynek.

(4) A "Bizalmas!" vagy annál magasabb minősítésű iratokat dupla, át nem látszó erős csomagolásban kell szállítani. A belső borítékot el kell látni a megfelelő minősítéssel, valamint a címzett teljes megjelölésével és címével, továbbá a szükséges kezelési utasításokkal. A belső borítékot megbízható védelmet nyújtó külső borítóba kell helyezni. A külső borítón csak a címzett szerv megnevezését, a célállomást, a küldő szerv megnevezését és a küldemény nyilvántartási számát kell feltüntetni. Nem szabad semmilyen olyan adatot feltüntetni, ami arra enged következtetni, hogy a csomag (boríték) külföldi minősítéssel és jelöléssel ellátott adatot tartalmaz.

(5) Ha a továbbítás során a küldeményt elveszítették, erről a küldő szervet a továbbításért felelős személy azonnal értesíti. Az elvesztés tényéről haladéktalanul jegyzőkönyvet kell felvenni, amely tartalmazza a küldemény azonosító

adatait, az elvesztés valószínű időpontját, helyét és minden olyan lényeges körülményt, ami a küldemény felkutatását elősegítheti.

(6) Külföldi minősítéssel és jelöléssel ellátott adatot külföldre vagy külföldről diplomáciai, konzuli futár, illetve katonai futár, valamint a nemzetközi jog alapján velük azonos kiváltságokat és mentességeket élvező személy továbbíthat. A Ttv. 5/B. § (7) bekezdésének hatálya alá tartozó adat külföldre vagy külföldről a nemzetközi szerződésben meghatározott személy útján, illetőleg vezetékes vagy vezeték nélküli adatátviteli rendszerben is továbbítható.

A megsemmisítés

45. § (1) A rontott adathordozót, illetve azokat a külföldi minősítéssel és jelöléssel ellátott adatokat, amelyek ügyviteli érdeket már nem képviselnek, megsemmisítés céljából a titkos ügykezelőnek kell átadni. A megsemmisítést a titkos ügykezelő kizárólag a megsemmisítendő külföldi minősítéssel és jelöléssel ellátott adatba betekintési engedéllyel rendelkező személlyel együtt végezheti.

(2) A megsemmisítésről minden esetben jegyzőkönyvet kell felvenni. A jegyzőkönyvnek tartalmaznia kell az azonosításához szükséges adatokat (nyilvántartási szám, lapszám, példány sorszám, minősítés), valamint a megsemmisítést végzők és a biztonsági megbízott aláírását. A jegyzőkönyvet az adat fizikai megsemmisítése után még 10 évig meg kell őrizni.

(3) A megsemmisítés tényét és időpontját, a megsemmisítési jegyzőkönyv számát a külföldi minősítéssel és jelöléssel ellátott adatról készített nyilvántartásba be kell jegyezni.

IV. Fejezet

ELEKTRONIKUS BIZTONSÁGI ALAPELVEK ÉS KÖVETELMÉNYEK

46. § Rendszer üzemeltetését, jóváhagyást követő módosítását, rendszerek összekapcsolását a Felügyelet engedélyezi.

47. § (1) A külföldi minősítéssel és jelöléssel ellátott adat elektronikus biztonsága (a továbbiakban: elektronikus biztonság) azt jelenti, hogy a rendszer és az általa kezelt adatok bizalmassága (illetéktelen hozzáférésnek és jogosulatlan használatnak a kizárása), sértetlensége (illetéktelen módosítás, illetve törlés kizárása) és rendelkezésre állása (az alkalmazási követelményeknek megfelelő módon az arra jogosult személyek számára történő elérhetőség biztosítása) biztosított.

(2) A biztonsági intézkedések célja a jogosulatlan tevékenységtől való visszariasztás, a rendszer fenyegetettsége elleni védelem kialakítása, a biztonságot sértő események felderítése és azonosítása, a biztonság visszaállítása, illetve a biztonságot sértő események kivizsgálásához szükséges adatok biztosítása. A biztonsági intézkedéseknek a rendszer teljes életciklusa alatt érvényesülni kell.

(3) A rendszerek kiépítéséhez nagy megbízhatóságú eszközöket kell alkalmazni. Biztonsági funkciót megvalósító eszközök kiválasztása során az illetékes biztonsági felügyelet iránymutatása szerint kell eljárni.

(4) A külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszert a jelen rendeletben megfogalmazott általános követelmények szerint kell védeni a fenyegetésektől. Meg kell vizsgálni a rendszer telepítési helyszínén a feldolgozott külföldi minősítéssel és jelöléssel ellátott adat mennyiségét, formáját és az egyéb biztonsággal összefüggő tényezőket, és amennyiben azok indokolják, kiegészítő biztonsági követelményeket lehet meghatározni.

(5) A rendszer csak megfelelő személyi, fizikai, dokumentum és elektronikus biztonsági feltételek megléte esetén üzemeltethető. Az erre vonatkozó részletes előírásokat, valamint a biztonsági másolatok készítésére, tárolására, a helyreállításra, a vészhelyzetben követendő eljárásokra vonatkozó részletes utasításokat, valamint rendellenesség, biztonságot veszélyeztető esemény bekövetkezése esetén végrehajtandó intézkedéseket a Rendszer Biztonsági Utasításban, illetve az Üzemeltetés Biztonsági Szabályzatban kell rögzíteni.

(6) Az elektronikus biztonság személyi, fizikai és dokumentum biztonsági követelményeit az R. szerinti eljárásrend szerint kell alkalmazni. Az elektronikus biztonsági eljárásrend tekintetében az R. IV. fejezete az irányadó.

A biztonságért felelős szervezetek és személyek felelőssége és feladatai

48. § A Felügyelet hatásköre kiterjed minden külföldi minősítéssel és jelöléssel ellátott kép, hang és adat elektronikus jelek formájában történő kezelésére szolgáló rendszerre. A Felügyelet a külföldi minősítéssel és jelöléssel ellátott adat elektronikus védelmét a vonatkozó NATO, NYEU, illetve EU szabályok alapján az Országos Rejtjelfelügyelet és az illetékes biztonsági felügyelet közreműködésével biztosítja.

49. § A NATO, NYEU, illetve EU előírások szerint elektronikus biztonsági felügyeleti szempontból a rendszerre kiterjedően a Felügyelet általános elektronikus biztonsági hitelesítő hatósági feladatokat lát el. E tevékenység keretében:

a) felelős a rendszer elektronikus biztonsági jóváhagyásáért, illetve akkreditálásáért;

b) jóváhagyja a NATO, NYEU, illetve EU előírások szerinti elektronikus biztonsági dokumentumokat, így különösen a Rendszer Biztonsági Utasítást és Üzemeltetés Biztonsági Szabályzatot;

c) kiadja a Rendszerengedélyt;

d) engedélyezi a rendszer módosítását;

e) a rendszer tekintetében felügyeleti ellenőrzést végez;

f) közvetlen kapcsolatot tart fenn az illetékes biztonsági felügyeletekkel, valamint az Országos Rejtjelfelügyelettel, és együttműködik a NATO, NYEU, illetve EU és tagállami elektronikus biztonsági szervekkel;

g) összekötő szerv a NATO, NYEU, illetve EU és a tagállamok rendszer engedélyezési ügyekben illetékes elektronikus biztonsági szervei felé.

50. § (1) Az Országos Rejtjelfelügyelet szakhatósági tevékenység keretében:

a) felelős a rendszerben használatra elfogadott rejtjelző eszközök és módszerek rendszeresítésére és azok üzembe helyezésére vonatkozó engedélyezési eljárás lefolytatásáért;

b) gondoskodik a rendszerben használatra elfogadott rejtjelző eszközök és módszerek alkalmazására vonatkozó különös szabályok kidolgozásáról;

c) a rendszerben történő használatra felajánlhat nemzeti rejtjelző eszközöket és módszereket.

(2) Az Országos Rejtjelfelügyelet szakmai felügyeleti tevékenység keretében:

a) ellátja a rendszer rejtjelbiztonsági felügyeletét;

b) a feladatkörébe tartozó ügyekben közvetlen kapcsolatot tart fenn, és együttműködik az elektronikus biztonsági szervekkel, így különösen a Felügyelettel, az illetékes biztonsági felügyeletekkel, valamint a NATO, NYEU, illetve EU illetékes szerveivel.

(3) A Honvédelmi Minisztérium a NATO, illetve NYEU rejtjelző szakanyagok országos szinten történő fogadására, kezelésére és az illetékes biztonsági felügyeletek felé történő elosztására Központi NATO, illetve NYEU Rejtjelanyag Elosztót üzemeltet.

(4) A Külügyminisztérium az EU rejtjelző szakanyagok országos szinten történő fogadására, kezelésére és az illetékes biztonsági felügyeletek felé történő elosztására Központi EU Rejtjelanyag Elosztót üzemeltet.

51. § (1) Az illetékes biztonsági felügyelet a NATO, NYEU, illetve EU előírások szerint elektronikus biztonsági felügyeleti szempontból a rendszerre vonatkozóan szakmai felügyeleti feladatokat lát el. E tevékenységét a NATO, NYEU, illetve EU előírások alapján és a Felügyelet elektronikus biztonsági hitelesítő hatósági feladatkörében hozott döntéseinek megfelelően végzi.

(2) Az illetékes biztonsági felügyelet a NATO, NYEU, illetve EU rendszerre kiterjedően:

a) felelős a szerv elektronikus biztonsági szabályzatainak elkészítéséért, azok tartalmának szakszerűségéért és rendelkezéseinek megtartásáért;

b) felelős a NATO, NYEU, illetve EU rejtjelző és rejtjelző elszámolású szakanyagok, dokumentumok, eszközök, berendezések - az 50. § (3), illetve (4) bekezdéseiben meghatározott szervektől történő - átvételéért, nyilvántartásáért, tárolásáért, valamint az ehhez szükséges rendszer kiépítéséért, illetve az arra vonatkozó biztonsági intézkedések betartásáért;

c) feladatkörébe tartozó ügyekben közvetlen kapcsolatot tart fenn és együttműködik az elektronikus biztonsági szervekkel, így különösen a Felügyelettel, az Országos Rejtjelfelügyelettel, valamint a NATO, NYEU, illetve EU illetékes szerveivel.

(3) Az illetékes biztonsági felügyelet fő feladatai a NATO, NYEU, illetve EU rendszerre kiterjedően:

a) tervezi, szervezi, ellenőrzi az elektronikus biztonsági feladatokat ellátó személyek tevékenységét, összehangolja a különböző szervezeti egységek ez irányú tevékenységét;

b) javaslatot tesz a rendszerspecifikus biztonsági feladatköröket ellátó személyek kijelölésére;

c) ellátja az elektronikus biztonsággal kapcsolatos koordinációs feladatokat;

d) gondoskodik a rendszerek biztonságos üzemeltetéséről, ellenőrzi a használat szabályosságát;

e) részt vesz az engedélyezési eljárásokban;

f) tervezi, szervezi és végrehajtja az elektronikus biztonsági továbbképzési feladatokat;

g) biztosítja, hogy hatékony mentési terveket és vészhelyzeti intézkedési terveket készítsenek az elektronikus információkra és a rendszerekre vonatkozóan;

h) az elektronikus biztonsági eseményeket kivizsgálja, illetve ellátja az ehhez kapcsolódó feladatokat;

i) naprakész nyilvántartást vezet az illetékességi körébe tartozó, Rendszerengedéllyel rendelkező rendszerekről, tárolja ezek biztonsági dokumentációját és az ezt kiegészítő tanúsítványokat;

j) gondoskodik arról, hogy a NATO, NYEU, illetve EU szabályozókban rögzített kisugárzás biztonsági követelmények érvényesüljenek;

k) érvényesíti az elektronikus biztonsági követelményeket illetékességi területén a rendszerek teljes életciklusában;

l) "Bizalmas" vagy magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszer esetében gondoskodik az érintett létesítmények kompromittáló kisugárzás biztonsági besorolásának meghatározásáról, szükség esetén az ezzel kapcsolatos mérések elvégeztetéséről;

m) gondoskodik arról, hogy a vonatkozó szabályzatokban rögzített számítógép és hálózati biztonsági követelmények a rendszerek teljes életciklusában érvényesüljenek;

n) rendszeres biztonsági ellenőrzést végez a rendszerre vonatkozóan;

o) gondoskodik a rendszer elektronikus biztonsági dokumentumainak, így különösen a Rendszer Biztonsági Utasítás és Üzemeltetés Biztonsági Szabályzat elkészíttetéséről és jóváhagyatásáról;

p) gondoskodik a rendszert tartalmazó terület, ezen belül az általános biztonsági környezetre, a helyszín biztonsági környezetre és az elektronikus biztonsági környezetre vonatkozó követelmények teljesítéséről.

52. § A rendszerek üzemeltetését végrehajtó személyeket a munkáltatói jogokat gyakorló vezető írásban jelöli ki a rendszer biztonságos üzemeltetésével kapcsolatos következő feladatokra:

a) a rendszerek működőképességének fenntartása, biztonsági funkciót megvalósító szoftverek telepítése és konfigurálása, hibaelhárítása;

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

c) az informatikai biztonsági funkciót megvalósító rendszerösszetevők telepítése, konfigurálása;

d) részvétel az elektronikus biztonsági ellenőrzésekben és azok előkészítésében;

e) a szakterületet illető tanácsadás a felhasználóknak, illetve az elektronikus biztonsági felelősöknek;

f) a szabályozás keretei között a rendszer önállóan történő működtetése;

g) az előírt nyilvántartások vezetése;

h) a rendszer logisztikai támogatása;

i) vírusvédelmi eljárások kidolgozása;

j) az Üzemeltetés Biztonsági Szabályzat tartalmának a felhasználókkal történő megismertetése, valamint ennek dokumentálása;

k) a felhasználók adatainak és jogosultságainak naprakész nyilvántartása;

l) jelszóhasználati szabályok kidolgozása;

m) a felhasználói jelszavak használatával kapcsolatos előírások betartatása.

53. § A rendszer biztonsági felelős főbb feladatai:

a) a rendszer biztonsági dokumentációjának elkészítése a rendszer üzemeltető állománnyal együttesen;

b) javaslattétel a külföldi minősítéssel és jelöléssel ellátott adat elektronikus biztonságát javító intézkedésekre, és jóváhagyás után azok végrehajtása;

c) az illetékes biztonsági felügyelet számára adatszolgáltatás az engedélyezési eljárás során;

d) a biztonsági dokumentációban foglaltak pontos betartása és betartatása;

e) a rendszer konfiguráció biztonsági ellenőrzése, beleértve azon adatok gyűjtését és rendszeres vizsgálatát, amelyek biztonsággal kapcsolatos eseményekre utalnak;

f) vészhelyzeti intézkedési terv elektronikus biztonságra vonatkozó részének elkészítése;

g) a vészhelyzet esetén szükséges tevékenység gyakoroltatása;

h) a külföldi minősítéssel és jelöléssel ellátott adathordozók előírások szerinti kezelésének biztosítása;

i) a rendszer biztonsági dokumentációjának nyilvántartása, tárolása, szükség szerinti rendelkezésre bocsátása;

j) a rendszer biztonsági naplófájlok rendszeres mentése, ezek átvizsgálása és tárolása;

k) a rendszer szintű hozzáféréssel rendelkező személyek azonosítóinak, jelszavainak tárolása.

54. § A rendszeren külföldi minősítéssel és jelöléssel ellátott adat kezelését végző személyeknek (a felhasználóknak) a rendszeren engedélyezett legmagasabb minősítési szintnek megfelelő minősítésű adatokhoz hozzáférést engedélyező Személyi Biztonsági Tanúsítvánnyal kell rendelkezniük.

A rendszer elemeinek és telepítési helyszínének biztonsága

55. § (1) Rendszer létesítése csak olyan szervnél engedélyezhető, amely a külföldi minősítéssel és jelöléssel ellátott adat minősítési szintjének megfelelő, e rendelet szerinti személyi, fizikai és dokumentum biztonsági feltételekkel rendelkezik.

(2) A rendszer védelmét a rendszeren feldolgozható legmagasabb minősítési szintnek megfelelő, e rendelet II. fejezetében meghatározott fizikai biztonság kialakításával kell biztosítani. "Bizalmas!" vagy ennél magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszert I. vagy II. osztályú biztonsági területen kell telepíteni. "Korlátozott terjesztésű!" vagy nem minősített külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszert adminisztratív zónában is lehet telepíteni.

(3) Azt a rendszert vagy elemeit, amelyen külföldi minősítéssel és jelöléssel ellátott adatot már kezeltek, a biztonsági területről kivinni kizárólag az adathordozó - és minden más, esetlegesen adat visszanyerésére alkalmas részegység - eltávolítását követően szabad, kivéve a más biztonsági területre történő szállítást.

(4) Olyan "Bizalmas!" vagy magasabb minősítésű adathordozó, amelyet már használtak külföldi minősítéssel és jelöléssel ellátott adat tárolására vagy feldolgozására, nem hagyhatja el a biztonsági területet, kivéve a másik biztonsági területre történő szállítás esetét.

(5) Adathordozón rögzített külföldi minősítéssel és jelöléssel ellátott adat csak a Felügyelet által engedélyezett eljárásokkal törölhető, melyet dokumentálni kell. Olyan módszereket kell alkalmazni, hogy a törölt külföldi minősítéssel és jelöléssel ellátott adat a továbbiakban ne legyen helyreállítható.

(6) Az adathordozó minősítése csak a külföldi minősítéssel és jelöléssel ellátott adat törlését követően szüntethető meg. "Szigorúan titkos!" minősítéssel ellátott adathordozó minősítése törléssel nem módosítható, nem szüntethető meg, de az engedélyezett eljárásokkal az adathordozó megsemmisíthető.

A rendszer elemeivel kapcsolatos biztonsági követelmények

56. § (1) "Bizalmas!" és magasabb minősítésű külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszer védelmének meg kell felelnie a kompromittáló kisugárzás elleni biztonsági követelményeknek. Ezen követelmények kiterjednek az elektromos kábelek vonalvezetésére, rádiófrekvenciás szűrők alkalmazására, a rendszer környezetében alkalmazható berendezésekre, elektromágneses árnyékolástechnikai megoldásokra, illetve csökkentett kisugárzású hardver eszközök alkalmazására, az építészeti, épületgépészeti, épületvillamossági, valamint a rendszerhez tartozó fém berendezések földelésére. A földelés megfelelőségét legalább évente kell méréssel igazolni.

(2) Naprakész nyilvántartást kell vezetni a rendszerben alkalmazott eszközökről, berendezésekről, hardverről, szoftverről és átviteli eszközökről. Az akkreditálást, illetve a jóváhagyást követően a rendszer konfiguráción olyan módosítást végrehajtani, amely az eredetileg akkreditált, illetve jóváhagyott rendszer biztonságát érinti, csak a Felügyelet előzetes engedélyével lehet végrehajtani.

(3) A rendszerben alkalmazott adathordozó biztonságát, különösen a kezelés és szállítás szempontjából, az e rendeletben meghatározott dokumentumbiztonsági követelményeknek megfelelően kell biztosítani.

(4) Minden, a rendszerben alkalmazott adathordozót a rajta tárolható legmagasabb minősítéssel rendelkező adat minősítési szintjének megfelelően kell nyilvántartani. Az adathordozón fel kell tüntetni a minősítést és a nyilvántartási számot. Amennyiben ez nem lehetséges a fel nem tüntethető azonosítók dokumentálására külön kísérőlapot kell készíteni.

(5) A rendszer biztonsági dokumentációiban meghatározott időszakonként a külföldi minősítéssel és jelöléssel ellátott adatokról biztonsági másolatokat kell készíteni, és erről nyilvántartást kell vezetni. A biztonsági másolatokat tartalmazó adathordozót a minősítési szintnek megfelelően nyilvántartásba kell venni, és ennek megfelelően kell tárolni.

57. § (1) A rendszerre csak a Felügyelet által engedélyezett operációs rendszer és egyéb szoftver telepíthető, amelyek jogosult felhasználásra vonatkozó tanúsítványait az üzemeltető szervnél kell őrizni. A biztonsági területre nem engedélyezett szoftver, illetve hardver, adathordozó, valamint saját tulajdonú, adat rögzítésére és továbbítására szolgáló eszköz nem vihető be.

(2) Az operációs rendszer, az alkalmazói programok és a segédprogramok telepítő lemezeit vagy biztonsági másolatait megfelelő biztonsági feltételek között kell tárolni. Szükség esetén a szoftver helyreállítása csak ezekről történhet.

(3) A rendszeren csak a biztonsági dokumentációban szereplő szoftverek alkalmazhatóak, más szoftverek alkalmazása nem engedélyezhető. Utólagosan telepített szoftver esetében a dokumentációt erre vonatkozóan ki kell egészíteni. Ha a rendszerre nem a gyártó által védett adathordozón forgalmazott új szoftvert telepítenek, a telepítést megelőzően különálló számítógépen biztonsági ellenőrzést kell végrehajtani, elsősorban vírus vagy más rosszindulatú szoftver kiszűrése érdekében.

58. § (1) A rendszer működését szabályozó konfigurációs beállításokhoz és a biztonsági célú naplózott adatokhoz csak az illetékes biztonsági felügyeletnek lehet hozzáférése. Az operációs rendszeren és annak biztonsági beállításain változtatást az illetékes biztonsági felügyelet engedélyezhet.

(2) A rendszerhez történő hozzáférést megelőzően a felhasználót minden alkalommal megbízhatóan azonosítani kell. Ez személyes használatra kiadott és egyidejűleg nyilvántartásba vett felhasználói névvel, valamint ehhez tartozó jelszóval, vagy ennél nagyobb biztonságot jelentő technológiával történhet. A felhasználókhoz az "ismerete szükséges" elv alkalmazásával írási, olvasási, módosítási, törlési stb. jogokat lehet engedélyezni.

59. § (1) A jelszóhasználat részletes szabályait az Üzemeltetés Biztonsági Szabályzat tartalmazza. A jelszó minimális hossza, illetve a maximális felhasználási ideje "Bizalmas!" és magasabb minősítésű rendszer esetében legalább 8 karakter, illetve legfeljebb 180 nap, "Korlátozott terjesztésű!" vagy nem minősített rendszer esetében legalább 6 karakter, illetve legfeljebb egy év. A jelszavakat módosítani kell, ha bárki más részére hozzáférhetővé válhatott, illetve ha személyi változás történt. Az első belépéshez generált jelszót a bejelentkezés után azonnal meg kell változtatni.

(2) A rendszer biztonsági felelős jelszavát a többi felhasználó számára előírtnál gyakrabban kell cserélni, és a rendszer biztonsági dokumentációban előírt módon, a rendszer minősítésének megfelelő fizikai biztonsági követelményeknek megfelelően kell tárolni.

(3) A felhasználó köteles a jelszavát megjegyezni és gondoskodni arról, hogy más személy részére ne váljon hozzáférhetővé.

(4) A felhasználói jelszót vészhelyzetben történő felhasználás esetére lepecsételt, lezárt borítékban a rendszer minősítési szintjének megfelelő biztonsági körülmények között lehet tárolni.

(5) A (2) és a (4) bekezdés szerint tárolt jelszavakhoz történő hozzáférés és nyilvántartás rendjéről az Üzemeltetés Biztonsági Szabályzatban kell rendelkezni.

60. § Vírusok és más rosszindulatú szoftverek ellen a rendszert védeni kell. A védelemnek rendszer indításkor, valamint a kivehető adathordozók használatakor automatikus ellenőrzést kell végrehajtania.

61. § (1) A rendszer naplózási funkciójával a következő eseményeket kell rögzíteni:

a) rendszer indítás, újraindítás, leállítás;

b) felhasználói belépések, kilépések;

c) felhasználók és felhasználói csoportok jogosultságainak és profiljainak módosítása;

d) naplózási funkció indítása, illetve leállítása;

e) a biztonsági naplózás adatainak törlése vagy ezekről másolat készítése;

f) a rendszer dátum és idő módosítása;

g) rendszer erőforrásokhoz történő sikertelen hozzáférési kísérlet;

h) automatikus riasztási funkciók működésének leállítása;

i) külső adathordozó használata;

j) valamely felhasználó rendszerről történő leválasztása vagy hozzáférésének letiltása.

(2) A naplózási funkciónak az alábbi paraméterekre kell kiterjednie:

a) az esemény típusa;

b) a felhasználó azonosítója;

c) az esemény ideje;

d) az esemény kimenetele (sikeres vagy sikertelen).

(3) A sikertelen rendszer hozzáférési kísérleteket ellenőrizni kell annak megállapítása érdekében, hogy történt-e a biztonságot veszélyeztető esemény.

(4) Az Üzemeltetési Biztonsági Szabályzatban meghatározott időszakonként vagy a biztonság megsértésének gyanúja esetén azonnal konfiguráció ellenőrzést kell végrehajtani annak megállapítása érdekében, hogy a rendszeren történt-e engedély nélküli változtatás.

(5) A rendszer működése folyamán a biztonságot veszélyeztető eseményeket a rendszer biztonsági dokumentációjában rögzíteni kell.

62. § (1) Amennyiben a külföldi minősítéssel és jelöléssel ellátott adat elektronikus biztonságát rejtjelzéssel is biztosítani kell, a rendszerre vonatkozó specifikus követelményeket az általános rejtjelzésre vonatkozó szabályozás alapján az illetékes biztonsági felügyelet határozza meg.

(2) Külföldi minősítéssel és jelöléssel ellátott adat "Bizalmas!" minősítési szintig nemzeti rejtjelző eszközön továbbítható.

(3) "Bizalmas!" és alacsonyabb minősítéssel ellátott külföldi minősítéssel és jelöléssel ellátott adat védelmére a NATO, NYEU, illetve az EU illetékes szerve vagy az Országos Rejtjelfelügyelet által jóváhagyott rejtjelző eszköz alkalmazható. "Titkos!" vagy "Szigorúan titkos!" külföldi minősítéssel és jelöléssel ellátott adat rejtjelzéssel történő

védelmére kizárólag a NATO, NYEU, illetve az EU illetékes szerve által jóváhagyott rejtjelző eszközök alkalmazhatóak.

(4) A rejtjelző eszközök rendszeresítését, használatbavételét az Országos Rejtjelfelügyelet engedélyezi. A rejtjelzés végrehajtásának, berendezéseinek, eszközeinek, eljárásainak, anyagainak és szakanyagainak biztonságára vonatkozóan a rejtjeltevékenységről szóló 43/1994. (III. 29.) Korm. rendelet az irányadó.

A rendszer biztonsági dokumentációja

63. § (1) A rendszerre vonatkozó biztonsági követelményeket és eljárásokat a Rendszer Biztonsági Utasítás és az Üzemeltetés Biztonsági Szabályzat tartalmazza, melyek betartása kötelező a rendszert működtető vagy felhasználó szervekre, illetve személyekre.

(2) A Rendszer Biztonsági Utasítást, minden "Bizalmas!" és magasabb minősítésű rendszer esetében el kell készíteni. Az alábbi fejezeteket kell tartalmaznia:

a) a rendszer alapadatai;

b) a rendszer leírása;

c) a rendszerrel szemben támasztott biztonsági követelmények;

d) a rendszer biztonsági környezetének leírása;

e) a rendszerre vonatkozó biztonsági intézkedések;

f) a biztonsága szervezése és a felelősségi körök meghatározása.

(3) A Rendszer Biztonsági Utasítás végrehajtására Üzemeltetés Biztonsági Szabályzatot kell készíteni minden "Bizalmas!" és magasabb minősítésű rendszer esetében. Ennek az alábbi fejezeteket kell tartalmaznia:

a) a biztonság helyi szervezése és helyi felelősségi körök meghatározása;

b) fizikai biztonság;

c) személyi biztonság;

d) dokumentum biztonság;

e) hardver és szoftver biztonság;

f) vészhelyzeti és helyreállítási terv;

g) kommunikáció biztonság;

h) konfiguráció menedzsment.

(4) "Korlátozott terjesztésű!" minősítésű külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszer esetében a biztonsági követelményeket és a biztonsággal kapcsolatos eljárásokat, illetve felelősségeket az Üzemeltetés Biztonsági Szabályzat tartalmazza.

(5) A rendszer létesítésének és üzemeltetésének engedélyezéséhez a biztonsági dokumentumoknak a következőket kell tartalmaznia:

a) helyszínrajz és szöveges leírás, amely a telep teljes területét, határait és a szomszédos, nem saját ellenőrzés alá tartozó létesítmények elhelyezkedését mutatja. Be kell jelölni a rendszer telepítésének helyét oly módon, hogy annak távolsága az idegen területektől egyértelműen meghatározható legyen (0-8 m, 8-20 m, 20-100 m, 100 m felett) és meg kell adni a kerítés, kapu típusát, magasságát, őrségbeléptető pontok helyét;

b) alaprajz és szöveges leírás, amely a rendszer telepítési helyét magába foglaló épület, épületrész részletes rajzát tartalmazza oly módon, hogy a telepítési hely megközelítése és a helyszín biztonsági körülményei (beléptető, ellenőrző pontok, a biztonsági rendszer elemei, az elektromos és adatvezetékek nyomvonalai, épületgépészet - víz, csatorna, fűtés stb. - elemei, falak anyaga és vastagsága, ajtók és ablakok típusa és jellemzői stb.) egyértelműen meghatározhatók legyenek;

c) telepítési hely alaprajz és szöveges leírás, amely a rendszer tényleges elemeit a valóságos helyzetüknek megfelelően (a gép, nyomtató, monitor iránya stb.) ábrázolja oly módon, hogy a gép körüli védett tér egyértelműen azonosítható legyen. Az alaprajz sematikusan tartalmazza a biztonságtechnikai eszközök és beléptető rendszer elemeit, a helyiségekben levő minden építészeti, épületgépészeti és épület elektromos eszköz és berendezés valóságos helyét, a hálózati áramellátás, biztonságtechnika és telefon kábelek és csatlakozók sematikusan ábrázolt nyomvonalát, a telepített rádiófrekvenciás szűrők helyét, valamint a berendezési tárgyakat (asztal, szék, tároló stb.).

(6) A rendszer biztonsági dokumentációit a Felügyelet hagyja jóvá.

V. Fejezet

EGYÉB BIZTONSÁGI INTÉZKEDÉSEK

64. § (1) A titokbirtokos szerv vezetője e rendelet keretei között Biztonsági Szabályzatban rendelkezik

a) a személyi biztonság követelményeiről;

b) a külföldi minősítéssel és jelöléssel ellátott adat védelméről, ezen belül a védelemre kötelezett, illetve a minősítés és jelölés alkalmazására jogosult személyek hatásköréről, a minősítési eljárásról, a minősítés felülvizsgálatáról, valamint megszüntetéséről, a külföldi minősítéssel és jelöléssel ellátott adatok megismerésének feltételeiről, azok átadásának, szállításának eljárási szabályairól, az ellenőrzés és a külföldi minősítéssel és jelöléssel ellátott adattal történő elszámoltatás rendjéről, az eljárások bizonylati rendjéről;

c) a külföldi minősítéssel és jelöléssel ellátott adat megsértése, elvesztése esetére meghatározott eljárásról, így különösen

ca) a külföldi minősítéssel és jelöléssel ellátott adathoz történő jogosulatlan hozzáférés vagy ennek veszélye esetén szükséges eljárásról,

cb) a biztonságtechnikai berendezés indokolt és indokolatlan működése esetén követendő eljárásról,

cc) a tűz vagy más elemi csapás következményeinek kivédésére, az okozott kár felszámolására irányuló feladatról,

cd) a veszélyeztetett a külföldi minősítéssel és jelöléssel ellátott adat mentésére kidolgozott eljárásról;

d) a fizikai biztonságra vonatkozó követelményekről;

e) az elektronikus biztonságra vonatkozó követelményekről.

(2) A titokbirtokos szerv vezetője e rendelet keretei között intézkedési tervben rendelkezik a külföldi minősítéssel és jelöléssel ellátott adatok vészhelyzetben történő védelméről.

(3) A megbeszélésekre - ha azokon külföldi minősítéssel és jelöléssel ellátott adatok felhasználására sor kerül - vonatkozó biztonsági szabályoknak meg kell felelniük a találkozó, illetve a megbeszélés szintjének. A megvitatott adatok minősítési szintjét a rendezvényt összehívó tagország hatóságai határozzák meg.

(4) Azokat a területeket, ahol "Titkos!" vagy ennél magasabb minősítéssel ellátott külföldi minősítéssel és jelöléssel ellátott adatokról is rendszeresen tárgyalnak, védeni kell a lehallgatásoktól. A kockázat szintjét az illetékes nemzetbiztonsági szolgálat határozza meg.

(5) A lehallgatások elleni védelem magában foglalja a műszaki jellegű berendezések alkalmazását, valamint a hangszigetelő falak, ajtók, padló- és mennyezetburkolatok alkalmazását az érzékenynek minősülő területeken.

(6) A lehallgatások elleni védelem biztosítása érdekében az adott helyiséget, annak berendezéseit műszaki, illetve fizikai biztonsági ellenőrzésnek kell alávetni. Ezeket az ellenőrzéseket a hatáskör szerint illetékes nemzetbiztonsági szolgálat végzi.

(7) Külföldi minősítéssel és jelöléssel ellátott adatokat feldolgozó találkozók, megbeszélések előkészítése során a rendezvény lebonyolításáért felelős biztonsági szervnek biztosítási tervet kell készítenie.

VI. Fejezet

A BIZTONSÁG MEGSÉRTÉSE ÉS A KÜLFÖLDI MINŐSÍTÉSSEL ÉS JELÖLÉSSEL ELLÁTOTT ADATOK VESZÉLYBE KERÜLÉSE

65. § (1) A Ttv. 5/B. §-a (2)-(6) bekezdésében meghatározott külföldi minősítéssel és jelöléssel ellátott adat biztonságának minden megsértését haladéktalanul jelenteni kell a Felügyelet elnökének - a Ttv. 5/B. §-a (7) bekezdésében meghatározott külföldi minősítéssel és jelöléssel ellátott adat esetén pedig a nemzetközi szerződésben meghatározott szerv vezetőjének -, aki köteles azt kivizsgáltatni, és a hatályos biztonsági előírásoknak megfelelő jelentési, illetve tájékoztatási kötelezettségének eleget tenni.

(2) A külföldi minősítéssel és jelöléssel ellátott adat biztonságának megsértéséről szóló jelentésnek tartalmaznia kell:

a) a veszélyeztetett külföldi minősítéssel és jelöléssel ellátott adatok azonosításához szükséges adatokat,

b) a kibocsátó szerv megnevezését és a kiadás időpontját,

c) a minősítést és annak érvényességi idejét,

d) az eredeti és a fogadó szervnél kapott nyilvántartási számot,

e) a tárgyat, a lap- és példánysorszámot,

f) a biztonság megsértésének körülményeit,

g) a veszélyeztetettség idejét (ismert vagy vélelmezett időhatárait),

h) a veszélyeztetettség helyét,

i) a veszélyeztetettség kialakulásának elsődleges okait,

j) ha ismert, a biztonság megsértéséért felelőssé tehető személy nevét,

k) a megtett intézkedések felsorolását.

(3) A vizsgálatot végző bizottságba csak olyan személyek jelölhetők ki, akik rendelkeznek a sérelmet szenvedett külföldi minősítéssel és jelöléssel ellátott adat minősítésének megfelelő betekintési engedéllyel, megfelelő vizsgálati tapasztalatuk van és függetlenek a sérelemben közvetlenül érintettektől.

MÓDOSULÓ RENDELKEZÉSEK

66. § (1) A minősített adat kezelésének rendjéről szóló 79/1995. (VI. 30.) Korm. rendelet 16. §-a helyébe a következő rendelkezés lép:

"16. § Államtitok esetén az "Államtitok!" megjelölést, szolgálati titok esetén a "Szolgálati titok!" megjelölést, továbbá a minősítési jelölést, az érvényességi időt, a minősítő nevét és beosztását, az adat magyar származását jelölő országjelet (MK/HU) az adat nyilvántartására és azonosítására szolgáló jelzéssel együtt az adathordozón, és ha van ilyen, annak borítóján is fel kell tüntetni. Több lapból álló papíralapú adathordozón a minősítési jelölést minden egyes lapon, annak felső részén és alsó részén középen is fel kell tüntetni."

(2) A minősített adat kezelésének rendjéről szóló 79/1995. (VI. 30.) Korm. rendelet 19. §-ának (1)-(2) bekezdése helyébe a következő rendelkezés lép:

"19. § (1) A minősített adatok kölcsönös védelmére vonatkozó nemzetközi szerződésben meg kell állapodni arról, hogy az átadott minősített adathordozón használt külföldi jelölés esetén mikor kell a "Szigorúan titkos!", "Titkos!", "Bizalmas!", illetve "Korlátozott terjesztésű!" jelölést feltüntetni, továbbá arról, hogy a magyar jelölésnek mi a külföldi megfelelője. Meg kell állapodni abban is, hogy az érvényességi idő feltüntetése hogyan történjen, valamint arról is, hogy a minősítési jelölésen kívül még milyen más kezelési utasítás használható.

(2) A külföldi minősítéssel és jelöléssel ellátott irat magyar fordításán a "Szigorúan titkos!", "Titkos!", "Bizalmas!", illetve "Korlátozott terjesztésű!" minősítési jelölés mellett a minősítést idegen nyelven, az eredeti formában is fel lehet tüntetni."

ZÁRÓ RENDELKEZÉSEK

67. § (1) Ez a rendelet a kihirdetését követő 8. napon lép hatályba. Ezzel egyidejűleg hatályát veszti a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint a korlátozottan megismerhető adatok védelmének eljárási szabályairól szóló 56/1999. (IV. 2.) Korm. rendelet, valamint a Központi Nyilvántartó, a nyilvántartó és az ellenőrző pont működési rendjéről szóló 4/2000. (II. 29.) HM rendelet.

(2) A biztonsági szabályzatokat, valamint az intézkedési terveket 2004. június 30-ig kell felülvizsgálni.

(3) Felhatalmazást kap a belügyminiszter, hogy megállapítsa a NATO, NYEU, illetve EU minősített adatok Állami Futárszolgálat útján való belföldi továbbításának különös szabályait.

1. számú melléklet a 179/2003. (XI. 5.) Korm. rendelethez

Minimum biztonsági követelmények

	Minimum pontszámok
"Szigorúan titkos!" külföldi minősítéssel és jelöléssel ellátott adatok	
Kötelező a 19-20. §-ban és a 23. §-ban meghatározottak vagy a 21-22. §-ban és a 23. §-ban meghatározottak alkalmazása	10
Kötelező a 24., 26-27. §-ban meghatározottak alkalmazása	6
További nem kötelező más fizikai biztonsági intézkedés	4
Teljes pontszám:	20
"Titkos!" külföldi minősítéssel és jelöléssel ellátott adatok	
Kötelező a 19-20. §-ban és a 23. §-ban meghatározottak vagy a 21-22. §-ban és a 23. §-ban meghatározottak alkalmazása	8
Kötelező a 24., 26-27. §-ban meghatározottak alkalmazása	4

További nem kötelező más fizikai biztonsági intézkedés	4
Teljes pontszám:	16
"Bizalmas!" külföldi minősítéssel és jelöléssel ellátott adatok	
Kötelező a 19-20. §-ban és a 23. §-ban meghatározottak vagy a 21-22. §-ban és a 23. §-ban meghatározottak alkalmazása	6
Kötelező a 24., 26-27. §-ban meghatározottak alkalmazása	2
További nem kötelező más fizikai biztonsági intézkedés	3
Teljes pontszám:	11
"Korlátozott terjesztésű!" külföldi minősítéssel és jelöléssel ellátott adatok	
Kötelező a 19-20. §-ban és a 23. §-ban meghatározottak vagy a 21-22. §-ban és a 23. §-ban meghatározottak alkalmazása	2
További nem kötelező más fizikai biztonsági intézkedés	-
Teljes pontszám:	2

2. számú melléklet a 179/2003. (XI. 5.) Korm. rendelethez

Fizikai biztonsági intézkedések ponttáblázata

	Pontszámok
I. fejezet Biztonsági tárolók és zárak	
Tárolók	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
R1 Részpontszám lehet 1 vagy 2 vagy 3 vagy 4	
Zárak	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
R2 Részpontszám lehet 1 vagy 2 vagy 3 vagy 4	
F1 I. fejezet pontszáma R1 x R2	
II. fejezet Helyiségek és ahhoz tartozó zárak	
Helyiségek	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
R3 Részpontszám lehet 1 vagy 2 vagy 3 vagy 4	
Helyiségekhez tartozó zárak	
4. osztályú	4

3. osztályú	3
2. osztályú	2
1. osztályú	1
nincsen zár	0
R4 Részpontszám lehet 0 vagy 1 vagy 2 vagy 3 vagy 4	
F2 II. fejezet pontszáma R3 x R4	
III. fejezet Épületek	
4. osztályú	5
3. osztályú	3
2. osztályú	2
1. osztályú	1
F3 III. fejezet pontszáma	
IV. fejezet Beléptető rendszer	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
R5 Részpontszám lehet 1 vagy 2 vagy 3 vagy 4	
Látogatók ellenőrzése	
kísérettel	3
kíséret nélkül, igazolvánnyal	1
nincsen intézkedés	0
R6 Részpontszám lehet 0 vagy 1 vagy 3	
F4 IV. fejezet pontszáma R5 + R6	
V. fejezet Reagáló erők és behatolás jelző rendszer	
5. osztályú	5
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
nincsen	0
R7 Részpontszám lehet 0 vagy 1 vagy 2 vagy 3 vagy 4 vagy 5	
Behatolás jelző rendszer	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
nincsen	0
R8 Részpontszám lehet 0 vagy 1 vagy 2 vagy 3 vagy 4	
F5 V. fejezet pontszáma R7+R8	

VI. fejezet Kerítés	
4. osztályú	4
3. osztályú	3
2. osztályú	2
1. osztályú	1
nincsen	0
R9 Részpontszám lehet 0 vagy 1 vagy 2 vagy 3 vagy 4	
Beléptető rendszer a kerítésnél	
van	1
nincsen	0
R10 Részpontszám lehet 0 vagy 1	
Behatolás jelző rendszer a kerítésnél	
van	2
nincs	0
R11 Részpontszám lehet 0 vagy 2	
Biztonsági világítás	
van	2
nincsen	0
R12 Részpontszám lehet 0 vagy 2	
Zárt láncú kamerarendszer	
van	2
nincsen	0
R13 Részpontszám lehet 0 vagy 2	
F6 VI. fejezet pontszáma (R9 x R10)+R11+R12+R13	
Összes pontszám: F1+F2+F3+F4+F5+F6	