

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

a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól¹

Hatályos: 2009. 03. 01. – 2010. 03. 31.

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 hatósággént 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 erő*: a fizikai biztonság érdekében elrendelt intézkedések végrehajtására kötelezett személyzet, így az őrk, 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. *Rendszer biztonsági 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. *Rendszer üzemeltetési biztonsági felelős*: a rendszer biztonsági 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 tárolhatóak. „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.

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.

Behatolás jelző rendszer

10. § Behatolás jelző rendszert az I. vagy II. osztályú biztonsági területen célszerű alkalmazni. A kiépítés során figyelembe kell venni, hogy a reagáló erőnek a riasztást követően még az előtt a területre kell érnie, hogy a külföldi minősítéssel és jelöléssel ellátott adatokhoz történő hozzáférés megtörténne. Behatolás jelző rendszerek telepíthetők 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 örök, vagy más erre felhatalmazott személyek által;

b) a biztonsági tároló legalább két óránkénti ellenőrzésének biztosítása személyi biztonsági tanúsítvánnyal rendelkező örök, vagy más erre felhatalmazott személyek által;

c) behatolás jelző 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) behatolás jelző 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 behatolás jelző 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 örök, vagy más erre felhatalmazott személyek által,

cb) nyílt tároló helyiség 4 óránkénti ellenőrzése személyi biztonsági tanúsítvánnyal rendelkező örök, 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) használatba vételkor 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 ajtnak 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 körbe hegesztett rácsszerkezet;

b) „Titkos!” minősítésű külföldi minősítéssel és jelöléssel ellátott adatok esetén 90 x 90 mm-es kiosztású, 10 mm átmérőjű köracélból álló, minden pontján körbe hegesztett 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 körbe hegesztett rácsszerkezet.

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

Biztonsági tárolók és záruk

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 záruk

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 záruk

21. § (1) 4. osztályú helyiség falazata, födeme 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, födeme 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, födeme 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, födeme és padozata korlátozott mechanikai ellenállásra képes.

Helyiségekhez tartozó záruk

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, födeme és padozata nagyfokú mechanikai ellenállásra képes. Ajtaja és ablakai (ha vannak) a falazattal egyenértékű ellenállást biztosítanak.

(2) 3. osztályú épület falazata, födeme 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 szármok 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 recepciók alkalmazása által valósul meg. A belépés igazolvány felmutatása mellett történhet.

(4)