**Ez a dokumentum kizárólag tájékoztató jellegű, az intézmények semmiféle felelősséget nem vállalnak a tartalmáért**

►B

# A TANÁCS HATÁROZATA

**(2001. március 19.)**

**a Tanács biztonsági szabályzatának elfogadásáról**

(2001/264/EK)

(HL L 11, 11.4.2001, o. 1)

Módosította:

| | | Hivatalos Lap | | |
|---|---|---|---|---|
| | | Szám | Oldal | Dátum |
| ►M1 | A Tanács határozata 2004/194/EK, (2004. február 10.) | L 63 | 48 | 28.2.2004 |
| ►M2 | A Tanács határozata 2005/571/EK, (2005. július 12.) | L 193 | 31 | 23.7.2005 |
| ►M3 | A Tanács határozata 2005/952/EK, (2005. december 20.) | L 346 | 18 | 29.12.2005 |

▼B

# A TANÁCS HATÁROZATA

**(2001. március 19.)**

**a Tanács biztonsági szabályzatának elfogadásáról**

**(2001/264/EK)**

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Közösséget létrehozó szerződésre és különösen annak 207. cikke (3) bekezdésére,

tekintettel a Tanács eljárási szabályzatának elfogadásáról szóló, 2000. június 5-i 2000/396/EK, ESZAK, Euratom tanácsi határozatra [1] és különösen annak 24. cikkére,

mivel:

(1) A Tanács tevékenységének a bizonyos fokú titoktartást igénylő területeken történő továbbfejlesztése érdekében helyénvaló egy olyan átfogó biztonsági rendszert létrehozni, amely kiterjed a Tanácsra, annak Főtitkárságára és a tagállamokra.

(2) Az ilyen rendszernek egy szövegben kell összefognia az e területre vonatkozó minden korábbi határozat és rendelkezés témáját.

(3) A gyakorlatban a CONFIDENTIEL UE és magasabb minősítésű uniós információk nagyobb része a közös biztonság- és védelmi politikára vonatkozik.

(4) Az így létrehozott biztonsági rendszer eredményességének biztosítása céljából a tagállamoknak részt kell venniük a működésében azáltal, hogy nemzeti intézkedéseket hoznak annak érdekében, hogy e határozat rendelkezéseit betartassák, amikor illetékes hatóságaik és alkalmazottaik EU minősített információkat kezelnek.

(5) A Tanács üdvözli a Bizottság abbéli szándékát, hogy e határozat alkalmazásának időpontjáig a hozzá tartozó mellékleteknek megfelelő átfogó rendszert vezessen be az uniós döntéshozatali folyamat zökkenőmentes működésének biztosítása végett.

(6) A Tanács rámutat annak fontosságára, hogy adott esetben az Európai Parlamentet és a Bizottságot is bevonják az unió és annak tagállamai érdekeinek védelméhez szükséges titoktartási szabályok és előírások alkalmazásába.

(7) Ez a határozat nem érinti a Szerződés 255. cikkét és az azt végrehajtó jogi aktusokat.

(8) Ez a határozat nem érinti a tagállamok fennálló gyakorlatát a nemzeti parlamenteknek az unió tevékenységével kapcsolatos tájékoztatása tekintetében,

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

*1. cikk*

A Tanács a mellékletben foglalt biztonsági szabályzatot jóváhagyja.

*2. cikk*

(1) A főtitkár/főképviselő meghozza a megfelelő intézkedéseket annak érdekében, hogy az EU minősített információk kezelése során az 1. cikkben említett szabályzatot a Tanács Főtitkárságán (a továbbiakban: Főtitkárság) belül a Főtitkárság tisztviselői és egyéb alkalmazottai, külső szerződéses megbízottai, illetve a Főtitkársághoz kirendelt személyzet, továbbá a Tanács helyiségeiben és az EU decentralizált szerveinél [2] betartsák.

---

[1] HL L 149., 2000.6.23., 21. o.

[2] Lásd a Tanács 2000. november 10-i következtetéseit.

▼B

(2) A tagállamok megfelelő, a nemzeti rendelkezéseikkel összhangban lévő intézkedésekkel biztosítják, hogy az EU minősített információk kezelésekor intézményeikben és helyiségeikben az 1. cikkben említett szabályzatot a következők betartsák:

a) a tagállamok Európai Unió melletti állandó képviseleteinek tagjai, valamint a Tanács vagy annak szervei ülésein, illetve a Tanács egyéb tevékenységeiben részt vevő nemzeti küldöttségek tagjai;

b) a tagállamok nemzeti közigazgatásának más tagjai, akik EU minősített információkat kezelnek, akár a tagállamok területén, akár külföldön szolgálnak; és

c) a tagállamok külső szerződéses megbízottai és az általuk kirendelt személyzet, akik EU minősített információkat kezelnek.

A tagállamok kötelesek haladéktalanul értesíteni a Főtitkárságot a meghozott intézkedésekről.

(3) Az (1) és a (2) bekezdésben említett intézkedéseket 2001. november 30. előtt meg kell hozni.

*3. cikk*

A melléklet I. részében foglalt alapelvek és biztonsági minimumszabályok betartásával a főtitkár/főképviselő intézkedéseket hozhat a melléklet II. része I. szakasza 1. és 2. pontjának megfelelően.

*4. cikk*

Alkalmazásának napjától kezdve ez a határozat a következők helyébe lép:

a) a Tanács 1998. április 27-i 98/319/EK határozata a Tanács birtokában lévő minősített információkhoz való hozzáférést a Tanács Főtitkárságának tisztviselői és alkalmazottai részére lehetővé tevő eljárásokról ([1]);

b) a főtitkár/főképviselő 2000. július 27-i határozata a Tanács Főtitkársága tekintetében a minősített információk védelmét szolgáló intézkedésekről ([2]);

c) a Tanács főtitkárának 1997. május 22-i 433/97 határozata a Cortesy-rendszer működéséért felelős személyek biztonsági ellenőrzésének eljárásáról.

*5. cikk*

(1) Ez a határozat kihirdetésének napján lép hatályba.

(2) Ezt a határozatot 2001. december 1-jétől kell alkalmazni.

([1]) HL L 140., 1998.5.12., 12. o.
([2]) HL C 239., 2000.8.23., 1. o.

▼B

*MELLÉKLET*

**AZ EURÓPAI UNIÓ TANÁCSÁNAK BIZTONSÁGI SZABÁLYZATA**

▼B

**TARTALOMJEGYZÉK**

I. RÉSZ

**Alapelvek és biztonsági minimumszabályok**

II. RÉSZ

I. SZAKASZ

A biztonsági szervezet az Európai Unió Tanácsában

II. SZAKASZ

Minősítések és jelölések

III. SZAKASZ

A minősítés szabályai

IV. SZAKASZ

Fizikai biztonság

V. SZAKASZ

A „szükséges ismeret” elvére és a biztonsági ellenőrzésre vonatkozó általános szabályok

VI. SZAKASZ

A Főtitkárság tisztviselőire és egyéb alkalmazottaira vonatkozó biztonsági ellenőrzési eljárás

VII. SZAKASZ

Az EU minősített anyagok előállítása, elosztása, továbbítása, tárolása és megsemmisítése

VIII. SZAKASZ

TRÈS SECRET UE/EU TOP SECRET anyagok nyilvántartó hivatalai

IX. SZAKASZ

A Tanács helyiségein kívül és rendkívül kényes ügyekben tartott különleges ülések esetén alkalmazandó biztonsági intézkedések

X. SZAKASZ

A biztonság megsértése és EU minősített információk illetéktelenek tudomására jutása

XI. SZAKASZ

Az IT-rendszerekben és kommunikációs rendszerekben kezelt információk védelme

XII. SZAKASZ

EU minősített információk átadása harmadik államok vagy nemzetközi szervezetek részére

**Függelékek**

*1. függelék*

A nemzeti biztonsági hatóságok jegyzéke

*2. függelék*

A nemzeti biztonsági minősítések összehasonlító táblázata

*3. függelék*

Gyakorlati minősítési útmutató

*4. függelék*

▼B

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához

— 1. szintű együttműködés

*5. függelék*

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához

— 2. szintű együttműködés

*6. függelék*

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához

— 3. szintű együttműködés

▼B

I. RÉSZ

## ALAPELVEK ÉS BIZTONSÁGI MINIMUMSZABÁLYOK

BEVEZETÉS

1. Ezek a rendelkezések az alapelveket és a biztonság minimumszabályait határozzák meg, melyeket a Tanácsnak, a Tanács Főtitkárságának (a továbbiakban: a Főtitkárság), a tagállamoknak és az Európai Unió decentralizált szerveinek (a továbbiakban: az EU decentralizált szervei) megfelelő módon be kell tartaniuk, hogy a biztonságot megőrizzék, és hogy mindegyik bizonyos lehessen abban, hogy a védelem közös szintje megvalósul.

2. Az „EU minősített információ” olyan információt és anyagot jelent, amelynek engedély nélküli kiszolgáltatása különböző mértékben sértheti az EU-nak, illetve egy vagy több tagállamának az érdekeit, függetlenül attól, hogy az ilyen információ az EU-n belül keletkezett, illetve a tagállamoktól, harmadik államoktól vagy nemzetközi szervezetektől származik.

3. E szabályzat alkalmazásában:

   a) A „dokumentum” kifejezés olyan levelet, feljegyzést, jegyzőkönyvet, jelentést, memorandumot, jelet/üzenetet, vázlatot, fényképet, diát, filmet, térképet, ábrát, tervet, jegyzetfüzetet, stencilt, indigót, írógép- vagy nyomtatószalagot, magnószalagot, kazettát, számítógépes mágneslemezt, CD-ROM-ot vagy más adathordozó eszközt jelent, amelyen információt tárolnak.

   b) Az „anyag” kifejezés az a) pont szerinti „dokumentumot” jelent, továbbá bármely legyártott vagy gyártás alatt álló felszerelési tárgyat.

4. A biztonság terén az elsődleges célok a következők:

   a) az EU minősített információk védelme a kémkedés, az illetéktelenek tudomására jutása vagy az engedély nélküli kiszolgáltatás ellen;

   b) a kommunikációs és információs rendszerekben és hálózatokban kezelt EU információk védelme az integritásukat és rendelkezésre állásukat fenyegető veszélyekkel szemben;

   c) az EU-információknak helyet adó berendezések védelme a szabotázzsal és a szándékos rongálással szemben;

   d) a biztonsági intézkedések kudarca esetén az okozott kár felmérése, a következmények korlátozása és a szükséges korrekciós intézkedések elfogadása.

5. A stabil biztonság alapjai a következők:

   a) Minden egyes tagállamban egy nemzeti biztonsági szervezet, amelynek hatáskörébe az alábbiak tartoznak:

      i. kémkedésre, szabotázsra, terrorizmusra és egyéb felforgató tevékenységekre vonatkozó bűnüldözési operatív információk gyűjtése és nyilvántartása; valamint

      ii. tájékoztatás és tanácsadás a kormány és – ez utóbbi útján – a Tanács számára a biztonságot fenyegető veszélyek természetéről és a védelem velük szemben alkalmazandó eszközeiről.

   b) Minden egyes tagállamban és a Főtitkárságon belül egy technikai INFOSEC-hatóság, amelynek hatáskörébe tartozik, hogy az érintett biztonsági hatósággal együttműködésben tájékoztasson a biztonságot fenyegető technikai veszélyekről és tanácsokat adjon a velük szemben alkalmazandó védelmi intézkedésekről;

   c) a hatóságok, hivatalok és a Főtitkárság megfelelő szolgálatai közötti rendszeres együttműködés, hogy meghatározzák:

      i. a védelemre szoruló információkat, erőforrásokat és berendezéseket; és

▼B

ii. a közös védelmi szabályokat, és adott esetben megfelelő ajánlásokat tegyenek.

6. A titoktartás terén körültekintés és tapasztalat szükséges a védendő információk és anyagok kiválasztása és a szükséges védelem fokának megválasztása során. Alapvető, hogy a védelem foka megfeleljen annak, hogy az egyes védendő információk és anyagok biztonsági szempontból mennyire fontosak. A zavartalan információáramlás biztosítása végett biztosítani kell a túlzottan szigorú minősítések elkerülését. A minősítési rendszer ezen elvek gyakorlatba való átültetésének eszköze. Hasonló minősítési rendszer alkalmazandó a kémkedés, a szabotázs, a terrorizmus és az egyéb veszély leküzdésére szolgáló intézkedések megtervezése és megszervezése során, hogy a minősített információknak helyet adó legfontosabb helyiségek és azokon belül a legérzékenyebb pontok részesüljenek a legmagasabb szintű védelemben.

ALAPELVEK

7. A biztonsági intézkedéseknek:

a) ki kell terjedniük a minősített információkhoz hozzáférni képes személyekre, a minősített információkat hordozó eszközökre, az ilyen információknak helyet adó valamennyi helyiségre és a fontos berendezésekre;

b) ki kell szűrniük azokat a személyeket, akiknek az alkalmazása veszélyeztetheti a minősített információk és az azokat tartalmazó fontos berendezések biztonságát, és rendelkezniük kell ezen személyek kizárásáról vagy eltávolításáról;

c) meg kell akadályozniuk, hogy illetéktelen személyek minősített információkhoz vagy az azokat tartalmazó berendezésekhez hozzáférhessenek;

d) biztosítaniuk kell, hogy a minősített információk elosztása kizárólag a „szükséges ismeret” elve alapján történjék, ami valamennyi biztonsági szempontból alapvető;

e) biztosítaniuk kell az összes – akár minősített, akár nem minősített, és különösen az elektromágneses formában tárolt, kezelt vagy továbbított – információ integritását (vagyis meg kell akadályozniuk azok megrongálódását, illetéktelen módosítását vagy illetéktelen törlését) és rendelkezésre állását (vagyis a hozzáférést nem tagadhatják meg azoktól, akiknek szükségük van arra és a hozzáféréshez felhatalmazással rendelkeznek).

A BIZTONSÁGI SZERVEZET

**Közös minimumszabályok**

8. A Tanács és minden tagállam biztosítja, hogy a biztonság közös minimumszabályait minden közigazgatási és/vagy kormányzati szerv, az EU egyéb intézményei, szervei és szerződéses megbízottai betartsák, hogy a minősített információk azzal a bizalommal kerüljenek átadásra, hogy azokat egyforma elővigyázatossággal kezelik. Ezek a minimumszabályok tartalmazzák a személyzet biztonsági ellenőrzésének kritériumait és az EU minősített információk védelmére irányuló eljárásokat. ►M3 Ezek a minimumszabályok magukban foglalják az abban az esetben alkalmazandó minimumszabályokat is, amikor a Tanács Főtitkársága szerződés útján ipari vagy egyéb szervezeteket bíz meg EU minősített információt magában foglaló, azzal járó és/vagy azt tartalmazó feladatokkal: e minimumszabályokat a II. rész XIII. szakasza tartalmazza. ◄

A SZEMÉLYZET BIZTONSÁGA

**Biztonsági ellenőrzés**

9. Minden olyan személyt, akinek CONFIDENTIEL UE vagy ennél magasabb minősítésű információkhoz kell hozzáférnie, megfelelő biztonsági ellenőrzésnek vetnek alá, mielőtt a hozzáféréshez a felhatalmazást megadnák. Hasonló biztonsági ellenőrzésre van szükség az olyan személyek esetében is, akiknek feladatkörébe a minősített információkat tartalmazó kommunikációs és információs rendszerek technikai üzemeltetése vagy karbantartása

▼B

tartozik. A biztonsági ellenőrzés célja annak megállapítása, hogy az illető személyek:

a) hűsége megkérdőjelezhetetlen-e;

b) jelleme és titoktartási képessége folytán nem férhet-e kétség ahhoz, hogy a minősített információk kezelése során feddhetetlenül járnak el; vagy

c) külföldi vagy más helyről kiinduló nyomásgyakorlás révén esetleg sebezhetők-e, például korábbi lakóhelyük vagy kapcsolataik miatt, amelyek biztonsági kockázatot jelenthetnek.

A biztonsági ellenőrzési eljárás során különösen alapos ellenőrzésnek kell alávetni azokat a személyeket, akik:

d) TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz való hozzáférésre kapnak felhatalmazást;

e) olyan beosztásban dolgoznak, ahol rendszeresen jelentős mennyiségű SECRET UE információhoz férnek hozzá;

f) feladatuk ellátása során különleges hozzáféréssel rendelkeznek valamely feladat szempontjából döntő fontosságú kommunikációs vagy információs rendszerhez, és így lehetőségük van arra, hogy illetéktelenül kerüljenek nagy mennyiségű EU minősített információ birtokába, illetve technikai szabotázscselekmények útján súlyosan ártsanak a feladat ellátásának.

A d), e) és f) pontokban említett esetekben a lehető legteljesebb mértékben alkalmazni kell az előélet lenyomozásának technikáját.

10. Ha valamely személyeket, akiknek nincsen megalapozott szükségük az ismeretre, olyan körülmények között alkalmaznak, ahol EU minősített információkhoz férhetnek hozzá (például futárok, biztonsági alkalmazottak, karbantartó vagy takarítószemélyzet stb.), az ilyen személyeket előzetesen megfelelő biztonsági ellenőrzésnek kell alávetni.

**A személyzeti biztonsági felhatalmazások nyilvántartása**

11. Minden olyan szolgálat, szerv vagy intézmény, amely EU minősített információkat kezel, vagy ahol valamely feladat szempontjából döntő fontosságú kommunikációs vagy információs rendszer van, köteles nyilvántartást vezetni az ott dolgozó személyzet biztonsági felhatalmazásáról. Minden biztonsági felhatalmazást szükség esetén ellenőriznek annak érdekében, hogy megfeleljen az adott személy aktuális feladatával járó kívánalmaknak; a biztonsági felhatalmazás felülvizsgálatának elsődlegességet kell biztosítani minden esetben, ha új információt kapnak arra vonatkozólag, hogy a minősített információkhoz való hozzáféréssel járó munka folytatása nem egyeztethető össze a biztonsági érdekekkel. Az ellenőrzési eredmények nyilvántartását az érintett szolgálat, szerv vagy intézmény biztonsági felelőse kezeli.

**A személyzet biztonsági képzése**

12. Azok a személyek, akiket olyan beosztásban alkalmaznak, amelyben minősített információkhoz férhetnek hozzá, hivatalba lépésükkor, majd rendszeres időközönként valamennyien alapos oktatásban részesülnek a biztonsági intézkedések szükségessége és az ezek megvalósítására irányuló eljárások tekintetében. Hasznos eljárás előírni, hogy az ilyen beosztású személyek írásbeli nyilatkozatot tegyenek, hogy a munkájuk szempontjából fontos biztonsági szabályokat teljes mértékben megértették.

**A vezetők felelőssége**

13. A vezetők kötelezettsége, hogy ismerjék a minősített információkkal dolgozó vagy valamely feladat ellátása szempontjából döntő fontosságú biztonságos kommunikációs vagy információs rendszerekhez hozzáféréssel rendelkező beosztottjaikat, továbbá hogy feljegyezzék és jelentsék azokat az eseményeket vagy nyilvánvalóan gyenge pontokat, amelyek kihatással lehetnek a biztonságra.

**A személyzet biztonsági státusa**

▼B

14. Ki kell alakítani azokat az eljárásokat, amelyek alapján – ha valamely személlyel kapcsolatban kedvezőtlen információ válik ismertté – meg lehet állapítani, hogy az illető személy dolgozik-e minősített információkkal vagy hozzáfér-e valamely feladat ellátása szempontjából döntő fontosságú kommunikációs vagy információs rendszerekhez, és erről az érintett hatóságot tájékoztatni kell. Ha azt állapítják meg, hogy a kérdéses személy biztonsági kockázatot jelent, az illetőt azon feladatokból, amelyek ellátása során a biztonságot veszélyeztetheti, ki kell zárni vagy beosztásából el kell távolítani.

FIZIKAI BIZTONSÁG

**A védelem szükségessége**

15. Az EU minősített információk védelmének biztosítása érdekében alkalmazandó fizikai biztonsági intézkedések mértékének arányosnak kell lennie a birtokolt információk és anyagok minősítésével, mennyiségével és veszélyeztetettségével. Ezért külön gondot kell fordítani arra, hogy a minősítés ne legyen túlzottan enyhe vagy szigorú, és ezért a minősítést rendszeresen felül kell vizsgálni. Az EU minősített információk valamennyi birtokosa egységes gyakorlatot köteles követni az információk minősítése tekintetében és közös védelmi szabályoknak köteles eleget tenni a védelmet igénylő információk és anyagok megőrzése, továbbítása és megsemmisítése tekintetében.

**Ellenőrzés**

16. Az EU minősített információk elhelyezésére szolgáló területek elhagyása előtt a minősített információk biztonságos megőrzéséért felelős személyeknek meg kell győződniük arról, hogy az információk tárolása kellően biztonságos-e és hogy az összes biztonsági berendezést (zárakat, riasztókat stb.) működésbe hozták-e. Munkaidő után további, független ellenőrzéseket kell végezni.

**Az épületek biztonsága**

17. Az EU minősített információk vagy a valamely feladat ellátása szempontjából döntő fontosságú kommunikációs és információs rendszerek elhelyezésére szolgáló épületeket az illetéktelen behatolás ellen védeni kell. Az EU minősített információk számára nyújtott védelem természete – például ablakrácsok, ajtózárak, őrök a bejáratnál, automatikus hozzáférés-ellenőrző rendszerek, biztonsági ellenőrzések és őrjáratok, riasztórendszerek, behatolásjelző rendszerek és őrkutyák – a következőktől függ:

a) a védendő információ és anyag minősítése, mennyisége és elhelyezkedése az épületen belül;

b) az ilyen információkat és anyagokat tartalmazó biztonsági tárolóeszközök minősége,

c) az épület fizikai jellemzői és elhelyezkedése.

18. A kommunikációs és információs rendszerek számára nyújtott védelem jellege hasonlóképpen attól függ, hogy a felmérések szerint milyen eszközérték forog kockán és mekkora a lehetséges kár illetéktelenek tudomászszerzése esetén, továbbá hogy milyenek a rendszer elhelyezésére szolgáló épület fizikai jellemzői és milyen az elhelyezkedése, valamint attól, hogy a rendszer miként van elhelyezve az épületen belül.

**Vészhelyzeti tervek**

19. Előzetesen részletes terveket kell kidolgozni a minősített információk védelmére helyi vagy országos vészhelyzetben.

INFORMÁCIÓBIZTONSÁG (INFOSEC)

20. Az információbiztonság a kommunikációs, információs és egyéb elektronikus rendszerekben kezelt, tárolt vagy továbbított információk titkosságának, integritásának és rendelkezésre állásának – véletlenszerű vagy szándékos cselekedet által okozott – sérülése elleni védelmét szolgáló biztonsági intézkedések meghatározására és alkalmazására vonatkozik. Megfelelő óvin-

▼B

tézkedéseket kell tenni annak érdekében, hogy megelőzzék illetéktelen felhasználók hozzáférését az EU-információkhoz, illetve hogy az arra jogosult felhasználók esetében megelőzzék az EU-információkhoz való hozzáférés megtagadását, továbbá hogy megelőzzék az EU információk megrongálódását, illetéktelen módosítását vagy törlését.

A SZABOTÁZS ÉS A SZÁNDÉKOS RONGÁLÁS MÁS FORMÁI ELLENI VÉDELEM

21. A szabotázzsal és a szándékos rongálással szembeni leghatásosabb biztosítékot a minősített információk elhelyezésére szolgáló fontos berendezések védelmére irányuló fizikai óvintézkedések jelentik, és ezeket a személyzet biztonsági ellenőrzése önmagában nem helyettesítheti. Az illetékes nemzeti szerv feladata, hogy bűnüldözési operatív információkat gyűjtsön a kémkedésről, a szabotázsról, a terrorizmusról és az egyéb felforgató tevékenységekről.

MINŐSÍTETT INFORMÁCIÓK ÁTADÁSA HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE

22. A Tanácstól származó EU minősített információk harmadik állam vagy nemzetközi szervezet részére történő átadásáról szóló határozatot csak a Tanács hozhatja meg. Ha az átadni kért információ kibocsátója nem a Tanács, akkor a Tanács először a kibocsátó beleegyezését kéri ki az információ átadásához. Ha a kibocsátó kiléte nem állapítható meg, helyette a Tanács határoz.

23. Ha a Tanács valamely harmadik államtól, nemzetközi szervezettől vagy más harmadik felektől kap minősített információt, akkor ez az információ a minősítésének megfelelő és az e szabályzatban az EU minősített információkra nézve megállapított szinttel egyenértékű, vagy az információt átadó harmadik fél által esetleg előírt ennél magasabb szintű védelemben részesül. Kölcsönös ellenőrzésekről meg lehet állapodni.

24. A fenti elvek alkalmazása a II. részben meghatározott részletes rendelkezéseknek megfelelően történik.

▼B

II. RÉSZ

I. SZAKASZ

## A BIZTONSÁGI SZERVEZET AZ EURÓPAI UNIÓ TANÁCSÁBAN

### A főtitkár/főképviselő

1. A főtitkár/főképviselő:

   a) végrehajtja a Tanács biztonsági politikáját;

   b) foglalkozik a Tanács vagy annak illetékes szervei által elé terjesztett biztonsági problémákkal;

   c) a tagállamok nemzeti biztonsági (vagy egyéb illetékes) hatóságaival szoros kapcsolatot tartva megvizsgálja a Tanács biztonsági politikájának megváltoztatását szükségessé tevő kérdéseket. Az 1. függelék tartalmazza e hatóságok jegyzékét.

2. A főtitkár/főképviselő különösen a következőkért felel:

   a) a Tanács tevékenységével összefüggő valamennyi, biztonsággal kapcsolatos ügy összehangolása;

   b) felkérés megtétele, hogy minden tagállam hozzon létre egy központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalt, és adott esetben annak megkövetelése, hogy ilyen nyilvántartó hivatalt az EU decentralizált szerveinél is hozzanak létre;

   c) megkeresés intézése a tagállamok kijelölt hatóságaihoz, hogy a nemzeti biztonsági hatóság a VI. szakaszban foglaltaknak megfelelően végezze el a Tanácsnál alkalmazott személyzet biztonsági ellenőrzését;

   d) olyan esetek kivizsgálása vagy kivizsgáltatása, amikor minősített EU-információk szivárogtak ki, ha a jelek arra utalnak, hogy ennek oka a Főtitkárságon vagy az EU egyik decentralizált szervénél keresendő;

   e) az illetékes biztonsági hatóságok felkérése vizsgálatok indítására, amikor EU minősített információk szivárogtak ki, de úgy tűnik, nem a Főtitkárságról vagy az EU decentralizált szerveitől; továbbá a vizsgálatok összehangolása, ha azokban több biztonsági hatóság vesz részt;

   f) az EU minősített információk védelmére a tagállamokban alkalmazott biztonsági intézkedések rendszeres időközönként történő vizsgálata az érintett nemzeti biztonsági hatóságokkal közösen és egyetértésben;

   g) szoros kapcsolat fenntartása az összes érintett biztonsági hatósággal a biztonsági intézkedések átfogó összehangolásának megvalósítása érdekében;

   h) a Tanács biztonsági politikájának és eljárásainak folyamatos felülvizsgálata, és adott esetben megfelelő ajánlások kidolgozása. E tekintetben beterjeszti a Tanács elé a Főtitkárság Biztonsági Hivatala által elkészített éves ellenőrzési tervet.

### A Tanács Biztonsági Bizottsága

3. Létrejön a Biztonsági Bizottság. Ez a szerv az egyes tagállamok nemzeti biztonsági hatóságainak a képviselőiből áll. Elnöki tisztét a főtitkár/főképviselő vagy annak megbízottja látja el. A megfelelő EU decentralizált szervek képviselői is meghívást kaphatnak, ha őket érintő kérdéseket vitatnak meg.

4. A Biztonsági Bizottság üléseit a Tanács utasítására, a főtitkár/főképviselő vagy valamely nemzeti biztonsági hatóság kérésére tartja. A bizottság jogosult megvizsgálni és értékelni a Tanács munkájával kapcsolatban felmerült bármely biztonsági kérdést, és szükség esetén ajánlásokat terjeszteni a Tanács elé. A Tanács Főtitkárságának tevékenysége tekintetében a bizottság jogosult a biztonsági kérdésekkel kapcsolatos ajánlásokat tenni a főtitkárnak/főképviselőnek.

### A Tanács Főtitkárságának Biztonsági Hivatala

▼B

5. Az 1. és 2. pontban említett feladatok teljesítése érdekében a Főtitkárság Biztonsági Hivatala a főtitkár/főképviselő rendelkezésére áll a biztonsági intézkedések összehangolása, felügyelete és végrehajtása végett.

6. A Főtitkárság Biztonsági Hivatalának vezetője biztonsági ügyekben a főtitkár/főképviselő legfontosabb tanácsadója és egyben a Biztonsági Bizottság titkára. E minőségében irányítja a biztonsági előírások naprakésszé tételét, valamint összehangolja a biztonsági intézkedéseket a tagállamok illetékes hatóságaival és adott esetben azokkal a nemzetközi szervezetekkel, amelyek a Tanáccsal biztonsági megállapodásokat kötöttek. Ennek érdekében összekötő tisztviselőként jár el.

7. A Tanács Biztonsági Hivatalának vezetője felelős a Főtitkárságon belüli IT-rendszerek és -hálózatok akkreditációjáért. Adott esetben a Főtitkárság Biztonsági Hivatalának vezetője és az érintett nemzeti biztonsági hatóságok együtt határoznak a Főtitkárságot, a tagállamokat, az EU decentralizált szerveit és/vagy harmadik feleket (államokat vagy nemzetközi szervezeteket) összekapcsoló IT-rendszerek és -hálózatok akkreditációjáról.

**Az EU decentralizált szervei**

8. Az EU decentralizált szerveinek minden vezetője felelős a biztonsági szabályok intézményén belüli végrehajtásáért. Rendszerint kijelöli személyzete valamely tagját, aki e területért neki felelősséggel tartozik. Ezt a személyt nevezik ki biztonsági tisztviselőnek.

**Tagállamok**

9. Minden tagállam kijelöli azt a nemzeti biztonsági hatóságot, amely az EU minősített információkért felel ([1]).

10. Az egyes tagállamok közigazgatásának keretén belül a megfelelő nemzeti biztonsági hatóság a következőkért felel:

    a) bármely nemzeti hatóság, szerv, illetve köz- vagy magánintézmény által belföldön vagy külföldön kezelt minősített EU-információk biztonságának a megőrzéséért;

    b) a TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalok létesítésének engedélyezéséért (ez a jogkör átruházható valamely központi nyilvántartó hivatal TRÈS SECRET UE/EU TOP SECRET ellenőrző tisztviselőjére);

    c) az EU minősített információk védelmét szolgáló biztonsági intézkedések rendszeres időközönkénti ellenőrzéséért;

    d) annak biztosításáért, hogy a nemzeti hatóságoknál, szerveknél vagy intézményeknél alkalmazott állampolgárok és külföldiek, akik TRÈS SECRET UE/EU TOP SECRET, SECRET UE és CONFIDENTIEL UE szintű minősített EU-információt kezelnek, előzőleg biztonsági ellenőrzésen essenek át;

    e) olyan biztonsági tervek kidolgozásáért, amelyeket szükségesnek ítélnek annak megakadályozására, hogy az EU minősített információk illetéktelen személyek kezébe kerülhessenek.

**Kölcsönös biztonsági ellenőrzések**

11. A Főtitkárság Biztonsági Hivatala és az érintett nemzeti biztonsági hatóság együttesen és kölcsönös egyetértésben, rendszeres időközönként ellenőrzi az EU minősített információk védelmét szolgáló biztonsági intézkedéseket a Főtitkárságon és a tagállamoknak az Európai Unió mellett működő állandó képviseletein, illetve a tagállamoknak a Tanács épületeiben található helyiségeiben ([2]).

12. Az EU decentralizált szerveinél az EU minősített információk védelmét szolgáló biztonsági intézkedéseket a Főtitkárság Biztonsági Hivatala vagy

([1]) Az EU minősített információkért felelős nemzeti biztonsági hatóságok jegyzékét az 1. függelék tartalmazza.

([2]) A diplomáciai kapcsolatokról szóló 1961. évi bécsi egyezmény sérelme nélkül.

▼B

– a Főtitkár kérésére – a fogadó tagállam nemzeti biztonsági hatósága ellenőrzi.

▼B

II. SZAKASZ

## MINŐSÍTÉSEK ÉS JELÖLÉSEK

MINŐSÍTÉSI SZINTEK ([1])

Az információk minősítése a következő szintek szerint történik:

1. TRÈS SECRET UE/EU TOP SECRET: ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása rendkívül súlyosan sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit.

2. SECRET UE: ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása súlyosan sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit.

3. CONFIDENTIEL UE: ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit.

4. RESTREINT UE: ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása hátrányosan érinthetné az Európai Unió, illetve egy vagy több tagállama érdekeit.

JELÖLÉSEK

5. Figyelmeztető jelölést lehet használni a dokumentum által érintett terület vagy valamilyen, a szükséges ismeret elve alapján történő különleges elosztás meghatározására.

6. ESDP/PESD (= EBVP) jelöléssel látják el azokat a dokumentumokat és azok másolatait, amelyek az unió, illetve egy vagy több tagállama biztonságával és védelmével kapcsolatosak, továbbá amelyek a katonai vagy nem katonai válságkezelésre vonatkoznak.

7. Bizonyos dokumentumokat, nevezetesen információtechnológiai (IT) rendszerekre vonatkozó dokumentumokat, további olyan jelelölésekkel is el lehet látni, amelyek a megfelelő szabályzatokban meghatározott kiegészítő biztonsági intézkedéseket vonnak maguk után.

A MINŐSÍTÉSEK ÉS A JELÖLÉSEK FELTÜNTETÉSE

8. A minősítéseket és a jelöléseket a következőképpen kell feltüntetni a dokumentumokon:

   a) a RESTREINT UE minősítésű dokumentumokon mechanikus vagy elektronikus eszközökkel;

   b) a CONFIDENTIEL UE minősítésű dokumentumokon mechanikus eszközökkel és kézzel, illetve előre lebélyegzett, regisztrált papírra történő nyomtatással;

   c) a SECRET UE és a TRÈS SECRET UE/EU TOP SECRET minősítésű dokumentumokon mechanikus eszközökkel és kézzel.

([1]) Az EU, a NATO, a NYEU és a tagállamok biztonsági minősítéseinek összehasonlító táblázatát a 2. függelék tartalmazza.

▼B

III. SZAKASZ

## A MINŐSÍTÉS SZABÁLYAI

1. Az információk csak akkor kapnak minősítést, ha ez szükséges. A minősítést világosan és szabályosan kell jelölni és a minősítés csak addig tartható fenn, amíg az információk védelemre szorulnak.

2. Az információ minősítése és későbbi visszaminősítése vagy a minősítés megszüntetése ([1]) kizárólag a kibocsátó feladata.

   A Főtitkárság tisztviselői és egyéb alkalmazottai csak főigazgatójuk utasítására vagy vele egyetértésben végzik el az információk minősítését, illetve minősítik azokat vissza vagy szüntetik meg minősítésüket.

3. A minősített dokumentumok kezelésére vonatkozó részletes eljárásokat úgy alakították ki, hogy a bennük foglalt információknak megfelelő védelmük biztosítva legyen.

4. A TRÈS SECRET UE/EU TOP SECRET dokumentumok kibocsátására felhatalmazott személyek számát a lehető legkisebbre kell korlátozni, és nevükről listát kell összeállítani, amelyet a Főtitkárság, az egyes tagállamok és adott esetben az EU decentralizált szerve vezet.

MINŐSÍTÉSEK ALKALMAZÁSA

5. Valamely dokumentum minősítését aszerint kell meghatározni, hogy tartalma a II. szakasz 1-4. pontjában foglalt meghatározásnak megfelelően milyen mértékű védelmet igényel. Fontos, hogy a minősítést szabályosan és mértéktartással használják. Ez különösen a TRÈS SECRET UE/EU TOP SECRET minősítés esetére vonatkozik.

6. A minősítendő dokumentum kibocsátójának szem előtt kell tartania a fenti szabályokat, és el kell kerülnie mind a felülminősítés, mind az alulminősítés irányába történő elmozdulást.

   Noha első látásra úgy tűnhet, hogy egy magasabb szintű minősítés a dokumentumnak nagyobb védelmet nyújt, a rutinszerűvé váló túlzottan szigorú minősítés megrendítheti a minősítési rendszer érvényességébe vetett bizalmat.

   Másrészt viszont a védelemmel kapcsolatos korlátozások elkerülése érdekében tilos valamely dokumentumot túl alacsony minősítéssel ellátni.

   A minősítésre vonatkozó gyakorlati útmutatót a 3. függelék tartalmazza.

7. Egy adott dokumentum egyes oldalai, bekezdései, szakaszai, mellékletei, függelékei, toldalékai és csatolmányai eltérő minősítést igényelhetnek, és ennek megfelelő jelölést kell kapniuk. A dokumentum egésze a legszigorúbban minősített rész minősítését kapja.

8. A csatolmányokat kísérő levél vagy feljegyzés ugyanolyan szigorú minősítést kap, mint a legszigorúbb minősítésű csatolmánya. A kibocsátónak világosan jeleznie kell, hogy a kísérő levél vagy feljegyzés milyen szintű minősítést kapjon, ha a csatolmányaitól elválasztják.

VISSZAMINŐSÍTÉS ÉS A MINŐSÍTÉS MEGSZÜNTETÉSE

9. EU minősített dokumentumokat csak a kibocsátó engedélyével lehet visszaminősíteni, vagy azok minősítését megszüntetni, szükség esetén az érdekelt felekkel történt egyeztetés után. A visszaminősítést, illetve a minősítés megszüntetését írásban kell megerősíteni. A dokumentumot kibocsátó intézmény, tagállam, hivatal, jogutód szervezet vagy felsőbb hatóság feladata a címzetteket tájékoztatni a minősítés megváltozásról, akiknek viszont azokat a további címzetteket kell tájékoztatniuk erről, akiknek ők a dokumentumot megküldték vagy lemásolták.

([1]) Visszaminősítés (downgrading, déclassement) a minősítési szint leszállítását jelenti; a minősítés megszüntetése (declassification, déclassification) mindenféle minősítés megszüntetését jelenti.

▼B

10. Ha lehetséges, a kibocsátók a minősített dokumentumokon meghatározzák azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalom visszaminősíthető vagy minősítése megszüntethető. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása érdekében, hogy az eredeti minősítés továbbra is szükséges-e.

▼B

IV. SZAKASZ

**FIZIKAI BIZTONSÁG**

ÁLTALÁNOS ISMERTETÉS

1. A fizikai biztonsági intézkedések fő célja megakadályozni, hogy illetéktelen személyek az EU minősített dokumentumokhoz és/vagy anyagokhoz hozzáférjenek.

BIZTONSÁGI KÖVETELMÉNYEK

2. Megfelelő fizikai biztonsági intézkedésekkel kell védeni mindazokat a helyiségeket, területeket, épületeket, irodákat, kommunikációs és információs rendszereket stb., ahol EU minősített információkat és anyagokat tárolnak és/vagy kezelnek.

3. A fizikai biztonságot jelentő védelem szükséges mértékének meghatározásánál minden vonatkozó tényezőt figyelembe kell venni. Ilyenek például:

   a) az információk és/vagy anyagok minősítése;

   b) a tárolt információk mennyisége és formája (például papíralapú vagy számítógépes adathordozó);

   c) az EU, a tagállamok és/vagy EU minősített információkat birtokukban tartó más intézmények vagy harmadik felek ellen irányuló titkosszolgálati fenyegetés, valamint különösen a szabotázs, a terrorizmus és az egyéb felforgató tevékenységek és/vagy bűncselekmények helyi értékelése.

4. Az alkalmazott fizikai biztonsági intézkedések a következőkre irányulnak:

   a) illetéktelen személyek titokban történő vagy erőszakos behatolásának megakadályozása;

   b) a hűtlen személyzet (belső kém) cselekményeinek elrettentése, megakadályozása és felderítése;

   c) annak megakadályozása, hogy a Főtitkárság, a tagállamok kormányszervei és/vagy egyéb intézmények vagy harmadik felek tisztviselői és egyéb alkalmazottai, akiknek nincs szükségük az ismeretre, az EU minősített információkhoz hozzáférjenek.

FIZIKAI BIZTONSÁGI INTÉZKEDÉSEK

**Biztonsági területek**

5. Azokat a területeket, ahol CONFIDENTIEL UE vagy ennél szigorúbb minősítésű információkat kezelnek és tárolnak, úgy kell kialakítani és strukturálni, hogy az alábbi osztályok valamelyikének megfeleljenek:

   a) I. osztályba tartozó biztonsági terület: ahol CONFIDENTIEL UE vagy ennél szigorúbb minősítésű információkat kezelnek és tárolnak olyan módon, hogy a területre való belépés gyakorlatilag a minősített információkhoz való hozzáférést jelent. Ilyen terület esetében a következők szükségesek:

      i. világosan meghatározott és védett körzet, amelynek valamennyi ki- és bejáratát ellenőrzik;

      ii. belépés-ellenőrző rendszer, amely csak a kellőképpen ellenőrzött és különleges felhatalmazással rendelkező személyeknek engedi meg a területre történő belépést;

      iii. a területen rendszerint őrzött információk minősítésének pontos meghatározása, vagyis azoké az információké, amelyekhez a belépés hozzáférést biztosít.

   b) II. osztályba tartozó biztonsági terület: ahol CONFIDENTIEL UE vagy ennél szigorúbb minősítésű információkat kezelnek és tárolnak olyan módon, hogy belső ellenőrzésekkel meg lehessen védeni azokat illetéktelen személyek hozzáférésével szemben, például az olyan irodahelyiség-

▼B

eknek helyt adó épületek, ahol CONFIDENTIEL UE vagy ennél szigorúbb minősítésű információkat kezelnek és tárolnak rendszeresen. Ilyen terület esetében a következők szükségesek:

i. világosan meghatározott és védett körzet, amelynek valamennyi ki- és bejáratát ellenőrzik;

ii. belépés-ellenőrző rendszer, amely csak a kellőképpen ellenőrzött és különleges felhatalmazással rendelkező személyeknek engedi meg, hogy kíséret nélkül a területre lépjenek. Minden más személy esetében kíséretről vagy azzal egyenértékű egyéb ellenőrzésről gondoskodnak, hogy megakadályozzák a jogosulatlan hozzáférést az EU minősített információkhoz és a technikai biztonsági ellenőrzés alá tartozó területekre való ellenőrizetlen belépést.

Azokat a területeket, ahol nem tartózkodik napi 24 órán át munkavégző személyzet, a rendes munkaidő után azonnal ellenőrizni kell annak megállapítása céljából, hogy az EU minősített információkat megfelelően biztonságba helyezték-e.

**Igazgatási terület**

6. Az I. vagy II. osztályba tartozó biztonsági területek körül vagy a hozzájuk vezető területen alacsonyabb biztonsági fokozatú igazgatási terület alakítható ki. Az ilyen területek láthatóan elhatárolt körzetet igényelnek, amely lehetővé teszi a személyzet és a járművek ellenőrzését. Ilyen igazgatási területeken csak RESTREINT UE információkat szabad kezelni és tárolni.

**A be- és kilépés ellenőrzése**

7. Az I. és II. osztályba tartozó biztonsági területekre való belépést az állandó személyzet vonatkozásában alkalmazandó beléptető vagy személyfelismerő rendszerrel kell ellenőrizni. A látogatók ellenőrzésére olyan rendszert kell kialakítani, amely megakadályozza az EU minősített információkhoz való jogosulatlan hozzáférést. A belépő felmutatásán alapuló beléptető rendszereket automatizált személyazonosító eszközök támogathatják, ám ezek csak segíthetik, de nem helyettesíthetik teljes mértékben az őröket. A fenyegetettség értékelésében bekövetkező változás a belépés és kilépés során alkalmazott ellenőrzési intézkedések szigorítását vonhatja maga után, például magas rangú személyiségek látogatása esetén.

**Őrjáratok**

8. Az I. és II. osztályba tartozó biztonsági területeken a rendes munkaidőn kívül őrjárati szolgálatot kell teljesíteni, hogy az EU információit és eszközeit illetéktelen személyek tudomására jutásától, a megrongálódástól vagy az elveszéstől megvédjék. Az őrjáratok gyakoriságát a helyi körülmények határozzák meg, de általános szabályként kétóránként kell ismétlődniük.

**Biztonsági tárolóeszközök és páncélszobák**

9. Az EU minősített információk tárolására háromféle tárolóeszköz-osztály használatos:

— A osztály: az I. vagy II. osztályba tartozó biztonsági területen TRÈS SECRET UE/EU TOP SECRET minősítésű információk tárolására nemzeti szinten jóváhagyott tárolóeszközök,

— B osztály: az I. vagy II. osztályba tartozó biztonsági területen SECRET UE és CONFIDENTIEL UE információk tárolására nemzeti szinten jóváhagyott tárolóeszközök,

— C osztály: csak RESTREINT UE információk tárolására alkalmas irodai bútorok.

10. Az I. vagy II. osztályba tartozó biztonsági területen kiépített páncélszobák, továbbá minden olyan, I. osztályba tartozó biztonsági terület esetében, ahol CONFIDENTIEL UE és ennél szigorúbb minősítésű információkat szabad polcon tárolnak vagy ábrákon, térképeken stb. mutatnak be, egy nemzeti biztonsági hatóságnak igazolnia kell, hogy a falak, a padlózat és a mennyezet, a zárral (zárakkal) felszerelt ajtó (ajtók) az ugyanilyen minősí-

▼B

tésű információk tárolására jóváhagyott biztonsági tárolóeszköz-osztállyal egyenértékű védelmet biztosítanak.

**Zárak**

11. Az EU minősített információk tárolására szolgáló biztonsági tárolóeszközökre és páncélszobákra felszerelt záraknak a következő követelményeknek kell megfelelniük:

— A csoport: nemzeti szinten A osztályú tárolóeszközökre jóváhagyott,

— B csoport: nemzeti szinten B osztályú tárolóeszközökre jóváhagyott,

— C csoport: csak C. osztályú irodai bútoroknál alkalmazható zárak.

**A kulcsok és kombinációk ellenőrzése**

12. A biztonsági tárolóeszközök kulcsait nem szabad kivinni az irodaépületből. A biztonsági tárolóeszközök kombinációit kívülről meg kell tanulniuk azoknak a személyeknek, akiknek azokat ismerniük kell. Vészhelyzet esetén való felhasználás érdekében az érintett szervezeti egység helyi biztonsági tisztviselője felelős a tartalékkulcsok és valamennyi kombináció írásos jegyzékének őrzéséért. Ez utóbbiakat külön lepecsételt, nem átlátszó borítékokban kell elhelyezni. A munka során használt kulcsokat, a tartalékkulcsokat és a kombinációkat külön biztonsági tárolóeszközökben kell őrizni. Ezeknek a kulcsoknak és kombinációknak legalább olyan szigorú biztonsági védelmet kell biztosítani, mint annak az anyagnak, amely használatukkal hozzáférhetővé válik.

13. Azon személyek körét, akik a biztonsági tárolóeszközök felnyitásához szükséges kombinációkat ismerik, a lehető legszűkebbre kell korlátozni. Új kombinációkat az alábbi esetekben kell beállítani:

a) új tárolóeszköz átvételekor;

b) a felhasználók minden változásakor;

c) ha azok ténylegesen illetéktelen személyek tudomására jutottak vagy ennek gyanúja merült fel;

d) lehetőleg hathavonta, de legalább tizenkét havonta.

**Behatolásjelző berendezések**

14. Ha az EU minősített információk védelmére riasztórendszereket, zártláncú televíziót és egyéb elektromos készüléket alkalmaznak, tartalék áramforrásnak kell rendelkezésre állnia a rendszer folyamatos működésének biztosításához arra az esetre, ha a hálózati áramellátás megszakad. További alapkövetelmény, hogy e rendszerek működési zavara vagy hatástalanítási kísérlet esetén a rendszer riassza, vagy egyéb megbízható módon figyelmeztesse a felügyeletet ellátó személyzetet.

**Jóváhagyott berendezések**

15. A nemzeti biztonsági hatóságok egyedül vagy egy másik ország szolgálatával közösen típus és modell szerint naprakész listákat vezetnek azokról a biztonsági berendezésekről, amelyeket különböző meghatározott körülmények között és feltételek mellett minősített információk közvetlen vagy közvetett védelméhez jóváhagytak. A Főtitkárság Biztonsági Hivatala ugyancsak vezet egy hasonló listát, amely többek között a nemzeti biztonsági hatóságok által szolgáltatott információkon alapul. Ilyen berendezések beszerzése előtt az EU decentralizált szervei konzultálnak a Főtitkárság Biztonsági Hivatalával, illetve adott esetben a fogadó tagállamuk nemzeti biztonsági hatóságával.

**A másológépek és telefaxok fizikai védelme**

16. A másológépeket és telefaxokat olyan mértékű fizikai védelemben kell részesíteni, hogy csak az arra felhatalmazott személyek használhassák őket, továbbá hogy valamennyi előállított minősített anyag megfelelő ellenőrzés alá kerüljön.

RÁLÁTÁS ÉS LEHALLGATÁS ELLENI VÉDELEM

▼B

**Rálátás**

17. Nappal és éjjel minden szükséges intézkedést meg kell tenni annak biztosítása érdekében, hogy illetéktelen személyek EU minősített információkat még véletlenül se láthassanak meg.

**Lehallgatás**

18. Azokat az irodákat, illetve területeket, ahol SECRET UE és ennél szigorúbb minősítésű információkat rendszeresen megtárgyalnak, védelemben kell részesíteni a passzív és aktív lehallgatással szemben, ha ennek kockázata felmerül. Az ilyen lehallgatási kísérletek kockázatának értékelése az illetékes biztonsági hatóság feladata, szükség esetén a nemzeti biztonsági hatóságokkal folytatott konzultációt követően.

19. A passzív lehallgatásnak kitett helyiségekben alkalmazandó védelmi intézkedések (például a falak, ajtók, padlózat és mennyezet hangszigetelése, a kiszűrődő hangok erősségének mérése), illetve az aktív lehallgatásnak kitett helyiségekben alkalmazandó védelmi intézkedések (pl. mikrofonok felkutatása) meghatározásához a Főtitkárság a nemzeti biztonsági hatóságok szakértőinek segítségét kérheti. Az EU decentralizált szerveinek biztonsági tisztviselői kérhetik, hogy a Főtitkárság Biztonsági Hivatala technikai ellenőrzéseket végezzen és/vagy a nemzeti biztonsági hatóságok szakértői segítséget nyújtsanak számukra.

20. Hasonlóképpen, ha a körülmények indokolják, az illetékes biztonsági tisztviselő kérésére a nemzeti biztonsági hatóságok technikai biztonsági szakemberei ellenőrizhetik a távközlési berendezéseket és a SECRET UE és annál magasabb szintű ülések során használt bármilyen elektromos vagy elektronikus irodai berendezéseket.

TECHNIKAILAG BIZTONSÁGOS TERÜLETEK

21. Bizonyos területek technikailag biztonságos területként jelölhetők ki. Itt a belépéskor különleges ellenőrzést végeznek. Ha senki sem tartózkodik ott, ezeket a területeket valamilyen jóváhagyott módszerrel lezárva tartják és az összes kulcsot biztonsági kulcsként kezelik. Ezeken a területeken rendszeres fizikai ellenőrzést végeznek, amelyet akkor is lefolytatnak, ha illetéktelen belépés történt vagy annak gyanúja merült fel.

22. A technikai berendezésekről és a bútorokról részletes leltárt kell készíteni, hogy azok mozgatását nyomon lehessen követni. Bútor vagy technikai berendezés ilyen területre csak akkor vihető be, ha a különlegesen képzett biztonsági személyzet a lehallgatókészülékek felderítése érdekében gondosan átvizsgálta. Általános szabály, hogy a technikailag biztonságos területeken távközlési vezetékek telepítését kerülni kell.

▼B

V. SZAKASZ

**A „SZÜKSÉGES ISMERET” ELVÉRE ÉS A BIZTONSÁGI ELLENŐRZÉSRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK**

1. Az EU minősített információkhoz való hozzáférést csak azoknak engedélyezik, akiknek feladataik vagy megbízatásuk ellátásához az információkat ismerniük szükséges. A TRÈS SECRET UE/EU TOP SECRET, SECRET UE és CONFIDENTIEL UE információkhoz való hozzáférést csak azon személyek számára engedélyezik, akiknek a megfelelő biztonsági ellenőrzése megtörtént.

2. Annak megállapítása, hogy kinek mit szükséges ismernie, a Főtitkárságnak, az EU decentralizált szervének, illetve a tagállamok azon szolgálatának vagy hatóságának a feladata, ahol az érintett személyt alkalmazni kívánják.

3. A személyzet ellenőrzése a tisztviselő munkáltatójának a kötelezettsége, és a vonatkozó alkalmazandó eljárások szerint történik. A Főtitkárság tisztviselői és egyéb alkalmazottai tekintetében a biztonsági ellenőrzési eljárásról a VI. szakasz rendelkezik.

   Az eljárás eredményeképpen kiállításra kerül a „biztonsági tanúsítvány”, amelyen feltüntetik a minősített információknak azt a szintjét, amelyhez az ellenőrzött személy hozzáférhet, továbbá azt az időpontot, amikor a tanúsítvány érvényességi ideje lejár.

   Egy adott minősítési szintre szóló biztonsági tanúsítvány birtokosa számára a kevésbé szigorú minősítésű információhoz is hozzáférést biztosíthat.

4. A Főtitkárság vagy a tagállamok tisztviselőin vagy egyéb alkalmazottain kívül az olyan személyeknek, akikkel esetleg szükséges lehet EU minősített információkat megtárgyalni, vagy akik részére szükséges lehet ilyen információkba betekintést biztosítani – például az EU-intézmények tagjainak, tisztviselőinek vagy alkalmazottainak – az EU minősített információk tekintetében biztonsági ellenőrzésen kell átesniük, és tájékoztatni kell őket a biztonsággal kapcsolatos kötelezettségeikről. Ugyanez a szabályt kell alkalmazni – hasonló körülmények között – a külső szerződéses megbízottakra, a szakértőkre és a tanácsadókra is.

A TRÈS SECRET UE/EU TOP SECRET MINŐSÍTÉSŰ INFORMÁCIÓKHOZ VALÓ HOZZÁFÉRÉS KÜLÖNÖS SZABÁLYAI

5. Mindazokat a személyeket, akiknek TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz kell hozzáférniük, előbb biztonsági ellenőrzésnek kell alávetni az ilyen információkhoz való hozzáférés tekintetében.

6. Mindazokat a személyeket, akiknek TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz kell hozzáférniük, hivatali vezetőjük jelöli ki, és nevüket a megfelelő TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalban nyilván kell tartani.

7. A TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz való hozzáférés előtt mindenkinek alá kell írnia egy nyilatkozatot arról, hogy kioktatták a Tanács biztonsági eljárásairól és hogy teljes mértékben megértette a TRÈS SECRET UE/EU TOP SECRET minősítésű információk megőrzésével kapcsolatos különleges felelősségét, valamint azokat a következményeket, amelyeket az EU szabályai és a nemzeti jog vagy a közigazgatási szabályok írnak elő, ha minősített információk szándékosan vagy gondatlanságból illetéktelen személyek kezébe kerülnek.

8. Olyan személy esetében, aki üléseken stb. jut TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz, az illető személyt alkalmazó szolgálat vagy szerv illetékes ellenőrző tisztviselője értesíti az ülést szervező szolgálatot arról, hogy az érintett személy rendelkezik megfelelő felhatalmazással.

9. A TRÈS SECRET UE/EU TOP SECRET listáról törölni kell azoknak a személyeknek a nevét, akiket a továbbiakban nem alkalmaznak TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz való hozzáférést igénylő feladatokra. Ezen túlmenően az ilyen személyeknek újból fel kell hívni a figyelmét a TRÈS SECRET UE/EU TOP SECRET minősítésű információk megőrzésére vonatkozó felelősségükre. Továbbá alá kell írniuk

▼B

egy arra vonatkozó nyilatkozatot, hogy a birtokukban lévő TRÈS SECRET UE/EU TOP SECRET minősítésű információkat nem használják föl, és nem adják tovább.

A SECRET UE ÉS A CONFIDENTIEL UE INFORMÁCIÓKHOZ VALÓ HOZZÁFÉRÉS KÜLÖNÖS SZABÁLYAI

10. Mindazokat a személyeket, akiknek SECRET UE vagy CONFIDENTIEL UE információkhoz kell hozzáférniük, először megfelelő szintű biztonsági ellenőrzésnek kell alávetni.

11. Mindazokkal a személyekkel, akiknek SECRET UE vagy CONFIDENTIEL UE információkhoz kell hozzáférniük, meg kell ismertetni a megfelelő biztonsági szabályokat, és tudatában kell lenniük a gondatlanság következményeinek.

12. Olyan személy esetében, aki üléseken stb. jut SECRET UE vagy CONFIDENTIEL UE információkhoz, az illető személyt alkalmazó szerv illetékes ellenőrző tisztviselője értesíti az ülést szervező szolgálatot arról, hogy az érintett személy rendelkezik megfelelő felhatalmazással.

A RESTREINT UE INFORMÁCIÓKHOZ VALÓ HOZZÁFÉRÉS KÜLÖNÖS SZABÁLYAI

13. A RESTREINT UE információkhoz hozzáféréssel rendelkező személyek figyelmét fel kell hívni ezekre a biztonsági szabályokra és a gondatlanság következményeire.

ÁTHELYEZÉSEK

14. Ha a személyi állomány valamely tagját olyan beosztásból helyezik át, amely EU minősített információk kezelésével jár, a nyilvántartó hivatal nyomon követi a vonatkozó anyagok szabályos átadását a távozó és a hivatalba lépő tisztviselő között.

KÜLÖNLEGES UTASÍTÁSOK

15. Azoknak a személyeknek a figyelmét, akiknek EU minősített információkat kell kezelniük, feladataik megkezdésekor és azt követően rendszeres időközönként a következőkre kell felhívni:

a) az indiszkrét társalgásból származó biztonsági veszélyek;

b) a sajtóval fenntartott kapcsolataikban megteendő elővigyázatossági intézkedések;

c) az EU és a tagállamok ellen tevékenykedő hírszerző szolgálatok tevékenységéből fakadó, EU minősített információkat és tevékenységeket fenyegető veszélyek;

d) haladéktalan jelentéstételi kötelezettség az illetékes biztonsági hatóságoknál bármely, kémtevékenység gyanújára alapot adó megkörnyékezési kísérletről vagy cselekményről, illetve minden, a biztonság szempontjából szokatlan körülményről.

16. Mindazokat a személyeket, akik rendes körülmények között gyakran kapcsolatba kerülnek olyan országok képviselőivel, amelyek hírszerző szolgálatai az EU és a tagállamok ellen tevékenykednek EU minősített információk és tevékenységek megismerése céljából, ki kell oktatni a különböző hírszerző szolgálatok által közismerten alkalmazott technikákról.

17. A Tanácsnak nincsenek biztonsági szabályai arra az esetre, ha EU minősített információkhoz való hozzáférésre felhatalmazott személy bárhová magánjellegű utazást tesz. Az illetékes biztonsági hatóság azonban a hatáskörébe tartozó tisztviselőket és egyéb alkalmazottakat tájékoztatja a rájuk vonatkozó utazási szabályokról. A biztonsági tisztviselők felelnek azért, hogy a személyzet tagjainak előadásokat szervezzenek az ilyen különleges utasítások felfrissítése érdekében.

▼B

VI. SZAKASZ

**A FŐTITKÁRSÁG TISZTVISELŐIRE ÉS EGYÉB ALKALMAZOTTAIRA VONATKOZÓ BIZTONSÁGI ELLENŐRZÉSI ELJÁRÁS**

1. A Tanács birtokában lévő minősített információkhoz a Főtitkárságnak csak azon tisztviselői és egyéb alkalmazottai, illetve a Főtitkárságnál dolgozók közül csak azon személyek férhetnek hozzá, akiknek feladataik alapján és a szolgálat követelményei miatt ismerniük vagy használniuk szükséges azokat.

2. Ahhoz, hogy a fenti 1. pontban említett személyek hozzáférhessenek a „TRÈS SECRET UE/EU TOP SECRET”, „SECRET UE” és „CONFIDENTIEL UE” minősítésű információkhoz, a 4. és 5. pontban említett eljárásnak megfelelően felhatalmazással kell rendelkezniük.

3. Felhatalmazást csak olyan személy kaphat, aki átesett a tagállamok illetékes nemzeti biztonsági hatósága által a 6-10. pontban említett eljárásnak megfelelően végzett biztonsági ellenőrzésen.

4. Az 1., 2. és 3. pontban említett felhatalmazások megadásáért a személyzeti szabályzat 2. cikkének első albekezdése szerinti kinevezéssel megbízott hatóság felel.

   A kinevezéssel megbízott hatóság azt követően adja meg a felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak a 6-12. pontban említett biztonsági ellenőrzésen alapuló véleményét.

5. Az ötéves időtartamra érvényes felhatalmazás érvényét veszti, ha az érintett személy már nem látja el azokat a feladatokat, amelyek a felhatalmazás megadását indokolták. A kinevezéssel megbízott hatóság megújíthatja a felhatalmazást a 4. pontban említett eljárásnak megfelelően.

   A kinevezéssel megbízott hatóság visszavonja a felhatalmazást, ha úgy ítéli meg, hogy arra megfelelő oka van. A felhatalmazás visszavonásáról szóló határozatról értesíteni kell az illetékes nemzeti hatóságot és az érintett személyt, aki kérheti, hogy a kinevezéssel megbízott hatóság hallgassa meg.

6. A biztonsági ellenőrzés célja annak megállapítása, hogy nincs kifogás az ellen, hogy az érintett személy a Tanács birtokában lévő minősített információkhoz hozzáférjen.

7. A biztonsági ellenőrzést az érintett személy segítségével és a kinevezéssel megbízott hatóság kérelmére annak a tagállamnak az illetékes hatósága végzi el, amelynek a felhatalmazandó személy az állampolgára. Ha az érintett személy egy másik tagállam területén lakik, az érintett nemzeti hatóságok kérhetik a lakóhelye szerinti állam hatóságainak együttműködését.

8. A biztonsági ellenőrzési eljárás részeként az érintett személynek kérdőívet kell kitöltenie.

9. A kinevezéssel megbízott hatóság megkeresésében meghatározza az érintett személy rendelkezésére bocsátandó minősített információk típusát és szintjét, hogy az illetékes nemzeti hatóságok a biztonsági ellenőrzési eljárást lefolytathassák, és véleményt adhassanak arról, milyen szintű felhatalmazást lenne helyénvaló megadni az adott személynek.

10. Az egész biztonsági ellenőrzési eljárásra és a kapott eredményekre az érintett tagállamban hatályos megfelelő szabályok és rendelkezések vonatkoznak, beleértve a jogorvoslattal kapcsolatos rendelkezéseket is.

11. Ha a tagállam illetékes nemzeti hatósága pozitív véleményt adott, a kinevezéssel megbízott hatóság megadhatja a felhatalmazást az érintett személynek.

12. Az illetékes nemzeti hatóságok elutasító véleményéről értesítik az érintett személyt, aki kérheti, hogy a kinevezéssel megbízott hatóság hallgassa meg. Ha a kinevezéssel megbízott hatóság szükségesnek tartja, kérhet további tisztázó tájékoztatást az illetékes nemzeti hatóságtól. Ha az elutasító véleményt a hatóságok megerősítik, akkor a felhatalmazást nem lehet megadni.

13. Mindazok a személyek, akik a 4. és 5. pont értelmében felhatalmazást kaptak, a felhatalmazás megadásának időpontjában, majd azt követően rend-

▼B

szeres időközönként minden szükséges utasítást megkapnak a minősített információk védelmével és a védelem biztosításának módjával kapcsolatosan. Ezeknek a személyeknek nyilatkozatot kell aláírniuk, amelyben igazolják, hogy ezeket az utasításokat megkapták és vállalják azok betartását.

14. A kinevezéssel megbízott hatóság minden szükséges intézkedést megtesz az e szakaszban foglaltak végrehajtása érdekében, különösen a felhatalmazással rendelkező személyek listájához való hozzáférés vonatkozásában irányadó szabályok tekintetében.

15. Kivételes esetben – ha a szolgálat érdekei úgy kívánják – a kinevezéssel megbízott hatóság, miután az illetékes nemzeti hatóságokat értesítette és azok erre egy hónapon belül nem reagáltak, legfeljebb hat hónapos időtartamra ideiglenes felhatalmazást adhat, amíg a 7. pontban említett biztonsági ellenőrzés eredményét meg nem kapja.

16. Az így megadott feltételes és ideiglenes felhatalmazások nem biztosítanak hozzáférést a TRÈS SECRET UE/EU TOP SECRET minősítésű információkhoz; a hozzáférés ezekhez az információhoz kizárólag azokra tisztviselőkre korlátozódik, akik ténylegesen és kedvező eredménnyel mentek át a 7. pontnak megfelelően elvégzett ellenőrzésen. Az ellenőrzés eredményére várva azok a tisztviselők, akik vonatkozásában TRÈS SECRET UE/EU TOP SECRET szintű ellenőrzést kértek, ideiglenesen és feltételesen felhatalmazást kaphatnak a SECRET UE vagy annál alacsonyabb minősítésű információkhoz való hozzáférésre.

▼B

VII. SZAKASZ

## AZ EU MINŐSÍTETT ANYAGOK ELŐÁLLÍTÁSA, ELOSZTÁSA, TOVÁBBÍTÁSA, TÁROLÁSA ÉS MEGSEMMISÍTÉSE

**Tartalomjegyzék**


Általános rendelkezések

| | |
|---|---|
| I. fejezet | Az EU minősített dokumentumok előállítása és elosztása |
| II. fejezet | Az EU minősített dokumentumok továbbítása |
| III. fejezet | A technikai továbbítás elektronikus és egyéb eszközei |
| IV. fejezet | Az EU minősített dokumentumok külön példányai és fordításai, valamint a belőlük készített kivonatok |
| V. fejezet | Az EU minősített dokumentumok számbavétele, ellenőrzése, tárolása és megsemmisítése |
| VI. fejezet | A Tanácsnak szánt dokumentumokra vonatkozó különös szabályok |

▼B

Általános rendelkezések

Ez a szakasz részletezi az EU minősített dokumentumok – ezen mellékletnek az alapelveket és biztonság minimális szintjét szabályozó I. része 3. a) pontja szerinti – előkészítéséhez, elosztásához, továbbításához, tárolásához és megsemmisítéséhez szükséges intézkedéseket. Ezt a szakaszt kell alapul venni a fenti intézkedések egyéb EU minősített anyagok vonatkozásában, azok típusának figyelembevételével és eseti alapon történő kiigazításakor.

*I. fejezet*

**Az EU minősített dokumentumok előállítása és elosztása**

ELŐÁLLÍTÁS

1. Az EU-minősítéseket és -jelöléseket a II. szakaszban megállapított módon kell alkalmazni, azok minden lap tetején és alján középen szerepelnek, és minden lapot meg kell számozni. Minden EU minősített dokumentumot hivatkozási számmal és keltezéssel kell ellátni. A TRÈS SECRET UE/EU TOP SECRET és SECRET UE minősítésű dokumentumok esetében ezt a hivatkozási számot minden oldalon fel kell tüntetni. Több példányban elosztott dokumentumok esetén az egyes példányokon az első oldalon fel kell tüntetni a példány sorszámát, az oldalak teljes számával együtt. A CONFIDENTIEL UE és annál magasabb minősítésű dokumentumok első oldalán minden mellékletet és csatolmányt fel kell sorolni.

2. A CONFIDENTIEL UE és annál magasabb minősítésű dokumentumokat – az e szakasz 27. pontjában meghatározott különleges esetet kivéve – csak olyan személyek gépelhetik, fordíthatják, tárolhatják, fénymásolhatják, másolhatják mágneses úton vagy mikrofilmezhetik, akiket az EU minősített információkhoz való hozzáférés szempontjából legalább a kérdéses dokumentum megfelelő biztonsági minősítési szintjéig ellenőriztek.

   A minősített dokumentumok számítógépes elkészítését szabályozó rendelkezéseket a XI. szakasz tartalmazza.

ELOSZTÁS

3. EU minősített információkat csak olyan személyek kaphatnak meg, akiknek ismerniük szükséges azokat, és akik a megfelelő biztonsági ellenőrzésen estek át. Az első elosztás címzettjeit a kibocsátó határozza meg.

4. A TRÈS SECRET UE/EU TOP SECRET dokumentumokat a TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalokon (lásd a VIII. szakaszt) keresztül osztják el. TRÈS SECRET UE/EU TOP SECRET üzenetek esetében az illetékes nyilvántartó hivatal engedélyezheti a kommunikációs központ vezetője számára, hogy elkészítse a címzettek listájában meghatározott számú másolatot.

5. A SECRET UE és ennél alacsonyabb minősítésű dokumentumokat az eredeti címzett is továbbíthatja más címzettek számára a „szükséges ismeret” elve alapján. A kibocsátó hatóságok azonban világosan feltüntetnek minden olyan korlátozást, amelyet be kívánnak tartatni. Ilyen korlátozások esetén a címzettek a dokumentumokat csak a kibocsátó hatóságok engedélyével adhatják tovább.

6. A szervhez való érkezésekor, illetve az onnan való távozáskor minden CONFIDENTIEL UE és annál magasabb minősítésű dokumentumot regisztrálnia kell a szerv nyilvántartó hivatalának. A rögzítendő adatoknak (hivatkozási számok, időpont és adott esetben a példány sorszáma) alkalmasnak kell lenniük a dokumentumok azonosítására, és be kell vezetni őket a szolgálati naplóba vagy egy különlegesen védett számítógépes adathordozóra.

*II. fejezet*

**Az EU minősített dokumentumok továbbítása**

CSOMAGOLÁS

▼B

7. A CONFIDENTIEL UE és annál magasabb minősítésű dokumentumokat erős, nem átlátszó dupla borítékban kell továbbítani. A belső borítékon fel kell tüntetni a megfelelő EU minősítési szintet, valamint – ha lehetséges – az átvevő teljes munkaköri beosztását és címét.

8. Csak a nyilvántartó hivatalt ellenőrző tisztviselő vagy a helyettese nyithatja fel a belső borítékot és nyugtázhatja a mellékelt dokumentumok átvételét, hacsak a borítékot nem kifejezetten egy meghatározott személynek címezték. Ebben az esetben a megfelelő nyilvántartó hivatal feljegyzi a boríték beérkezését, és csak a címzett személy nyithatja fel a belső borítékot és adhat elismervényt a benne foglalt dokumentum átvételéről.

9. A belső borítékban átvételi elismervényt kell elhelyezni. Az elismervényen, amely nem minősített irat, fel kell tüntetni a hivatkozási számot, az időpontot és a dokumentum példányának a sorszámát, de a tárgyát sohasem.

10. A belső borítékot egy külső borítékba kell helyezni, amelyen az átvétel igazolása céljából fel kell tüntetni a küldemény számát. A külső borítékon semmilyen körülmények között nem tüntethető fel a biztonsági minősítés jelölése.

11. A CONFIDENTIEL UE és annál magasabb minősítésű dokumentumok esetében a futárok és a küldöncök a küldeményszám alapján kapják meg az átvételi elismervényt.

TOVÁBBÍTÁS ÉPÜLETEN VAGY ÉPÜLETEGYÜTTESEN BELÜL

12. Adott épületen vagy épületegyüttesen belül a minősített dokumentumok lepecsételt borítékban továbbíthatók, amelyen csak a címzett neve van feltüntetve, feltéve hogy a kézbesítést végző személy a dokumentum minősítési szintjének megfelelő biztonsági ellenőrzésen esett át.

EU-DOKUMENTUMOK EGY ORSZÁGON BELÜLI TOVÁBBÍTÁSA

13. Egy országon belül TRÈS SECRET UE/EU TOP SECRET dokumentumok továbbítását csak hivatalos futárszolgálat vagy a TRÈS SECRET UE/EU TOP SECRET minősítésű információhoz való hozzáférésre felhatalmazott személyek végezhetik.

14. Ha TRÈS SECRET UE/EU TOP SECRET dokumentumok épületen vagy épületegyüttesen kívülre történő továbbítására futárszolgálat vesznek igénybe, akkor az e fejezetben foglalt, a csomagolással és átvétellel kapcsolatos rendelkezéseket be kell tartani. A kézbesítő szolgálatoknak elegendő személyzettel kell rendelkezniük, amely biztosítja, hogy a TRÈS SECRET UE/EU TOP SECRET dokumentumokat tartalmazó csomagok mindenkor egy felelős tisztviselő közvetlen felügyelete alatt maradjanak.

15. TRÈS SECRET UE/EU TOP SECRET dokumentumokat üléseken és megbeszéléseken való helyi felhasználás céljából a futárokon kívül kivételesen tisztviselők is kivihetik az épületből vagy épületegyüttesből, feltéve hogy:

    a) az érintett tisztviselőnek felhatalmazása van arra, hogy hozzáférhessen ezekhez a TRÈS SECRET UE/EU TOP SECRET dokumentumokhoz;

    b) a szállítás módja megfelel a TOP SECRET dokumentumok továbbítására irányadó nemzeti szabályoknak;

    c) a tisztviselő semmilyen körülmények között sem hagyja őrizetlenül a TRÈS SECRET UE/EU TOP SECRET dokumentumokat;

    d) gondoskodnak arról, hogy az így szállított dokumentumok jegyzékét a dokumentumokat birtokló TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal megőrizze és nyilvántartásba vegye, és e nyilvántartás alapján ellenőrizze azokat visszahozataluk alkalmával.

16. Egyazon országon belül a SECRET UE és CONFIDENTIEL UE dokumentumok postai úton is továbbíthatók, amennyiben az ilyen továbbítás a nemzeti szabályozás alapján megengedett és összhangban áll a nemzeti szabályozás rendelkezéseivel, illetve továbbíthatók futárszolgálat vagy EU minősített információkhoz való hozzáférésre felhatalmazott személy útján.

▼B

17. E szabályzat alapján minden tagállam és az EU minden decentralizált szerve kidolgozza az EU minősített dokumentumok személyes szállítására vonatkozó rendelkezéseket. A dokumentumot továbbító személynek el kell olvasnia és alá kell írnia ezeket az utasításokat. Az utasításokban különösen egyértelművé kell tenni, hogy a dokumentumok semmilyen körülmények között:

    a) nem kerülhetnek ki az adott személy birtokából, hacsak nincsenek a IV. szakaszban foglalt rendelkezéseknek megfelelő biztonságos őrizet alatt;

    b) nem maradhatnak őrizetlenül sem tömegközlekedési eszközön, sem magántulajdonú járműben, sem étteremben, szállodában vagy más hasonló helyen. Nem tárolhatók szállodai széfben és nem hagyhatók őrizetlenül szállodai szobában;

    c) nem olvashatók nyilvános helyen, például repülőn vagy vonaton.

TOVÁBBÍTÁS EGYIK TAGÁLLAMBÓL A MÁSIKBA

18. A CONFIDENTIEL UE és annál magasabb minősítésű anyagokat egyik tagállamból a másikba diplomáciai vagy katonai futárszolgálat útján kell továbbítani.

19. Azonban a SECRET UE és CONFIDENTIEL UE minősítésű anyag személyes szállítása is engedélyezhető, amennyiben a szállításra vonatkozó rendelkezések biztosítják, hogy az anyag ne kerülhessen illetéktelen személy kezébe.

20. A nemzeti biztonsági hatóságok engedélyezhetik a személyes szállítást, ha diplomáciai vagy katonai futár nem áll rendelkezésre, illetve ha ezeknek a futároknak az igénybevétele olyan késedelemmel járna, amely hátrányos kihatással lehetne az EU műveleteire, és ha az anyagra a címzettnek sürgősen szüksége van. A SECRET UE vagy annál alacsonyabb minősítésű anyagok diplomáciai és katonai futárokon kívüli más személyek által történő nemzetközi személyes szállítására vonatkozó utasításokat az egyes tagállamok dolgozzák ki. Ezeknek az utasításoknak a következőket kell tartalmazniuk:

    a) az anyagot továbbító személynek megfelelő biztonsági felhatalmazással kell rendelkeznie az érintett tagállamtól;

    b) a megfelelő irodának vagy nyilvántartó hivatalnak minden így szállított anyagot nyilvántartásba kell vennie;

    c) az EU anyagot tartalmazó csomagokat vagy zsákokat a vámvizsgálat elkerülése vagy megelőzése végett hivatalos pecséttel kell ellátni, valamint egy azonosító címkével a megtalálónak szóló utasításokkal;

    d) az anyagot szállító személynek rendelkeznie kell egy valamennyi tagállam által elismert futárigazolvánnyal és/vagy kiküldetési megbízással, amely felhatalmazza őt az abban meghatározott csomag szállítására;

    e) szárazföldi útvonalon egyetlen EU-n kívüli állam területén sem szabad átutazni vagy annak határát átlépni, kivéve ha a feladó állam kifejezett biztosítékot kapott az adott államtól;

    f) az anyagot szállító személy útját úgy kell megszervezni, hogy a célállomás, az útvonal és az igénybe venni kívánt szállítóeszközök kiválasztása tekintetében feleljen meg az EU-rendelkezéseknek, illetve ha e tekintetben a nemzeti rendelkezések szigorúbbak, ez utóbbiaknak;

    g) az anyag nem kerülhet ki az azt szállító személy birtokából, kivéve ha azt a IV. szakaszban foglalt biztonságos őrizetre vonatkozó rendelkezéseknek megfelelően helyezik el;

    h) az anyag nem maradhat őrizetlenül tömegközlekedési eszközön vagy magántulajdonú járműben, sem étteremben, szállodában vagy más hasonló helyen. Nem tárolható szállodai széfben és nem hagyható őrizetlenül szállodai szobában;

▼B

i) ha a szállított anyag dokumentumokat tartalmaz, akkor azokat nem lehet nyilvános helyen olvasni (például vonaton, repülőn stb.).

A minősített anyag szállítására kijelölt személynek olyan biztonsági tájékoztatót kell elolvasnia és aláírnia, amely minimálisan a fentiekben felsorolt utasításokat és azokat az eljárásokat tartalmazza, amelyek vészhelyzetben vagy olyan esetben követendők, amikor a minősített anyagot tartalmazó csomagot vámtisztviselők vagy repülőtéri biztonsági tisztviselők akarják átvizsgálni.

A RESTREINT UE DOKUMENTUMOK TOVÁBBÍTÁSA

21. Attól eltekintve, hogy a szállítás során biztosítani kell, hogy a dokumentumok ne kerülhessenek illetéktelen személyek kezébe, a RESTREINT UE dokumentumok szállítására nézve különleges rendelkezések nincsenek megállapítva.

A FUTÁROK BIZTONSÁGA

22. A SECRET UE és CONFIDENTIEL UE dokumentumok szállítására alkalmazott valamennyi futárnak és küldöncnek megfelelő biztonsági felhatalmazással kell rendelkeznie.

*III. fejezet*

**A technikai továbbítás elektronikus és egyéb eszközei**

23. Az EU minősített információk biztonságos továbbítását a kommunikációs biztonságot szolgáló intézkedések hivatottak biztosítani. Az EU minősített információk továbbítására vonatkozó részletes szabályokat a XI. szakasz tartalmazza.

24. Csak akkreditált kommunikációs központok és hálózatok és/vagy terminálok és rendszerek továbbíthatnak CONFIDENTIEL UE és SECRET UE minősítésű információkat.

*IV. fejezet*

**Az EU minősített dokumentumok külön példányai és fordításai, valamint a belőlük készített kivonatok**

25. TRÈS SECRET UE/EU TOP SECRET dokumentumok másolását vagy fordítását csak a kibocsátójuk engedélyezheti.

26. Ha TRÈS SECRET UE/EU TOP SECRET szintű biztonsági felhatalmazással nem rendelkező személyek kérnek olyan információkat, amelyek – bár azokat TRÈS SECRET UE/EU TOP SECRET dokumentumok tartalmazzák – nem rendelkeznek ilyen minősítéssel, akkor a TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal vezetője kaphat engedélyt a szóban forgó dokumentum szükséges számú kivonatának az elkészítésére. Egyidejűleg meg kell tennie a szükséges intézkedéseket annak biztosítására, hogy ezek a kivonatok megkapják a megfelelő biztonsági minősítést.

27. A SECRET UE és alacsonyabb minősítésű dokumentumokat a címzett sokszorosíthatja és lefordíthatja az adott nemzeti biztonsági rendelkezések keretein belül és a szükséges ismeret elvének szigorú betartása mellett. Az eredeti dokumentumra vonatkozó biztonsági intézkedések a másolatokra és/vagy a fordításokra is vonatkoznak. Az EU decentralizált szerveinek is be kell tartaniuk e biztonsági szabályzatot.

*V. fejezet*

**Az EU minősített dokumentumok számbavétele, ellenőrzése, tárolása és megsemmisítése**

SZÁMBAVÉTEL ÉS ELLENŐRZÉS

28. A VIII. szakasz szerinti minden egyes TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal évente köteles a VIII. szakasz 9-11. pontjában meghatározott rendelkezéseknek megfelelően tételesen számba venni a

▼B

TRÈS SECRET UE/EU TOP SECRET dokumentumokat. A TRÈS SECRET UE/EU TOP SECRET szintűnél alacsonyabb minősítésű dokumentumokat belső ellenőrzésnek kell alávetni a nemzeti iránymutatásoknak megfelelően, illetve a Főtitkárság vagy az EU decentralizált szervei esetében a főtitkár/főképviselő utasításainak megfelelően.

Ezek a műveletek lehetőséget kínálnak arra, hogy kikérjék a dokumentumok birtokosainak véleményét:

a) egyes dokumentumok visszaminősítésének vagy minősítésük megszüntetésének lehetőségéről;

b) a megsemmisítendő dokumentumokról.

AZ EU MINŐSÍTETT DOKUMENTUMOK IRATTÁRI TÁROLÁSA

29. Annak érdekében, hogy a tárolás minél kevesebb problémával járjon, az összes nyilvántartó hivatal ellenőrző tisztviselői felhatalmazást kapnak arra, hogy a TRÈS SECRET UE/EU TOP SECRET, SECRET UE és CONFIDENTIEL UE dokumentumokat mikrofilmre vegyék vagy egyéb módon, mágneses vagy optikai adathordozón tárolják irattári megőrzés céljából, feltéve hogy:

a) a mikrofilmes/tárolási eljárást olyan személyek végzik, akik a megfelelő minősítési szintnek megfelelő érvényes biztonsági felhatalmazással rendelkeznek;

b) a mikrofilm/adathordozó ugyanolyan biztonságban részesül, mint az eredeti dokumentumok;

c) a TRÈS SECRET UE/EU TOP SECRET dokumentum mikrofilmre vételéről/tárolásáról kibocsátója értesítést kap;

d) a filmtekercsek vagy más típusú adathordozók csak azonos TRÈS SECRET UE/EU TOP SECRET, SECRET UE, illetve CONFIDENTIEL UE minősítésű dokumentumokat tartalmaznak;

e) a TRÈS SECRET UE/EU TOP SECRET, SECRET UE vagy CONFIDENTIEL UE dokumentum mikrofilmre vitelét/tárolását világosan feltüntetik az éves leltárnál használt nyilvántartásban;

f) a mikrofilmre vitt vagy egyéb módon tárolt dokumentumok eredetijét a 31-36. pontban rögzített szabályoknak megfelelően megsemmisítik.

30. Ezek a szabályok vonatkoznak a tárolás egyéb, a nemzeti biztonsági hatóságok által engedélyezett formáira, például az elektromágneses adathordozókra és az optikai lemezekre is.

EU MINŐSÍTETT DOKUMENTUMOK RUTINSZERŰ MEGSEMMISÍTÉSE

31. Annak érdekében, hogy szükségtelenül ne halmozódjanak fel olyan EU minősített dokumentumok, amelyeket a birtokában tartó szerv vezetője elavultnak vagy felesleges számúnak ítél, azokat a lehető legrövidebb időn belül meg kell semmisíteni a következő módon:

a) a TRÈS SECRET UE/EU TOP SECRET dokumentumokat csak az azokért felelős központi nyilvántartó hivatal semmisítheti meg. Az egyes megsemmisített dokumentumokról megsemmisítési jegyzőkönyvet kell felvenni, amelyet a TRÈS SECRET UE/EU TOP SECRET ellenőrző tisztviselő és a megsemmisítés során tanúként jelen lévő, TRÈS SECRET UE/EU TOP SECRET biztonsági felhatalmazással rendelkező tisztviselőnek kell aláírnia. Ezt a szolgálati naplóba be kell jegyezni;

b) a nyilvántartó hivatal a megsemmisítési jegyzőkönyveket az elosztóívvel együtt tíz évig őrzi meg. Másolatot csak akkor küldenek a kibocsátónak vagy a megfelelő központi nyilvántartó hivatalnak, ha azok ezt kifejezetten kérik;

c) a TRÈS SECRET UE/EU TOP SECRET dokumentumokat – a TRÈS SECRET UE/EU TOP SECRET dokumentumok készítése során keletkezett valamennyi minősített hulladékot is beleértve, mint például a rontott példányok, piszkozatok, gépelt jegyzetek és indigópapírok – a TRÈS SECRET UE/EU TOP SECRET ellenőrző tisztviselő felügyelete alatt

▼B

elégetéssel, zúzással, felaprítással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni.

32. A SECRET UE dokumentumokat a 31. c) pontban említett eljárások egyikét alkalmazva, egy biztonsági felhatalmazással rendelkező személy felügyelete alatt az a nyilvántartó hivatal semmisíti meg, amelyik felel értük. A megsemmisített SECRET UE dokumentumokról aláírt megsemmisítési jegyzőkönyvet kell felvenni, amelyet a nyilvántartó hivatal az elosztóívekkel együtt legalább három évig megőriz.

33. A CONFIDENTIEL UE dokumentumokat az 31. c) pontban említett eljárások egyikét alkalmazva, egy biztonsági felhatalmazással rendelkező személy felügyelete alatt az a nyilvántartó hivatal semmisíti meg, amelyik felel értük. Megsemmisítésüket a nemzeti rendelkezéseknek, illetve a Főtitkárság és az EU decentralizált szervei esetében a főtitkár/főképviselő utasításainak megfelelően kell nyilvántartani.

34. RESTREINT UE dokumentumokat az ilyen dokumentumokért felelős nyilvántartó hivataloknak vagy a felhasználóknak kell megsemmisíteniük a nemzeti rendelkezéseknek, illetve a Főtitkárság és az EU decentralizált szervei esetében a főtitkár/főképviselő utasításainak megfelelően.

MEGSEMMISÍTÉS VÉSZHELYZETBEN

35. A Főtitkárság, a tagállamok és az EU decentralizált szervei a helyi feltételek alapján terveket dolgoznak ki az EU minősített anyagok válsághelyzetben történő védelmére, beleértve adott esetben a vészhelyzeti megsemmisítési és kiürítési terveket is; szervezeteik vonatkozásában kiadják az annak megakadályozására szükségesnek ítélt utasításokat, hogy az EU minősített információk illetéktelen személyek kezébe kerülhessenek.

36. A SECRET UE és CONFIDENTIEL UE anyagok válsághelyzetben történő védelmére és/vagy megsemmisítésére irányuló intézkedések semmilyen körülmények között sem akadályozhatják az olyan TRÈS SECRET UE/EU TOP SECRET anyagok – a kriptográfiai berendezéseket is beleértve – védelmét vagy megsemmisítését, amelyek ellátása minden más feladattal szemben elsőbbséget élvez. A kriptográfiai berendezések vészhelyzetben történő védelmére és megsemmisítésére vonatkozó intézkedéseket ad hoc utasítások útján szabályozzák.

*VI. fejezet*

**A Tanácsnak szánt dokumentumokra vonatkozó különös szabályok**

37. A Főtitkárságon belül a „Minősített Információk Hivatala” követi nyomon a Tanácsnak szánt dokumentumokban szereplő SECRET UE vagy CONFIDENTIEL UE minősítésű információkat.

A személyzeti és igazgatási főigazgató felügyelete mellett a Minősített Információk Hivatala:

a) ellátja az ilyen információk nyilvántartásba vételével, sokszorosításával, fordításával, továbbításával, elküldésével és megsemmisítésével kapcsolatos igazgatási feladatokat;

b) naprakészen tartja a minősített információkra vonatkozó adatok listáját;

c) rendszeres időközönként rákérdez, hogy szükséges-e az információ minősítésének további fenntartása;

d) a Biztonsági Hivatallal együttműködve meghatározza az információk minősítésének és a minősítés megszüntetésének gyakorlati szabályait.

38. A Minősített Információk Hivatala a következő adatokról vezet nyilvántartást:

a) a minősített információ előállításának időpontja;

b) a minősítési szint;

c) a minősítés lejártának időpontja;

d) a kibocsátó neve és szervezeti egysége;

▼B

e) a címzett vagy címzettek és sorszámuk;

f) tárgy;

g) szám;

h) a szétosztott példányok száma;

i) a Tanács elé beterjesztett minősített információk leltárának elkészítése;

j) a minősített információk visszaminősítésének és minősítésük megszüntetésének nyilvántartása.

39. Az e szakasz I–V. fejezetében meghatározott általános szabályokat a Főtitkárság Minősített Információk Irodájára is alkalmazni kell, kivéve ha azokat az e fejezetben foglalt különös szabályok módosítják.

▼B

VIII. SZAKASZ

**TRÈS SECRET UE/EU TOP SECRET ANYAGOK NYILVÁNTARTÓ HIVATALAI**

1. A TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalok célja biztosítani az TRÈS SECRET UE/EU TOP SECRET dokumentumoknak a biztonsági előírásoknak megfelelő nyilvántartását, kezelését és elosztását. Az egyes tagállamokban, a Főtitkárságon és adott esetben az EU decentralizált szerveinél működő TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal vezetője a TRÈS SECRET UE/EU TOP SECRET ellenőrző tisztviselő.

2. A központi nyilvántartó hivatalok fő átvevő és elosztó hatóságként működnek a tagállamokban, a Főtitkárságon és az EU decentralizált szerveinél, ahol ilyen nyilvántartó hivatalok létesültek, továbbá adott esetben egyéb EU-intézményekben, nemzetközi szervezetekben és olyan harmadik államokban, amelyekkel a Tanács a minősített információk cseréjére vonatkozó biztonsági eljárásokról szóló megállapodást kötött.

3. Ha szükséges, alárendelt nyilvántartó hivatalokat hoznak létre, amelyek a TRÈS SECRET UE/EU TOP SECRET dokumentumok belső igazgatásáért felelnek. Ezek naprakész nyilvántartást vezetnek a felelősségi körükbe tartozó minden dokumentum elosztásáról.

4. A hosszú távú igényekre reagálva, az I. szakaszban foglaltaknak megfelelően, alárendelt TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalokat kell létrehozni, és ezeket a központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalhoz csatolják. Ha a TRÈS SECRET UE/EU TOP SECRET dokumentumokba csak ideiglenesen és alkalmilag szükséges betekinteni, ezeket a dokumentumokat az alárendelt TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal létrehozása nélkül is ki lehet adni, feltéve hogy szabályokat állapítanak meg annak biztosítása érdekében, hogy a dokumentumok a megfelelő TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal ellenőrzése alatt maradjanak és az összes fizikai és személyzeti biztonsági intézkedést betartsák.

5. Az alárendelt TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalok a központi nyilvántartó hivatal kifejezett engedélye nélkül nem továbbíthatnak közvetlenül ugyanazon központi nyilvántartó hivatal alá tartozó alárendelt nyilvántartó hivatalnak TRÈS SECRET UE/EU TOP SECRET dokumentumokat.

6. A nem ugyanazon központi nyilvántartó hivatalokhoz tartozó alárendelt nyilvántartó hivatalok között a TRÈS SECRET UE/EU TOP SECRET dokumentumok minden cseréjét a központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalokon keresztül kell lebonyolítani.

A KÖZPONTI TRÈS SECRET UE/EU TOP SECRET NYILVÁNTARTÓ HIVATALOK

7. A központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal vezetője mint ellenőrző tisztviselő az alábbiakért felel:

   a) a TRÈS SECRET UE/EU TOP SECRET dokumentumoknak a VII. szakaszban meghatározott szabályoknak megfelelő továbbítása;

   b) az alá tartozó valamennyi alárendelt TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalt, illetve a kinevezett ellenőrző tisztviselők és felhatalmazott helyetteseik nevét és aláírását tartalmazó lista vezetése;

   c) a központi nyilvántartó hivatal által elosztott TRÈS SECRET UE/EU TOP SECRET dokumentumokról a nyilvántartó hivatalok által kiadott átvételi elismervények megőrzése;

   d) a birtokában lévő és az elosztott TRÈS SECRET UE/EU TOP SECRET dokumentumokról szóló nyilvántartás vezetése;

   e) naprakész lista vezetése valamennyi központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalról, amellyel rendszeresen levelezik,

▼B

a kinevezett ellenőrző tisztviselők és felhatalmazott helyetteseik nevével és aláírásával együtt;

f) a nyilvántartó hivatal birtokában lévő valamennyi TRÈS SECRET UE/EU TOP SECRET dokumentum fizikai megőrzése a IV. szakaszban meghatározott rendelkezéseknek megfelelően.

TRÈS SECRET UE/EU TOP SECRET ALÁRENDELT NYILVÁNTARTÓ HIVATALOK

8. A TRÈS SECRET UE/EU TOP SECRET alárendelt nyilvántartó hivatal vezetője mint ellenőrző tisztviselő felel:

a) a TRÈS SECRET UE/EU TOP SECRET dokumentumoknak a VII. szakaszban és a VIII. szakasz 5. és 6. pontjában meghatározott rendelkezéseknek megfelelő továbbításáért;

b) az általa ellenőrzött TRÈS SECRET UE/EU TOP SECRET dokumentumokhoz való hozzáférésre felhatalmazott személyek naprakész listájának vezetéséért;

c) azért, hogy a TRÈS SECRET UE/EU TOP SECRET dokumentumok elosztása a kibocsátójuk utasításai szerint, illetve a szükséges ismeret elve alapján történjék, miután először ellenőrizte, hogy a címzett rendelkezik-e a megfelelő szintű biztonsági felhatalmazással;

d) az ellenőrzése alá tartozó valamennyi birtokolt vagy elosztott, illetve más TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivataloknak átadott TRÈS SECRET UE/EU TOP SECRET dokumentumok naprakész nyilvántartásának vezetéséért, továbbá a megfelelő átvételi elismervények megőrzéséért;

e) naprakész lista vezetéséért azokról a TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalokról, amelyekkel jogosult TRÈS SECRET UE/EU TOP SECRET dokumentumokat kicserélni, az ellenőrző tisztviselők és felhatalmazott helyetteseik nevével és aláírásával együtt;

f) az alárendelt nyilvántartó hivatal birtokában lévő valamennyi TRÈS SECRET UE/EU TOP SECRET dokumentum fizikai megőrzéséért a IV. szakaszban meghatározott rendelkezéseknek megfelelően.

LELTÁR

9. Tizenkét havonta minden TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal köteles tételes leltárt készíteni az összes TRÈS SECRET UE/EU TOP SECRET dokumentumról, amellyel elszámolni köteles. Akkor tekinthető úgy, hogy egy dokumentummal elszámoltak, ha a nyilvántartó hivatalban fizikailag megtalálható vagy a hivatal rendelkezik annak a TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalnak az átvételi elismervényével, amelynek a dokumentumot továbbította, illetve ha birtokában van a dokumentum megsemmisítési jegyzőkönyve, vagy a dokumentum visszaminősítését vagy minősítésének megszüntetését elrendelő utasítás.

10. Az alárendelt nyilvántartó hivatalok az éves leltár megállapításait a felettes központi nyilvántartó hivatalnak azon a napon küldik meg, amelyet ez utóbbi meghatározott.

11. A nemzeti biztonsági hatóságok, továbbá azon EU-intézmények, nemzetközi szervezetek és EU decentralizált szervek, ahol központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal működik, a TRÈS SECRET UE/EU TOP SECRET központi nyilvántartó hivatalokban évente végzett leltározás megállapításait minden évben legkésőbb április 1-jéig megküldik a főtitkárnak/főképviselőnek.

▼B

IX. SZAKASZ

## A TANÁCS HELYISÉGEIN KÍVÜL ÉS RENDKÍVÜL KÉNYES ÜGYEKBEN TARTOTT KÜLÖNLEGES ÜLÉSEK ESETÉN ALKALMAZANDÓ BIZTONSÁGI INTÉZKEDÉSEK

ÁLTALÁNOS ISMERTETÉS

1. Amikor az Európai Tanács, a Tanács, a miniszterek üléseit vagy egyéb fontos üléseket a Tanács brüsszeli és luxembourgi helyiségein kívül tartják meg, és ha az ezeken megvitatott kérdések vagy információk fokozottan kényes jellegével kapcsolatos különleges biztonsági követelmények indokolják, az alábbiakban meghatározott biztonsági intézkedéseket kell megtenni. Ezek az intézkedések csak az EU minősített információk védelmére vonatkoznak, így esetleg egyéb biztonsági intézkedéseket is szükséges lehet tervbe venni.

HATÁSKÖRÖK

**Fogadó tagállam**

2. Az a tagállam, amelynek területén az ülést tartják (fogadó tagállam) a Főtitkárság Biztonsági Hivatalával együttműködve felel az Európai Tanács, a Tanács, a miniszterek üléseinek vagy egyéb fontos üléseknek a biztonságáért és a küldöttek, illetve munkatársaik fizikai biztonságáért.

A biztonság védelmét illetően különösen a következőkről kell gondoskodnia:

a) tervek kidolgozása a biztonságot fenyegető veszélyek és a biztonsággal összefüggő váratlan események kezelésére; a tervezett intézkedések különösen az EU minősített dokumentumoknak az irodahelyiségekben történő biztonságos megőrzésére irányulnak;

b) intézkedések megtétele annak érdekében, hogy EU minősített üzenetek fogadása és küldése céljából lehetővé váljék az esetleges hozzáférés a Tanács kommunikációs rendszeréhez. A fogadó tagállam szükség szerint biztonságos telefonrendszerekhez való hozzáférést is biztosít.

**Tagállamok**

3. A tagállamok hatóságainak biztosítaniuk kell az alábbiakat:

a) nemzeti küldötteik számára a megfelelő szintű biztonsági ellenőrzéséről szóló tanúsítványok megküldése – szükség szerint jeladás vagy fax útján – közvetlenül vagy a Főtitkárság Biztonsági Hivatalán keresztül az ülés biztonsági tisztviselőjének;

b) a fogadó tagállam hatóságainak és adott esetben a Főtitkárság Biztonsági Hivatalának értesítése bármely egyedi fenyegetésről annak érdekében, hogy megfelelő intézkedéseket lehessen tenni.

**Az ülés biztonsági tisztviselője**

4. Biztonsági tisztviselőt kell kinevezni, akinek feladata az általános belső biztonsági intézkedések előkészítése és ellenőrzése, valamint az egyéb érintett biztonsági hatóságokkal való egyeztetés. Az általa tett intézkedések általában az alábbiakra terjednek ki:

a) i. védelmi intézkedések az ülés helyszínén annak biztosítására, hogy az ülés minden olyan váratlan eseménytől mentesen folyjék le, ami veszélyeztethetné az ott felhasznált EU minősített információk biztonságát;

ii. az ülés helyszínére, a küldöttségek számára biztosított területekre és a konferenciatermekbe belépési engedéllyel rendelkező személyzet, valamint a berendezések ellenőrzése;

iii. állandó egyeztetés a fogadó tagállam illetékes hatóságaival és a Főtitkárság Biztonsági Hivatalával;

▼B

b) a biztonsági utasítások beillesztése az ülés dossziéjába, kellőképpen figyelembe véve az e biztonsági szabályzatban rögzített követelményeket és minden egyéb, szükségesnek ítélt biztonsági utasítást.

**A Főtitkárság Biztonsági Hivatala**

5. A Főtitkárság Biztonsági Hivatala tanácsadóként vesz részt az ülés előkészítésében; képviselteti magát a helyszínen, hogy szükség esetén tanácsot adjon és segítse az ülés biztonsági tisztviselőjét és a küldöttségeket.

6. Az ülés minden küldöttsége kijelöl egy biztonsági tisztviselőt, aki a küldöttségen belül felel a biztonsági ügyekért, valamint az ülés biztonsági tisztviselőjével és – adott esetben – a Főtitkárság Biztonsági Hivatalának képviselőjével való kapcsolattartásért.

BIZTONSÁGI INTÉZKEDÉSEK

**Biztonsági területek**

7. A következő biztonsági területeket kell kialakítani:

a) egy II. osztályba tartozó biztonsági terület, amely a szerkesztői szobát, a Főtitkárság irodáit és a reprográfiai berendezéseket, valamint adott esetben a küldöttségek irodahelyiségeit foglalja magában;

b) egy I. osztályba tartozó biztonsági terület, amely a konferenciatermet, valamint a tolmácsok és a hangmérnökök fülkéit foglalja magában;

c) szolgálati területek, amelyek a sajtó számára fenntartott területből és az ülés helyszínének igazgatási célokra, étkezés és szállás céljára szolgáló részeiből, valamint a sajtóközponttal és az ülés helyszínével közvetlenül határos területekből állnak.

**Belépők**

8. A küldöttségek kérésére, azok igényeinek megfelelően az ülés biztonsági tisztviselője adja ki a megfelelő kitűzőket. Ha szükséges, különbséget lehet tenni a különböző biztonsági területekhez való hozzáférést illetően.

9. Az ülésre vonatkozó biztonsági utasítások előírják, hogy az ülés helyszínének területén minden érintett személy mindenkor látható módon viselje és helyezze ki kitűzőjét, hogy őket a biztonsági személyzet szükség szerint ellenőrizhesse.

10. A kitűzőt viselő résztvevők mellett az ülés helyszínére a lehető legkevesebb számú embert engedik be. Ha a nemzeti küldöttségek látogatókat akarnak fogadni az ülés ideje alatt, erről értesítik az ülés biztonsági tisztviselőjét. A látogatóknak látogatói kitűzőt kell adni. Látogatói belépőnyomtatványt töltenek ki, amelyen feltüntetik a látogató és a felkeresni kívánt személy nevét. A látogatókat mindenkor biztonsági őr vagy a felkeresett személy kíséri. A látogatói belépőnyomtatványt a kísérő tartja magánál, aki azt a látogatói kitűzővel együtt leadja a biztonsági személyzetnél, amikor a látogató az ülés helyszínét elhagyja.

**Fényképezőgépek és hangrögzítő berendezések ellenőrzése**

11. Kamerát vagy hangrögzítő berendezést az I. osztályba tartozó biztonsági területre – az ülés biztonsági tisztviselője által kellően felhatalmazott fotósok és hangmérnökök által hozott berendezések kivételével – bevinni nem lehet.

**Aktatáskák, hordozható számítógépek és csomagok ellenőrzése**

12. A biztonsági területre engedély birtokában belépők rendszerint ellenőrzés nélkül bevihetik aktatáskáikat és (csak saját áramforrással rendelkező) hordozható számítógépeiket. A küldöttségeknek címzett csomagokat a küldöttségek átvehetik, ezeket vagy a küldöttség biztonsági tisztviselője vizsgálja meg, vagy speciális berendezéssel világítják át, vagy a biztonsági személyzet nyitja fel átvizsgálás céljából. Ha az ülés biztonsági tisztviselője szükségesnek tartja, a kézitáskák és csomagok átvizsgálására szigorúbb intézkedéseket is meg lehet határozni.

▼B

**Technikai biztonság**

13. Az ülésterem technikai biztonságát technikai biztonsági csoport biztosíthatja, amely az ülés alatt elektronikus felügyeletet is végezhet.

**A küldöttségek dokumentumai**

14. A küldöttségek felelnek az EU minősített dokumentumoknak az ülésekre és az onnan való szállításáért. A küldöttségek e dokumentumoknak a számukra kijelölt helyiségekben való felhasználása során azok ellenőrzéséért és biztonságáért is felelnek. A minősített dokumentumoknak az ülés helyére, illetve az onnan történő szállításában kérhetik a fogadó tagállam segítségét.

**A dokumentumok biztonságos megőrzése**

15. Ha a Főtitkárság, a Bizottság vagy a küldöttségek nem tudják minősített dokumentumaikat a jóváhagyott szabályoknak megfelelően tárolni, ezeket a dokumentumokat lepecsételt borítékban, átvételi elismervény ellenében leadhatják az ülés biztonsági tisztviselőjénél, hogy az a jóváhagyott szabályoknak megfelelő tárolásukról gondoskodjon.

**Az irodahelyiségek ellenőrzése**

16. Az ülés biztonsági tisztviselője gondoskodik arról, hogy a Főtitkárság és a küldöttségek irodahelyiségeit minden munkanap végén ellenőrizzék annak biztosítása érdekében, hogy minden EU minősített dokumentumot biztonságos helyen őrizzenek; ha nem így történik, meg kell tennie a szükséges intézkedéseket.

**Az EU minősített hulladék ártalmatlanítása**

17. Minden hulladék EU minősített anyagként kezelendő, és tárolásához szemetes kosarakat vagy zsákokat kell biztosítani a Főtitkárság és a küldöttségek részére. A Főtitkárságnak és a küldöttségeknek kijelölt helyiségeik elhagyása előtt át kell adniuk hulladékukat az ülés biztonsági tisztviselőjének, aki intézkedik azok előírásszerű megsemmisítéséről.

18. Az ülés végén a Főtitkárság és a küldöttségek birtokában lévő, de már szükségtelen minden dokumentumot hulladékként kell kezelni. Az üléssel kapcsolatban hozott biztonsági intézkedések megszüntetése előtt a Főtitkárság és a küldöttségek helyiségeit alaposan át kell vizsgálni. Az átvéli elismervény ellenében átvett dokumentumokat, amilyen mértékben csak lehetséges, a VII. szakaszban meghatározottak szerint kell megsemmisíteni.

▼B

X. SZAKASZ

**A BIZTONSÁG MEGSÉRTÉSE ÉS EU MINŐSÍTETT INFORMÁCIÓK ILLETÉKTELENEK TUDOMÁSÁRA JUTÁSA**

1. A biztonság megsértése akkor következik be, ha a Tanács biztonsági szabályzatával ellentétes cselekedet vagy mulasztás következményeként EU minősített információk veszélybe kerülhetnek, vagy illetéktelenek tudomására juthatnak.

2. EU minősített információk illetéktelenek tudomására jutása akkor következik be, ha az információk részben vagy teljes egészükben illetéktelen személyek kezébe, vagyis olyan személyek kezébe jutnak, akik nem rendelkeznek megfelelő biztonsági felhatalmazással vagy nincs szükségük az ismeretre, illetve ha valószínűsíthető, hogy ilyen esemény bekövetkezett.

3. EU minősített információk illetéktelenek tudomására jutása bekövetkezhet óvatlanság, gondatlanság vagy indiszkréció következtében, valamint azon szolgálatok tevékenysége következtében is, amelyek EU minősített információkkal és tevékenységekkel kapcsolatos ismereteket akarnak megszerezni az EU-ban és tagállamaiban, továbbá felforgató szervezetek tevékenysége következtében.

4. Fontos, hogy mindazok, akiknek EU minősített információkat kell kezelniük, alapos tájékoztatást kapjanak a biztonsági eljárásokról, az indiszkrét társalgás veszélyeiről és a sajtóval való kapcsolattartásról. Tisztában kell lenniük annak fontosságával, hogy a biztonság minden általuk észlelt megsértéséről azonnal tájékoztassák annak a tagállamnak, intézménynek vagy szervnek a biztonsági hatóságát, amely őket alkalmazza.

5. Ha valamely biztonsági hatóság felfedezi, hogy az EU minősített információra vonatkozó biztonságot megsértették vagy azt, hogy EU minősített anyagok vesztek vagy tűntek el, illetve erről tájékoztatást kap, akkor idejében intézkedéseket tesz:

   a) a tényállás megállapítására;

   b) az okozott kár felmérésére és minimalizálására;

   c) az ismételt előfordulás megelőzésére;

   d) az illetékes hatóságok értesítésére arról, hogy a biztonság megsértése milyen következményekkel jár.

   Ezzel összefüggésben a következő információkat kell szolgáltatni:

   i. az érintett információk leírása, beleértve azok minősítését, hivatkozási számát, példányának sorszámát, keltezését, kibocsátóját, tárgyát és terjedelmét;

   ii. a biztonság megsértése körülményeinek rövid leírása, beleértve azt az időpontot és időtartamot is, amikor az információ ki volt téve annak, hogy illetéktelenek tudomására jusson;

   iii. nyilatkozat arról, hogy a kibocsátót tájékoztatták-e.

6. Minden biztonsági hatóság– miután értesült arról, hogy a biztonság megsértésére sor kerülhetett – köteles ezt a tényt haladéktalanul jelenteni az alábbi eljárást alkalmazva: az alárendelt TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatal jelenti az esetet a Főtitkárság Biztonsági Hivatalának annak központi TRÈS SECRET UE/EU TOP SECRET nyilvántartó hivatalán keresztül; ha az EU minősített információ illetéktelenek tudomására jutása valamely tagállam joghatósága alá esik, arról a Főtitkárság Biztonsági Hivatalát az illetékes nemzeti biztonsági hatóság útján az 5. pont szerint kell értesíteni.

7. A RESTREINT UE információkkal kapcsolatos eseteket csak akkor kell jelenteni, ha szokatlan jellemzőket mutatnak.

8. Miután a biztonság megsértéséről értesült, a főtitkár/főképviselő:

   a) értesíti a kérdéses minősített információt kibocsátó hatóságot;

▼B

b) felkéri az illetékes biztonsági hatóságokat a nyomozás megindítására;

c) összehangolja a nyomozást, ha az ügyben több biztonsági hatóság is érintett;

d) jelentést kér arról, hogy a biztonságot milyen körülmények között sértették meg, az időpontról vagy arról az időtartamról, amelynek során ez megtörténhetett, arról, hogy ezt mikor fedezték fel, továbbá részletes leírást kér az érintett anyag tartalmáról és minősítéséről. Ugyancsak jelentést kér az EU, illetve egy vagy több tagállama érdekeit ért károkról és azokról az intézkedésekről, amelyeket az ismételt előfordulás megelőzése érdekében tettek.

9. Az információt kibocsátó hatóság tájékoztatja a címzetteket és megfelelő utasításokat ad.

10. Az EU minősített információk illetéktelenek tudomására jutásáért felelős személy a vonatkozó szabályok és rendelkezések szerint fegyelmi eljárás alá vonható. Ez az eljárás nem érinti az esetleges bírósági eljárást.

▼B

XI. SZAKASZ

**AZ IT-RENDSZEREKBEN ÉS KOMMUNIKÁCIÓS RENDSZEREKBEN KEZELT INFORMÁCIÓK VÉDELME**

**Tartalomjegyzék**


| | |
|---|---|
| I. fejezet | Bevezetés |
| II. fejezet | Fogalommeghatározások |
| III. fejezet | Hatáskörök a biztonság terén |
| IV. fejezet | Nem technikai jellegű biztonsági intézkedések |
| V. fejezet | Technikai jellegű biztonsági intézkedések |
| VI. fejezet | Biztonság a kezelés során |
| VII. fejezet | Beszerzés |
| VIII. fejezet | Ideiglenes vagy alkalomszerű felhasználás |

▼B

*I. fejezet*

**Bevezetés**

ÁLTALÁNOS SZEMPONTOK

1. A biztonsági politika és a biztonsági követelmények minden olyan kommunikációs és információs rendszerre és hálózatra (a továbbiakban: RENDSZEREK) vonatkoznak, amelyek CONFIDENTIEL UE és annál magasabb minősítésű információkat kezelnek.

2. A RESTREINT UE információt kezelő RENDSZEREK esetében ugyancsak szükség van biztonsági intézkedésekre ezen információk titkosságának védelme érdekében. Minden RENDSZERNÉL szükségesek biztonsági intézkedések maguknak a rendszereknek és a bennük található információk integritásának és rendelkezésre állásának a védelmében. Az ezeknek a rendszereknek az esetében alkalmazandó biztonsági intézkedéseket a kijelölt biztonsági akkreditációs hatóság (Security Accreditation Authority, a továbbiakban: SAA) határozza meg, és azok arányosak a becsült kockázattal, illetve megfelelnek az e biztonsági szabályzatban meghatározott politikának.

3. A beépített IT-RENDSZEREKET tartalmazó érzékelő rendszerek védelmét azoknak a rendszereknek az általános összefüggésében kell az e szakaszban foglalt rendelkezések lehető legteljesebb alkalmazása mellett meghatározni és részletezni, amelyekhez azok tartoznak.

A RENDSZEREKKEL SZEMBENI FENYEGETÉSEK ÉS A RENDSZEREK SEBEZHETŐSÉGE

4. Általánosságban a fenyegetés a biztonság véletlenszerű sérülésének, illetve szándékos megsértésének a lehetőségeként határozható meg. RENDSZEREK esetében ez a titkosság, az integritás és a rendelkezésre állás egy vagy több tulajdonságának az elvesztését jelenti. A sebezhetőség az ellenőrzés elégtelenségeként vagy hiányaként definiálható, amely megkönnyíti vagy lehetővé teszi a konkrét fenyegetés létrejöttét egy meghatározott tárggyal vagy céllal szemben. A sebezhetőség keletkezhet mulasztásból vagy összefügghet az ellenőrzés hanyagságával, hiányosságával vagy következetlenségével; természetét tekintve lehet technikai, eljárási vagy üzemeltetési jellegű.

5. A RENDSZEREKBEN kezelt, gyors visszakeresésre, továbbításra és felhasználásra szánt, koncentrált formában meglévő EU minősített és nem minősített információk számos fenyegetésnek vannak kitéve. Ezek között található az információkhoz való illetéktelen hozzáférés vagy ellenkezőleg, a jogosultsággal rendelkező felhasználók hozzáférésének megtagadása. Ugyancsak kockázatot jelent az információk engedély nélküli kiszolgáltatása, megrongálódása, módosítása vagy törlése. Ezen túlmenően a bonyolult és esetenként érzékeny berendezések költségesek, és gyakran nehéz őket gyorsan megjavítani vagy pótolni. Következésképpen ezek a RENDSZEREK vonzó célpontjai a hírszerző műveleteknek és a szabotázscselekménynek, különösen ha a biztonsági intézkedéseket hatástalannak vélik.

BIZTONSÁGI INTÉZKEDÉSEK

6. Az e szakaszban megállapított biztonsági intézkedések főként arra irányulnak, hogy védelmet nyújtsanak az információk engedély nélküli kiszolgáltatásával (a titkosság elvesztésével), valamint az információk integritásának és rendelkezésre állásának elvesztésével szemben. Az EU minősített információkat kezelő RENDSZEREK megfelelő biztonsága védelmének eléréséhez – a hagyományos biztonság megfelelő normáin túlmenően – a minden RENDSZER számára külön kidolgozott megfelelő biztonsági eljárásokat és technikákat kell meghatározni.

7. A biztonsági intézkedések kiegyensúlyozott kombinációját kell meghatározni és végrehajtani, hogy a RENDSZER biztonságos környezetben működhessen. Ezeknek az intézkedéseknek az alkalmazási területei magukban foglalják a fizikális elemeket, a személyzetet, a nem technikai eljárásokat, valamint a számítógépes és kommunikációs üzemeltetési eljárásokat.

▼B

8. Számítógépes biztonsági intézkedésekkel (hardver és szoftver biztonsági tulajdonságokkal) kell megvalósítani a szükséges ismeret elvét, illetve megakadályozni vagy felfedni az információk engedély nélküli kiszolgáltatását. Annak mértékét, hogy mennyiben kell a számítógépes biztonsági intézkedésekre hagyatkozni, a biztonsági követelmények megállapításának folyamata során kell meghatározni. Az akkreditációs eljárás keretében kell meghatározni, hogy fennáll-e a biztonság megfelelő szintje ahhoz, hogy a számítógépes biztonsági intézkedésekre lehessen hagyatkozni.

A RENDSZERSPECIFIKUS BIZTONSÁGI KÖVETELMÉNYEK MEGÁLLAPÍTÁSA (SSRS)

9. Minden CONFIDENTIEL UE és magasabb minősítésű információt kezelő RENDSZER esetében az IT-rendszer-üzemeltetési hatóság (IT SYSTEM OPERATIONAL AUTHORITY, ITSOA) – adott esetben a projekt személyzetének és az INFOSEC-hatóságnak a hozzájárulásával és támogatásával – elkészíti a RENDSZERspecifikus biztonsági követelmények megállapítását (SYSTEM-Specific Security Requirement Statement, a továbbiakban: SSRS), amelyet az SAA hagy jóvá. SSRS-re akkor is szükség van, ha a RESTREINT UE vagy nem minősített információk integritását és rendelkezésre állását az SAA elengedhetetlennek ítéli.

10. Az SSRS-t a projekt kezdetének lehető legkorábbi szakaszában kell kidolgozni és a projekt előrehaladtával tovább kell fejleszteni és javítani; az SSRS a projekt és a RENDSZER életciklusának különböző szakaszaiban különböző szerepeket tölt be.

11. Az SSRS az IT-rendszer-üzemeltetési hatóság és az SAA között létrejött kötelező érvényű megállapodást képez, és ennek alapján akkreditálható a RENDSZER.

12. Az SSRS a betartandó biztonsági elvek és a betartandó részletes biztonsági követelmények teljes és részletes meghatározása. A Tanács biztonsági politikáján és kockázatértékelésén alapul, illetve olyan paraméterek határozzák meg, amelyek átfogják az üzemeltetési környezetet, a személyi biztonsági felhatalmazás legalacsonyabb szintjét, a kezelt információk legmagasabb minősítését, a biztonsági üzemmódot, illetve a felhasználók követelményeit. Az SSRS annak a projektdokumentációnak szerves része, amelyet a megfelelő hatóságokhoz nyújtanak be technikai, költségvetési és biztonsági jóváhagyás céljából. Végleges formájában az SSRS azoknak a feltételeknek a teljes körű leírása, amelyeknek meg kell valósulniuk ahhoz, hogy a RENDSZER biztonságos legyen.

BIZTONSÁGI ÜZEMMÓDOK

13. A CONFIDENTIEL UE és az annál magasabb minősítésű információkat kezelő valamennyi rendszer arra kap akkreditációt, hogy az alábbi biztonsági üzemmódok egyikében vagy – ha a követelmények különböző időszakok során indokolják – több biztonsági üzemmódban, illetve azok nemzeti megfelelőiben működjék:

    a) kizárólagos („dedicated”) üzemmód;

    b) domináns („system high”) üzemmód; és

    c) többszintű („multi-level”) üzemmód.

*II. fejezet*

**Fogalommeghatározások**

KIEGÉSZÍTŐ JELÖLÉSEK

14. Kiegészítő jelöléseket, úgymint a CRYPTO-t vagy bármely más, az EU által elismert, különös kezelést előíró jelölést kell alkalmazni, ha a biztonsági minősítés által meghatározottakon túlmenően korlátozott terjesztésre és különös kezelésre van szükség.

▼B

15. A KIZÁRÓLAGOS BIZTONSÁGI ÜZEMMÓD olyan üzemmódot jelent, amelyben a RENDSZERHEZ hozzáféréssel rendelkező MINDEN személy a RENDSZERBEN kezelt információk legmagasabb minősítési szintjének megfelelő biztonsági felhatalmazással rendelkezik, és minden személynek közösen szükséges ismernie a RENDSZERBEN kezelt MINDEN információt.

*Megjegyzések:*

1. Mivel mindenkinek szükséges az ismeret, nem feltétlenül szükséges, hogy a számítógépes biztonsági tulajdonságok a RENDSZEREN belül biztosítsák az információk elkülönítését.

2. A többi biztonsági tulajdonságnak (például fizikai, személyzeti és eljárási) meg kell felelnie a RENDSZERBEN kezelt információk legmagasabb minősítési szintje és minden kategóriamegjelölése követelményeinek.

16. A DOMINÁNS BIZTONSÁGI ÜZEMMÓD olyan üzemmódot jelent, amelyben a RENDSZERHEZ hozzáféréssel rendelkező MINDEN személy a RENDSZERBEN kezelt információk legmagasabb minősítési szintjének megfelelő biztonsági felhatalmazással rendelkezik, de a RENDSZERHEZ hozzáféréssel rendelkező NEM MINDEN személynek szükséges ismernie a RENDSZERBEN kezelt MINDEN információt.

*Megjegyzések:*

1. Mivel nincs minden felhasználónak általánosan szüksége minden ismeretre, a számítógépes biztonsági tulajdonságok szempontjából követelmény, hogy szelektív hozzáférést biztosítsanak a RENDSZERBEN található információkhoz, és elkülönítve kezeljék azokat.

2. A többi biztonsági tulajdonságnak (például fizikai, személyzeti és eljárásbeli) meg kell felelnie a RENDSZERBEN kezelt információk legmagasabb minősítési szintje és minden kategóriamegjelölése követelményeinek.

3. Az ebben az üzemmódban kezelt, illetve az ebben az üzemmódban a RENDSZER rendelkezésére álló valamennyi információt és a létrehozott outputot – amíg erről másként nem határoznak – olyan védelemben kell részesíteni, mintha az éppen kezelt információval azonos kategóriamegjelöléssel és a legmagasabb minősítési szinttel rendelkezne, hacsak valamelyik meglévő jelölő funkció nem biztosít kellő szintű megbízhatóságot.

17. A TÖBBSZINTŰ BIZTONSÁGI ÜZEMMÓD olyan üzemmódot jelent, amelyben a RENDSZERHEZ hozzáféréssel rendelkező személyek közül NEM MINDEN személy rendelkezik biztonsági felhatalmazással a RENDSZERBEN kezelt információk legmagasabb minősítési szintjéig, és amelyben a RENDSZERHEZ hozzáféréssel rendelkező személyek közül NEM MINDEN személynek szükséges ismernie a RENDSZERBEN kezelt minden információt.

*Megjegyzések:*

1. Ez az üzemmód egyidejűleg lehetővé teszi a különböző minősítésű és különböző kategóriamegjelölésű információk kezelését.

2. Mivel nem minden személy rendelkezik a legmagasabb szinteknek megfelelő biztonsági felhatalmazással, és nem minden személynek szükséges ismernie minden információt, ezért a számítógépes biztonsági tulajdonságok szempontjából követelmény, hogy szelektív hozzáférést biztosítsanak a RENDSZERBEN található információkhoz, és elkülönítve kezeljék azokat.

18. Az INFORMÁCIÓBIZTONSÁG (INFOSEC) olyan biztonsági intézkedések alkalmazását jelenti, amelyek célja a kommunikációs, információs és egyéb elektronikus rendszerekben kezelt, tárolt vagy továbbított információk védelme titkosságuk, integritásuk vagy rendelkezésre állásuk véletlenszerű vagy szándékos elvesztésével szemben, továbbá annak megelőzése, hogy e rendszerek maguk elveszítsék integritásukat vagy megszűnjék rendelkezésre

▼B

állásuk. Az INFOSEC intézkedések magukban foglalják a számítógépes biztonsággal, a továbbítás biztonságával, a kisugárzási biztonsággal és a kriptográfiai biztonsággal kapcsolatos intézkedéseket, valamint az információkat és a RENDSZEREKET fenyegető veszélyek felderítését, dokumentálását és leküzdését.

19. A SZÁMÍTÓGÉPES BIZTONSÁG (COMPUSEC) a számítógépes rendszerek esetében a hardver, förmver és szoftver biztonsági tulajdonságok alkalmazását jelenti abból a célból, hogy védelmet nyújtson az információk engedély nélküli kiszolgáltatásával, kezelésével, módosításával/törlésével vagy a hozzáférés megtagadásával (denial of service) szemben, illetve hogy mindezeket megelőzze.

20. A SZÁMÍTÓGÉPES BIZTONSÁGI TERMÉK olyan általános számítógépes biztonsági terméket jelent, amelyet egy IT-rendszerbe kívánnak beépíteni azért, hogy ott fokozza, illetve biztosítsa a kezelt információk titkosságát, integritását vagy rendelkezésre állását.

21. A KOMMUNIKÁCIÓS BIZTONSÁG (COMSEC) biztonsági intézkedések alkalmazását jelenti a távközlésben annak megakadályozása érdekében, hogy illetéktelen személyek a távközlési közlemények megszerzésével vagy tanulmányozásával értékes információkhoz jussanak, illetve annak érdekében, hogy biztosítsák a távközlési közlemények hitelességét.

*Megjegyzés:*

1. Ezek az intézkedések magukban foglalják a kriptográfiai biztonságot, a továbbítás biztonságát és a kisugárzási biztonságot, továbbá az eljárások biztonságát és a fizikai, a személyzeti, a dokumentációs és a számítógépes biztonságot.

22. Az ÉRTÉKELÉS a RENDSZER biztonsági vonatkozásainak, illetve valamely kriptográfiai vagy számítógépes biztonsági terméknek a megfelelő hatóság által végzett részletes technikai vizsgálatát jelenti.

*Megjegyzések:*

1. Az értékelés az igényelt biztonsági működés meglétét és az ilyen működés nem kívánatos mellékhatásainak hiányát vizsgálja, továbbá e működés szilárd ellenálló képességét méri fel.

2. Az értékelés meghatározza annak mértékét, hogy a RENDSZER biztonsági követelményeinek, illetve a számítógépes biztonsági termék biztonsági igényeinek mennyiben tesznek eleget, továbbá megállapítja a RENDSZER, illetve a kriptográfiai vagy a számítógépes biztonsági termék működésének megbízhatósági szintjét.

23. A TANÚSÍTÁS hivatalos igazolás arról, hogy – egy értékelés lefolytatásának és eredményeinek független felülvizsgálata alapján – a RENDSZER milyen mértékben tesz eleget a biztonsági követelményeknek, illetve arról, hogy a számítógépes biztonsági termék mennyiben felel meg az előre meghatározott biztonsági jellemzőknek.

24. Az AKKREDITÁCIÓ azt az engedélyt és jóváhagyást jelenti, amelyet egy RENDSZER számára kiadnak, hogy működési környezetében EU minősített információkat kezelhessen.

*Megjegyzés:*

Ilyen akkreditációra azt követően kerülhet sor, hogy az összes megfelelő biztonsági eljárást végrehajtották és elérték a rendszererőforrások védelmének elégséges szintjét. Az akkreditációt általában az SSRS alapján kell lefolytatni, és a következőkre kell kiterjednie:

a) a rendszer akkreditációja céljának meghatározása, különösen az, hogy az információk milyen minősítési szintjeit kell kezelni és melyek a javasolt rendszer- vagy hálózatbiztonsági üzemmódok;

b) kockázatkezelési értékelés készítése, amelyben azonosítják a fenyegetéseket és a sebezhető pontokat, valamint ismertetik a szükséges ellenintézkedéseket;

▼B

c) a biztonsági üzemeltetési eljárások (SecOPs), a javasolt műveletek (pl. a biztosítandó üzemmódok, szolgáltatások) részletes leírása, az akkreditáció alapjául szolgáló RENDSZERbiztonsági tulajdonságok leírását is beleértve;

d) a biztonsági tulajdonságok megvalósítására és fenntartására vonatkozó terv;

e) a kezdeti és a későbbi rendszerbiztonsági vagy hálózatbiztonsági teszt, értékelés és tanúsítás terve; továbbá

f) szükség esetén a tanúsítás az akkreditáció más elemeivel együtt.

25. Az IT-RENDSZER a berendezések, módszerek és eljárások – és adott esetben a személyi állomány – együttesét jelenti, amelyet oly módon szerveztek meg, hogy az információk kezelésének feladatait ellássa.

*Megjegyzések:*

1. Ez alatt a rendszeren belül az információk kezelésére konfigurált eszközök együttesét kell érteni.

2. Ezek a rendszerek konzultációs, irányítási, ellenőrző, kommunikációs, tudományos vagy igazgatási alkalmazásokat támogathatnak, a szövegszerkesztést is beleértve.

3. Egy rendszer határai általában az egyetlen IT-rendszer-üzemeltetési hatóság (ITSOA) ellenőrzése alá tartozó elemek együtteseként határozhatók meg.

4. Egy IT-rendszer olyan alrendszereket tartalmazhat, amelyek némelyike maga is IT-rendszer.

26. Az IT-RENDSZER-BIZTONSÁGI TULAJDONSÁGOK magukban foglalják valamennyi hardver/förmver/szoftver működést, jellemzőt és tulajdonságot; ezekhez tartoznak az üzemeltetési eljárások, az elszámoltathatósági eljárások és a hozzáférés-ellenőrzés, az IT-terület, a távoli terminál/munkaállomás területe, a vezetési követelmények, a fizikai struktúrák és készülékek, a személyzeti és kommunikációs ellenőrzések, amelyekre mind azért van szükség, hogy a védelem elfogadható szintjét biztosítsák az IT-rendszerben kezelt minősített információk számára.

27. Az IT-HÁLÓZAT az adatcsere céljából összekapcsolt IT-rendszerek földrajzilag elszórtan elhelyezkedő együttesét jelenti, amely az összekapcsolt IT-rendszerek összetevőit és a támogató adat- vagy kommunikációs hálózatokkal létrehozott interfészeiket foglalja magában.

*Megjegyzések:*

1. Egy IT-hálózat az adatcsere érdekében igénybe veheti egy vagy több egymással összekapcsolt kommunikációs hálózat szolgáltatásait. Több IT-hálózat igénybe veheti egy közös kommunikációs hálózat szolgáltatásait.

2. Az IT-hálózatot „helyi” hálózatnak nevezzük, ha több számítógépet kapcsol össze ugyanazon a helyszínen.

28. Az IT-HÁLÓZATBIZTONSÁGI TULAJDONSÁGOK a hálózatot alkotó egyes IT-rendszerek IT-rendszer-biztonsági tulajdonságait tartalmazzák azokkal a további összetevőkkel és tulajdonságokkal együtt, amelyek magához a hálózathoz kapcsolódnak (például hálózati kommunikáció, biztonsági azonosító és jelölő mechanizmusok és eljárások, hozzáférés-ellenőrzések, programok és ellenőrzési eseménynaplók), és amelyek szükségesek ahhoz, hogy a minősített információk számára a védelem elfogadható szintjét biztosítsák.

29. Az IT-TERÜLET azt a területet jelenti, ahol egy vagy több számítógép, azok helyi perifériái és tárolóegységei, vezérlőegységei, valamint a velük összekapcsolt hálózati és kommunikációs berendezések találhatók.

▼B

*Megjegyzés:*

Ez a kifejezés nem foglalja magában azt a külön területet, ahol a távoli perifériás eszközök vagy terminálok/munkaállomások találhatók, még akkor sem, ha ezek a készülékek az IT-területen lévő berendezésekkel össze vannak kapcsolva.

30. A TÁVOLI TERMINÁL/MUNKAÁLLOMÁS TERÜLETE azt a területet jelenti, ahol az IT-területtől elkülönülten számítógépek, ezek helyi perifériás eszközei vagy termináljai/munkaállomásai és a hozzájuk kapcsolódó kommunikációs berendezések találhatók.

31. A TEMPEST-ellenintézkedések olyan biztonsági intézkedések, amelyek célja a berendezések és a kommunikációs infrastruktúra védelme az ellen, hogy nem szándékos elektromágneses kisugárzás és konduktivitás útján a minősített információk illetéktelenek tudomására juthassanak.

*III. fejezet*

**Hatáskörök a biztonság terén**

ÁLTALÁNOSSÁGOK

32. A Biztonsági Bizottságnak az I. szakasz 4. pontjában meghatározott hatásköre az INFOSEC-kérdésekre is kiterjed. A Biztonsági Bizottságnak úgy kell megszerveznie tevékenységeit, hogy szakmai tanácsokat tudjon adni a fenti kérdésekben.

33. A biztonsággal kapcsolatos problémák (váratlan események, a szabályok megsértése stb.) esetében a Bizottság Biztonsági Hivatala haladéktalanul intézkedik. Minden problémát a Főtitkárság Biztonsági Hivatala elé kell terjeszteni.

34. A főtitkár/főképviselő vagy adott esetben az EU valamely decentralizált szervének a vezetője INFOSEC-hivatalt hoz létre, hogy iránymutatást adjon a biztonsági hatóságnak a RENDSZEREK részeként tervezett különleges biztonsági tulajdonságok végrehajtására és ellenőrzésére.

A BIZTONSÁGI AKKREDITÁCIÓS HATÓSÁG (SAA)

35. Attól függően, hogy mely RENDSZERT kell akkreditálni, az SAA a következők egyike lehet:

— a) egy nemzeti biztonsági hatóság (NSA);

— b) egy, a főtitkár/főképviselő által kijelölt hatóság;

— c) az EU valamely decentralizált szervének a biztonsági hatósága; vagy

— d) ezek delegált/kijelölt képviselői.

36. Az SAA felel annak biztosításáért, hogy a RENDSZEREK megfeleljenek a Tanács biztonsági politikájának. Egyik feladata az, hogy a RENDSZEREK számára megadja a jóváhagyást EU minősített információk kezelésére a működési környezetükben meghatározott minősítési szintig. A Főtitkárság, illetve adott esetben az EU decentralizált szervei tekintetében az SAA a főtitkár/főképviselő, illetve a decentralizált szervek vezetői nevében viseli a biztonsággal kapcsolatos felelősséget.

A főtitkársági SAA hatásköre kiterjed minden, a Főtitkárság helyiségeiben működő RENDSZERRE. Az egyes tagállamokban üzemeltetett RENDSZEREK és azok alkotórészei az illető tagállam hatáskörében maradnak. Ha valamely RENDSZER eltérő alkotórészei a főtitkársági SAA és egyéb SAA-k hatáskörébe kerülnek, a felek közös akkreditációs bizottságot állítanak föl, amelynek tevékenységét a főtitkársági SAA hangolja össze.

AZ INFOSEC-HATÓSÁG (IA)

37. Az INFOSEC-hatóság felel az INFOSEC-hivatal tevékenységeiért. A Főtitkárságot, illetve adott esetben az EU decentralizált szerveit illetően az INFOSEC-hatóság felel az alábbiakért:

▼B

— technikai tanácsadás és támogatás nyújtása az SAA számára,

— részvétel az SSRS kidolgozásában;

— az SSRS felülvizsgálata annak érdekében, hogy összhangban legyen ezzel a biztonsági szabályzattal, valamint az INFOSEC-politika és -architektúra dokumentumaival,

— adott esetben részvétel az akkreditációs testületekben/bizottságokban, és az akkreditációval kapcsolatos INFOSEC-ajánlások elkészítése az SAA számára,

— támogatás nyújtása az INFOSEC-képzéssel és -oktatással kapcsolatos tevékenységekhez,

— technikai tanácsadás nyújtása az INFOSEC vonatkozású váratlan események kivizsgálása során,

— technikai irányadó elvek kidolgozása annak biztosítása érdekében, hogy csak engedélyezett szoftvereket lehessen felhasználni.

AZ IT-RENDSZER-ÜZEMELTETÉSI HATÓSÁG (ITSOA)

38. A RENDSZER vezérlésének és biztonsági tulajdonságainak a végrehajtásáért és működtetéséért viselt felelősséget az INFOSEC-hatóságnak a lehető legkorábbi szakaszban át kell ruháznia az IT-rendszer-üzemeltetési hatóságra (IT-System Operational Authority, ITSOA). Ez a felelősség a RENDSZER teljes életciklusa alatt, a projekt eltervezésétől egészen a végső megszüntetéséig fennáll.

39. Az ITSOA felel az egész RENDSZER részeként tervezett minden biztonsági intézkedésért. Ez a felelősség magában foglalja a biztonsági üzemeltetési eljárások (Security Operating Procedures, SecOPs) kialakítását. Az ITSOA határozza meg azokat a biztonsági normákat és eljárásokat, amelyeket a RENDSZER szállítóinak be kell tartaniuk.

40. Amennyiben szükséges, az ITSOA átruházhatja hatáskörének egyes részeit például az INFOSEC-tisztviselőre vagy a munkaterület szerint illetékes INFOSEC-tisztviselőre. Egy személy különböző INFOSEC-feladatokat is elláthat.

FELHASZNÁLÓK

41. Valamennyi felhasználó felel azért, hogy tevékenységével ne veszélyeztesse az általa használt RENDSZER biztonságát.

INFOSEC-KÉPZÉS

42. A Főtitkárságon, az EU decentralizált szervein vagy a tagállamok kormányzati szervein belül különböző szintű és adott esetben különböző személyzetet megcélzó INFOSEC-képzést és oktatást kell biztosítani.

*IV. fejezet*

**Nem technikai jellegű biztonsági intézkedések**

SZEMÉLYZETI BIZTONSÁG

43. A RENDSZER felhasználóinak az adott RENDSZERBEN kezelt információk minősítésének és tartalmának megfelelő biztonsági felhatalmazással és jogos információigénnyel kell rendelkezniük. A RENDSZEREK biztonsága szempontjából meghatározó egyes berendezésekhez vagy információkhoz való hozzáféréshez különleges, a tanácsi eljárásoknak megfelelően megadott felhatalmazás szükséges.

44. Az SAA jelöli ki az összes biztonsági szempontból kritikus beosztást és határozza meg, hogy az azokat betöltő személyzetet milyen biztonsági ellenőrzésnek és felügyeletnek kell alávetni.

45. A RENDSZEREK meghatározása és tervezése úgy történik, hogy megkönnyítse a hatáskörök és a feladatok elosztását a személyi állomány körében

▼B

oly módon, hogy egy személyben teljeskörűen senki ne ismerhesse meg vagy ellenőrizhesse a kulcsfontosságú rendszerbiztonsági pontokat. Azt a célt kell kitűzni, hogy a rendszer vagy a hálózat módosítása vagy szándékos rongálása két vagy több személy összejátszása nélkül ne legyen lehetséges.

FIZIKAI BIZTONSÁG

46. A (a 29. és 30. pont szerinti) IT-területek, illetve távoli terminál/munkaállomás területek, ahol IT eszközökkel CONFIDENTIEL UE vagy annál magasabb minősítésű információkat kezelnek, vagy ahol ilyen információkhoz potenciálisan hozzá lehet férni, EU I. vagy II. osztályba tartozó, illetve adott esetben az ezeknek megfelelő nemzeti biztonsági területként kerülnek meghatározásra.

47. Azokon az IT-területen és távoli terminál/munkaállomás területeken, ahol a RENDSZER biztonsága módosítható, az arra felhatalmazott tisztviselő vagy más alkalmazott egyedül soha nem tartózkodhat.

A RENDSZERHEZ VALÓ HOZZÁFÉRÉS ELLENŐRZÉSE

48. Mindazok az információk és anyagok, amelyek lehetővé teszik egy RENDSZERHEZ való hozzáférés ellenőrzését, az általuk hozzáférhető információk legmagasabb minősítésének és kategóriamegjelölésének megfelelő védelemben részesülnek.

49. Ha a hozzáférés ellenőrzésére szolgáló információkat és anyagokat e célra a továbbiakban nem használják fel, akkor azokat a 61-63. pontnak megfelelően meg kell semmisíteni.

*V. fejezet*

**Technikai jellegű biztonsági intézkedések**

AZ INFORMÁCIÓBIZTONSÁG

50. Az információ kibocsátójának a feladata, hogy beazonosítson és minősítsen minden információt hordozó dokumentumot, legyen az akár nyomtatott formában, akár számítógépes adathordozón. A kinyomtatott anyag minden oldalán alul és felül fel kell tüntetni az anyag minősítését. Az előállított anyagnak – akár nyomtatott formában, akár számítógépes adathordozón áll rendelkezésre – ugyanazt a minősítést kell kapnia, mint amivel a készítéséhez felhasznált legmagasabb minősítésű információ rendelkezik. A RENDSZER üzemmódja is befolyásolhatja az adott rendszerben előállított anyagok minősítését.

51. Egy szervezetnek és az információbirtokosoknak a feladata, hogy megvizsgálják az egyes információs elemek halmozódásának és az összefüggő elemekből levonható következtetéseknek a problematikáját és eldöntsék, hogy az információk összességére nézve szükség van-e magasabb szintű minősítésre vagy sem.

52. Az a tény, hogy az információ rövidített kód vagy átviteli kód, illetve bináris ábrázolás formájában áll rendelkezésre, semmilyen biztonsági védelmet nem ad és ezért nem befolyásolhatja az információ minősítését.

53. Ha információt egyik RENDSZERBŐL egy másikba továbbítanak, az információnak a továbbítás közben és a fogadó RENDSZERBEN az információ eredeti minősítésének és kategóriájának megfelelő védelemben kell részesülnie.

54. Valamennyi számítógépes adathordozó a tárolt információ, illetve az adathordozó megjelölése szerinti legmagasabb minősítésnek megfelelően kezelendő, és mindenkor ennek megfelelő védelemben részesítendő.

55. Az EU minősített információk rögzítésére szolgáló, újból felhasználható számítógépes adathordozók mindaddig megtartják a korábbi használatuk során alkalmazott legmagasabb minősítésüket, amíg az adott információt megfelelő módon vissza nem minősítik vagy a minősítést meg nem szüntetik, és az adathordozót ennek megfelelően át nem minősítik, illetve amíg a

▼B

Főtitkárság vagy valamely tagállam által jóváhagyott eljárásnak megfelelően (lásd a 61. és 63. pontot) minősítését meg nem szüntetik vagy meg nem semmisítik.

**AZ INFORMÁCIÓK ELLENŐRZÉSE ÉS AZ AZOKKAL VALÓ ELSZÁMOLÁS KÖTELEZETTSÉGE**

56. A SECRET UE és az annál magasabb minősítésű információkhoz történő hozzáférésről automatikus eseménynapló (audit trails) készül vagy azt kézzel vezetett naplóban kell nyilvántartani. Ezeknek a nyilvántartásoknak a megőrzése e biztonsági szabályzatnak megfelelően történik.

57. Az IT-területen outputként rendelkezésre álló EU minősített anyagokat egyetlen minősített anyagként lehet kezelni, és nem szükséges nyilvántartásba venni, feltéve hogy az anyag beazonosítása megtörtént, minősítése fel van tüntetve rajta és azt megfelelő módon ellenőrzik.

58. Ha egy anyagot EU minősített információkat kezelő RENDSZER segítségével állítanak elő és azt egy IT-területről egy távoli terminál/munkaállomás területére továbbítják, akkor az ilyen anyag ellenőrzésére az SAA jóváhagyásával kialakított eljárások szolgálnak. A SECRET UE és az annál magasabb minősítésű anyagok esetében ezek az eljárások meghatározott utasításokat tartalmaznak az információkkal való elszámolás kötelezettségére vonatkozóan.

**AZ ELTÁVOLÍTHATÓ SZÁMÍTÓGÉPES ADATHORDOZÓK KEZELÉSE ÉS ELLENŐRZÉSE**

59. Minden CONFIDENTIEL UE és annál magasabb minősítésű számítógépes adathordozó anyagként kezelendő és az általános szabályok vonatkoznak rá. A megfelelő azonosító és minősítési jelöléseket az adathordozók sajátos fizikai megjelenését tekintetbe véve kell alkalmazni, azok egyértelmű felismerhetőségének biztosítása érdekében.

60. A felhasználók felelnek annak biztosításáért, hogy az EU minősített információkat megfelelő minősítési jelöléssel ellátott adathordozókon tárolják és megfelelő védelemben részesítsék. Meg kell határozni azokat az eljárásokat, amelyek biztosítják, hogy a számítógépes adathordozókon található információk tárolása az EU információk valamennyi szintje tekintetében e biztonsági szabályzatnak megfelelően történjék.

**A SZÁMÍTÓGÉPES ADATHORDOZÓK MINŐSÍTÉSÉNEK MEGSZÜNTETÉSE ÉS AZ ILYEN ADATHORDOZÓK MEGSEMMISÍTÉSE**

61. Az EU minősített információk rögzítésére szolgáló számítógépes adathordozókat a Főtitkárság vagy valamely tagállam által jóváhagyott eljárásnak megfelelően lehet visszaminősíteni vagy minősítésüket megszüntetni.

62. Nem lehet minősítésüket megszüntetni vagy újból felhasználni azokat a számítógépes adathordozókat, amelyeken korábban TRÈS SECRET UE/EU TOP SECRET minősítésű vagy különleges kategóriájú információkat tároltak.

63. Ha egy számítógépes adathordozó minősítését nem lehet megszüntetni, illetve az nem használható fel újra, akkor azt a Főtitkárság vagy valamely tagállam által jóváhagyott eljárásnak megfelelően meg kell semmisíteni.

KOMMUNIKÁCIÓS BIZTONSÁG

64. Elektromágneses úton továbbított EU minősített információk esetében különleges intézkedéseket kell tenni az ilyen továbbítások titkosságának, integritásának és rendelkezésre állásának védelme érdekében. Az SAA határozza meg a továbbítások felderítéssel és lehallgatással szemben biztosítandó védelmének követelményeit. A kommunikációs rendszerben továbbításra kerülő információkat a titkossággal, az integritással és a rendelkezésre állással szemben támasztott követelmények alapján kell védeni.

65. Ha a titkosság, az integritás és a rendelkezésre állás védelméhez kriptográfiai módszerek szükségesek, akkor ezeket a módszereket és a kapcsolódó termékeket az SAA-nak kifejezetten erre a célra jóvá kell hagynia.

▼B

66. Továbbítás során a SECRET UE és magasabb minősítésű információk titkosságát a Tanács Biztonsági Bizottságának ajánlása alapján a Tanács által jóváhagyott kriptográfiai módszerekkel vagy termékekkel kell védeni. Továbbítás során a RESTREINT UE vagy CONFIDENTIEL UE információk titkosságát a Tanács Biztonsági Bizottságának ajánlása alapján a főtitkár/főképviselő által vagy valamely tagállam által jóváhagyott kriptográfiai módszerekkel vagy termékekkel kell védeni.

67. Az EU minősített információk továbbítására alkalmazandó részletes szabályokat külön biztonsági utasításokban kell meghatározni, melyeket a Tanács Biztonsági Bizottságának ajánlása alapján a Tanács hagy jóvá.

68. Kivételes működési körülmények között a RESTREINT UE, a CONFIDENTIEL UE és a SECRET UE minősítésű információk rejtjelezés nélkül is továbbíthatók, feltéve hogy erre minden egyes esetben kifejezetten engedélyt adnak. Ezek a kivételes körülmények a következők:

a) fenyegető vagy tényleges válság-, konfliktus- vagy háborús helyzet; valamint

b) ha a gyors kézbesítés mindennél fontosabb és nem állnak rendelkezésre rejtjelező eszközök, továbbá úgy értékelik, hogy a továbbított információ nem használható fel időben ahhoz, hogy a folyamatokat hátrányosan befolyásolja.

69. A RENDSZEREKNEK képesnek kell lenniük arra, hogy szükség esetén, fizikai kapcsolatmegszakítás útján vagy az SAA által jóváhagyott speciális szoftvertulajdonságok segítségével, egyik vagy mindegyik távoli munkaállomásukon vagy terminájukon kategorikusan megtagadják a hozzáférést az EU minősített információkhoz.

TELEPÍTÉSI ÉS KISUGÁRZÁSI BIZTONSÁG

70. A RENDSZEREK első telepítését és azok későbbi nagyobb változtatásait oly módon kell szabályozni, hogy a telepítést biztonsági szempontból ellenőrzött telepítők végezzék olyan technikailag képzett személyzet állandó felügyelete mellett, amely az EU minősített információkhoz való hozzáférés tekintetében a rendszerben várhatóan tárolni vagy kezelni kívánt információk legmagasabb minősítési szintjének megfelelő biztonsági felhatalmazással rendelkezik.

71. Minden berendezést a Tanács érvényes biztonsági politikájának megfelelően kell telepíteni.

72. A CONFIDENTIEL UE és az annál magasabb minősítésű információkat kezelő RENDSZEREK olyan védelemben részesülnek, hogy biztonságukat ne fenyegethesse kompromittáló kisugárzás, amelynek tanulmányozása és ellenőrzése a „TEMPEST” elnevezést kapta.

73. A TEMPEST-nek a Főtitkárságon és az EU decentralizált szerveinél működő berendezések számára kialakított ellenintézkedéseit a Főtitkárság Biztonsági Hatósága által kijelölt TEMPEST-hatóság vizsgálja felül és hagyja jóvá. Az EU minősített információkat kezelő nemzeti berendezések esetében a jóváhagyó hatóság az elismert nemzeti TEMPEST-jóváhagyó hatóság.

*VI. fejezet*

**Biztonság a kezelés során**

BIZTONSÁGI ÜZEMELTETÉSI ELJÁRÁSOK

74. A biztonsági üzemeltetési eljárások (SecOPs) határozzák meg a biztonsági ügyekben elfogadásra kerülő elveket, a követendő üzemeltetési eljárásokat és a személyzet hatáskörét. A biztonsági üzemeltetési eljárások kidolgozásáért az IT-rendszer-üzemeltetési hatóság (ITSOA) felel.

SZOFTVERVÉDELEM ÉS KONFIGURÁCIÓKEZELÉS

▼B

75. Az alkalmazási programok biztonsági védelmét magának a programnak, nem pedig az általa kezelendő információknak a biztonsági minősítése alapján kell meghatározni. A használt szoftverek változatait integritásuk és megfelelő működésük biztosítása érdekében rendszeres időközönként ellenőrizni kell.

76. A szoftverek új vagy módosított változatait csak azután lehet EU minősített információk kezelésére használatba venni, ha az ITSOA bevizsgálta azokat.

**KÁRTÉKONY SZOFTVEREK ÉS SZÁMÍTÓGÉPES VÍRUSOK KISZŰRÉSE**

77. A kártékony szoftverek és számítógépes vírusok kiszűrését az SAA által előírt követelményeknek megfelelően rendszeres időközönként kell végezni.

78. A Főtitkárságra, az EU decentralizált szerveihez vagy a tagállamokhoz érkező minden számítógépes adathordozót csak azután lehet bármely RENDSZERBE bevinni, hogy a kártékony szoftverek és számítógépes vírusok kiszűrését szolgáló ellenőrzés megtörtént.

KARBANTARTÁS

79. A kész SSRS-sel rendelkező RENDSZEREK terv szerinti és kérésre történő karbantartására vonatkozó szerződések és eljárások meghatározzák, hogy az IT-területre belépő karbantartó személyzetnek és felszerelésüknek mely követelményeknek és rendelkezéseknek kell eleget tenniük.

80. A követelményeket az SSRS-ben és az eljárásokat a SecOPs-ben pontosan meg kell határozni. Csak kivételes körülmények esetén engedélyezhető, hogy a karbantartást végző szerződéses megbízott távoli hozzáférést igénylő diagnosztikai eljárást alkalmazzon, és akkor is csak szigorú biztonsági ellenőrzés mellett és csak az SAA jóváhagyásával.

*VII. fejezet*

**Beszerzés**

81. Bármely biztonsági termék csak akkor használható a beszerzendő RENDSZERREL együtt, ha a megfelelő értékelő vagy tanúsító szerv által nemzetközileg elismert kritériumok (mint például az Információtechnológia Biztonsági Értékelésének Közös Kritériumai, lásd ISO 15 408) szerint végzett értékelésére és tanúsítására már sor került vagy az folyamatban van.

82. Annak eldöntésénél, hogy egy berendezést, különösen egy számítógépes adathordozót inkább bérbe vegyenek vagy megvásároljanak, azt kell szem előtt tartani, hogy az ilyen berendezés – ha egyszer már EU minősített információk kezelésére használták – csak akkor vihető ki a megfelelően biztonságos környezetből, ha az SAA jóváhagyásával minősítését megszüntették, azonban ez a jóváhagyás nem mindig lehetséges.

AKKREDITÁCIÓ

83. Az EU minősített információk kezelése előtt minden olyan RENDSZERT, amelyre vonatkozólag SSRS-t kell készíteni, az SAA-nak akkreditálnia kell az SSRS-ben, a SecOPs-ban és az egyéb vonatkozó dokumentációban előírt információk alapján. Az alrendszereket és a távoli terminálokat/munkaállomásokat minden olyan RENDSZER részeként akkreditálni kell, amellyel össze vannak kapcsolva. Ha a RENDSZER egyszerre szolgálja ki a Tanácsot és valamely más szervezetet, akkor a Tanács és az érintett biztonsági hatóságok közös egyetértéssel állapodnak meg az akkreditációról.

84. Az akkreditációs eljárás egy, az adott RENDSZERHEZ igazított és az SAA által meghatározott akkreditációs stratégiának megfelelően folytatható le.

ÉRTÉKELÉS ÉS TANÚSÍTÁS

85. Bizonyos esetekben az akkreditáció előtt a RENDSZER hardver, förmver és szoftver biztonsági tulajdonságait értékelni kell és tanúsítani, hogy azok alkalmasak az információk megvédésére a minősítés tervezett szintjén.

▼B

86. A rendszer tervezésének ki kell térnie értékelési és tanúsítási követelményekre, és az SSRS-ben világosan meg kell határozni azokat.

87. Az értékelési és tanúsítási eljárást a jóváhagyott iránymutatásoknak megfelelően az ITSOA megbízásából eljáró, technikailag képzett és megfelelő biztonsági felhatalmazással rendelkező személyzet folytatja le.

88. A munkacsoportok állhatnak valamely kijelölt tagállam értékelési vagy tanúsítási hatóságából vagy annak kijelölt képviselőiből, például egy hozzáértő és biztonsági felhatalmazással rendelkező szerződéses megbízottból.

89. Az értékelési és tanúsítási eljárások leegyszerűsíthetők (például csak az integrációs szempontokra korlátozódhatnak), ha a RENDSZEREK meglévő, nemzeti szinten már értékelt és tanúsított számítógépes biztonsági termékeken alapulnak.

**A BIZTONSÁGI TULAJDONSÁGOK RENDSZERES ELLENŐRZÉSE AZ AKKREDITÁCIÓ FENNTARTÁSA ÉRDEKÉBEN**

90. Az ITSOA állapítja meg azokat a rendszeres ellenőrzési eljárásokat, amelyek biztosítják, hogy a RENDSZER valamennyi biztonsági tulajdonsága mindig fennálljon.

91. Az újbóli akkreditációt szükségessé tevő, illetve az SAA előzetes jóváhagyásához kötött változások fajtáit világosan meg kell határozni és körül kell írni az SSRS-ben. Olyan jellegű módosítás, javítás vagy üzemzavar után, amely kihatással lehetett a RENDSZER biztonsági tulajdonságaira, az ITSOA gondoskodik annak az ellenőrzésnek a végrehajtásáról, amellyel megállapítható a biztonsági tulajdonságok megfelelő működése. A RENDSZER akkreditációjának fennmaradása rendszerint az ellenőrzések kielégítő eredményétől függ.

92. Az SAA rendszeresen ellenőrzi vagy felülvizsgálja mindazokat a RENDSZEREKET, amelyekben biztonsági tulajdonságokat hoztak létre. A TRÈS SECRET UE/EU TOP SECRET vagy további jelölésekkel ellátott információkat kezelő RENDSZEREKET évente legalább egyszer meg kell vizsgálni.

*VII. fejezet*

**Ideiglenes vagy alkalomszerű felhasználás**

**A MIKROSZÁMÍTÓGÉPEK ÉS SZEMÉLYI SZÁMÍTÓGÉPEK BIZTONSÁGA**

93. Az önálló üzemmódban vagy hálózatba szervezett konfigurációban működő, beépített merevlemezzel (vagy egyéb nem felejtő adathordozóval) rendelkező mikroszámítógépek és személyi számítógépek, valamint a beépített merevlemezzel rendelkező hordozható számítástechnikai készülékek (például hordozható PC-k és elektronikus „notebook” – ok) ugyanúgy információk tárolására szolgáló adathordozónak minősülnek, mint a flopilemezek vagy az egyéb eltávolítható számítógépes adathordozók.

94. Ezeknek a berendezéseknek a hozzáférés, a kezelés, a tárolás és a szállítás tekintetében a védelem olyan szintjében kell részesülniük, ami a korábban általuk tárolt vagy kezelt információk legmagasabb minősítési szintjének felel meg (a jóváhagyott eljárásoknak megfelelően végrehajtott visszaminősítésig vagy a minősítés ezeknek megfelelő megszüntetéséig).

**MAGÁNTULAJDONBAN LÉVŐ IT-BERENDEZÉSEK FELHASZNÁLÁSA HIVATALOS TANÁCSI MUNKÁRA**

95. Tilos magántulajdonban lévő, eltávolítható számítógépes adathordozó, szoftver és tárolókapacitással rendelkező IT-hardver (például PC-k és hordozható számítástechnikai készülékek) felhasználása EU minősített információk kezelésére.

96. A Főtitkárság Biztonsági Hivatala, egy tagállam hatósága vagy az EU decentralizált szerve vezetőjének engedélye nélkül magántulajdonban lévő

▼B

hardvert, szoftvert és adathordozót tilos olyan I. vagy II. osztályba tartozó területre bevinni, ahol EU minősített információkat kezelnek.

**SZERZŐDÉSES MEGBÍZOTT TULAJDONÁBAN LÉVŐ VAGY EGY TAGÁLLAM ÁLTAL BIZTOSÍTOTT IT-BERENDEZÉSEK FELHASZNÁLÁSA HIVATALOS TANÁCSI MUNKÁRA**

97. A szerződéses megbízott tulajdonában álló IT-berendezéseket és szoftvereket csak a Főtitkárság Biztonsági Hivatala, egy tagállam hatósága vagy az EU decentralizált szerve vezetőjének az engedélyével lehet hivatalos tanácsi munkára használni. Egy tagállam által biztosított IT-berendezések és szoftverek használata engedélyezhető a Főtitkárságon vagy az EU érintett decentralizált szervénél dolgozó alkalmazottaknak, de ebben az esetben a berendezéseket a Főtitkárság megfelelő leltárának ellenőrzése alá kell vonni. Amennyiben az IT-berendezést EU minősített információ kezelésére kívánják felhasználni, úgy ez ügyben előbb az SAA-val kell konzultálni annak érdekében, hogy az adott berendezés használatára vonatkozó INFOSEC-elemeket megfelelően figyelembe vegyék és végrehajtsák.

▼B

XII. SZAKASZ

## EU MINŐSÍTETT INFORMÁCIÓK ÁTADÁSA HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE

AZ EU MINŐSÍTETT INFORMÁCIÓK ÁTADÁSÁT SZABÁLYOZÓ ELVEK

1. Az EU minősített információk harmadik államoknak való átadásáról a Tanács határoz a következők alapján:

   — az ilyen információk természete és tartalma,

   — a szükséges ismeret elve az átvevők tekintetében,

   — ennek előnyei az EU szempontjából.

   A szóban forgó EU minősített információk átadásához a kibocsátó beleegyezése szükséges.

2. Ezeket a határozatokat eseti alapon hozzák az alábbiaktól függően:

   — az együttműködés kívánatos mértéke az érintett harmadik állammal vagy nemzetközi szervezettel,

   — az iránt tanúsítható bizalom, amely annak a biztonsági szintnek a függvénye, amelyet a kérdéses államra vagy szervezetre bízott EU minősített információk tekintetében ott alkalmaznának, illetve annak, hogy az ott és az EU-ban alkalmazott biztonsági szabályok mennyiben egyeztethetők össze; e kérdésről a Tanács Biztonsági Bizottsága szakvéleményt ad a Tanács számára.

3. Az EU minősített információk harmadik állam vagy nemzetközi szervezet részéről történő elfogadása kötelezettségvállalást jelent arra nézve, hogy az információkat kizárólag azokra a célokra használják majd fel, amelyek érdekében átadásukat vagy kicserélésüket kérték, továbbá hogy biztosítani fogják a Tanács által előírt védelmet.

SZINTEK

4. Ha a Tanács úgy határozott, hogy valamely minősített információt át lehet adni egy adott államnak vagy nemzetközi szervezetnek, illetve azokkal ezt az információt ki lehet cserélni, meghatározza az együttműködés lehetséges szintjét. Ez különösen az illető állam vagy szervezet által alkalmazott biztonsági politikától és biztonsági rendelkezésektől függ.

5. Az együttműködésnek három szintje létezik:

   *1. szint* Együttműködés olyan harmadik államokkal vagy nemzetközi szervezetekkel, amelyek biztonsági politikája és rendelkezései nagyon közel állnak az EU biztonsági politikájához és rendelkezéseihez.

   *2. szint* Együttműködés olyan harmadik államokkal vagy nemzetközi szervezetekkel, amelyek biztonsági politikája és rendelkezései jelentősen eltérnek az EU biztonsági politikájától és rendelkezéseitől.

   *3. szint* Alkalmi együttműködés olyan harmadik államokkal vagy nemzetközi szervezetekkel, amelyek biztonsági politikája és rendelkezései nem értékelhetők.

6. Az egyes együttműködési szintek határozzák meg, hogy milyen – a Tanács Biztonsági Bizottsága szakvéleményének tükrében az egyes eseteknek megfelelően újrafogalmazott – biztonsági szabályok alkalmazását kérik a kedvezményezettektől a nekik átadott minősített információ védelme érdekében. Ezeket az eljárásokat és biztonsági szabályokat a 4., 5. és 6. függelék részletezi.

MEGÁLLAPODÁSOK

7. Ha a Tanács úgy határozott, hogy tartós vagy hosszú távú igény van minősített információk cseréjére az EU és harmadik államok vagy más nemzetközi szervezetek között, akkor „minősített információk cseréjére vonatkozó biztonsági eljárásokról szóló megállapodást” dolgoz ki velük, meghatározva

▼B

az együttműködés célját és a kicserélt információk védelmére vonatkozó kölcsönös szabályokat.

8. A 3. szintű alkalmi együttműködés esetében, amely időben és tárgyát tekintve értelemszerűen korlátozott, a kicserélendő információk természetét és az adott információkkal kapcsolatos kölcsönös kötelezettségeket meghatározó egyszerű egyetértési megállapodás léphet a „minősített információk cseréjére vonatkozó biztonsági eljárásokról szóló megállapodás” helyébe azzal a feltétellel, hogy ezen információk minősítése legfeljebb RESTREINT UE lehet.

9. A biztonsági eljárásokról szóló megállapodások vagy egyetértési megállapodások tervezetét a Biztonsági Bizottság megvitatja, mielőtt azokat a Tanácshoz határozathozatalra benyújtják.

10. A nemzeti biztonsági hatóságok megadják a főtitkár/főképviselő számára mindazt a szükséges segítséget, amivel biztosítható, hogy az átadandó információkat a biztonsági eljárásokról szóló megállapodásokban vagy a vonatkozó egyetértési megállapodásokban foglalt rendelkezéseknek megfelelően használják fel és részesítsék védelemben.

▼M3

XIII. SZAKASZ

**AZ IPARI BIZTONSÁGRA VONATKOZÓ KÖZÖS MINIMUMSZABÁLYOK**

1. Ez a szakasz azon ipari tevékenységek biztonsági vonatkozásaival foglalkozik, amelyek elengedhetetlenek az EU minősített információt magukban foglaló, azzal járó és/vagy azt tartalmazó feladatok elvégzésére felhatalmazó szerződések tárgyalásához, illetve megkötéséhez, valamint e feladatok ipari vagy egyéb szervezetek által történő elvégzéséhez, beleértve az EU minősített információ közbeszerzési eljárás során történő kiadását, illetve az ahhoz való hozzáférést (ajánlattételi időszak és szerződéskötést megelőző tárgyalások).

FOGALOMMEGHATÁROZÁSOK

2. E közös minimumszabályok alkalmazásában:

a) „minősített szerződés”: bármely, áruellátásra, munkálatok elvégzésére, illetve szolgáltatásnyújtásra irányuló szerződés, ahol e feladatok elvégzése EU minősített információhoz való hozzáférést, vagy ilyen információ keletkeztetését teszi szükségessé vagy foglalja magában;

b) „minősített alvállalkozói szerződés”: olyan, valamely vállalkozó által egy másik vállalkozóval (azaz alvállalkozóval) kötött, áruellátásra, munkálatok elvégzésére, illetve szolgáltatásnyújtásra irányuló szerződés, ahol e feladatok elvégzése EU minősített információhoz való hozzáférést, vagy ilyen információ keletkeztetését teszi szükségessé vagy foglalja magában;

c) „vállalkozó”: szerződéskötési képességgel rendelkező természetes vagy jogi személy;

d) „kijelölt biztonsági hatóság (DSA)” egy adott EU tagállam nemzeti biztonsági hatóságának (NSA) felelő hatóság, amelynek feladata az ipari vagy egyéb szervezetek tájékoztatása az ipari biztonságot érintő ügyekre vonatkozó nemzeti politikáról, valamint iránymutatás és segítségnyújtás biztosítása e politikák végrehajtása során. A DSA feladatait az NSA is elvégezheti;

e) „létesítménybiztonsági engedély”: annak az NSA/DSA által történő hivatalos meghatározása, hogy biztonsági szempontból egy létesítmény megfelelő biztonsági védelmet tud-e nyújtani a meghatározott biztonsági minősítésű szintű EU minősített információnak, illetve hogy az EU minősített információhoz hozzáférő személyeket megfelelő biztonsági ellenőrzésnek vetették-e alá, és tájékoztatták-e őket az EU minősített információhoz való hozzáféréshez, illetve az annak védelméhez szükséges vonatkozó biztonsági követelményekről;

f) „ipari vagy egyéb szervezet”: áruellátással, munkálatok elvégzésével vagy szolgáltatásnyújtással foglalkozó szervezet; ez magában foglalhat ipari, kereskedelmi, szolgáltatói, tudományos, kutatási, oktatási és fejlesztési tevékenységet végző szervezeteket;

g) „ipari biztonság”: védintézkedések és -eljárások alkalmazása, a vállalkozó vagy alvállalkozó által kezelt EU minősített információ szerződéskötést megelőző tárgyalás és szerződéskötés során történő elvesztésének vagy veszélyeztetésének megelőzése, felderítése és pótlása érdekében;

h) „nemzeti biztonsági hatóság” (NSA): valamely EU tagállam kormányának hatósága, amelynek alapvető feladata az EU minősített információ védelme;

i) „a szerződés biztonsági minősítésének általános szintje”: a teljes szerződés biztonsági minősítésének megállapítása, amely a teljes szerződés bármely része értelmében keletkeztetendő, kiadandó, hozzáférhető vagy keletkeztethető, kiadható, hozzáférhető információ és/vagy anyag minősítése alapján történik. A szerződés biztonsági minősítésének általános szintje nem lehet alacsonyabb bármely részének legmagasabb minősítési szintjétől, magasabb azonban az összesítés hatása miatt lehet;

▼M3

j) „biztonsági vonatkozások záradéka (SAL)”: az egyedi szerződéses feltételek szerződő hatóság által összeállított jegyzéke, amely szerves részét képezi az EU minősített információhoz való hozzáférést vagy ilyen információ keletkeztetését magában foglaló minősített szerződésnek, s amely meghatározza a biztonsági követelményeket, illetve a szerződésnek a biztonsági védelmet igénylő elemeit;

k) „biztonsági minősítési útmutató (SCG)”: olyan dokumentum, amely – az alkalmazandó biztonsági minősítési szint meghatározása mellett – leírja egy program vagy szerződés minősített elemeit. Az SCG kiterjeszthető a program vagy szerződés teljes időtartamára, az egyes információk pedig újraosztályozhatók, illetve alacsonyabb szintbe sorolhatók. Az SCG a SAL részét képezi.

SZERVEZÉS

3. A Tanács Főtitkársága szerződéses úton megbízhat valamely tagállamban bejegyzett ipari vagy egyéb szervezetet EU minősített információt magában foglaló, azzal járó és/vagy azt tartalmazó feladatokkal.

4. A Tanács Főtitkársága biztosítja, hogy a minősített szerződések odaítélésekor az ezen minimumszabályokból eredő valamennyi előírást betartják.

5. Valamennyi tagállam biztosítja, hogy nemzeti biztonsági hatóságuk (NSA) rendelkezzen az ipari biztonságra vonatkozó, ezen minimumszabályok alkalmazásához szükséges struktúrákkal. Ezek magukban foglalhatnak egy vagy több kijelölt biztonsági hatóságot (DSA).

6. Az EU minősített információ ipari vagy egyéb szervezeten belüli védelme alapvetően az adott szervezet vezetőségének felelőssége.

7. Az e minimumszabályok hatálya alá eső szerződések vagy alvállalkozói szerződések odaítélésekor a Tanács Főtitkársága és/vagy az NSA/DSA, adott esetben azonnal értesíti annak a tagállamnak a nemzeti biztonsági hatóságát/kijelölt biztonsági hatóságát, amelyben az érintett vállalkozó vagy alvállalkozó be van jegyezve.

MINŐSÍTETT SZERZŐDÉSEK

8. A minősített szerződések biztonsági minősítése az alábbi elvek figyelembevételével történik:

a) a Tanács Főtitkársága meghatározza, adott esetben, a szerződés védelmet igénylő vonatkozásait, és az abból következő biztonsági minősítést; ennek során figyelembe veszi a szerződés odaítélése előtt keletkezett információnak a kibocsátó általi, eredeti biztonsági minősítését;

b) a szerződés minősítésének általános szintje nem lehet alacsonyabb bármely elemének legmagasabb minősítési szintjétől;

c) a szerződéses tevékenységek során keletkezett EU minősített információ minősítése az SCG-vel összhangban történik;

d) szükség estén a Tanács Főtitkársága felelős a szerződés általános minősítési szintjének vagy a szerződés bármely eleme biztonsági minősítésének – a kibocsátóval folytatott konzultációt követő – megváltoztatásáért és az érintett feleknek az erről történő tájékoztatásáért;

e) a vállalkozónak vagy alvállalkozónak kiadott, illetve a szerződéses tevékenység során keletkezett minősített információ kizárólag a minősített szerződésben meghatározott célokra használható fel, s azt a kibocsátó előzetes írásbeli hozzájárulása nélkül nem lehet harmadik felek számára kiadni.

9. A tagállamok nemzeti/kijelölt biztonsági hatóságai felelnek annak biztosításáért, hogy a vállalkozók és alvállalkozók, akikkel CONFIDENTIEL UE vagy SECRET UE minősítésű információt tartalmazó minősített szerződést kötnek, az adott tagállam nemzeti jogszabályaival és rendeleteivel összhangban megtegyék a megfelelő intézkedéseket a minősített szerződésben foglaltak teljesítése során általuk kiadott vagy keletkeztetett EU minősített információ védelme érdekében. A biztonsági követelmények be nem tartása a szerződés felbontását eredményezheti.

▼M3

10. Valamennyi olyan ipari vagy egyéb szervezetnek, amely CONFIDENTIEL UE vagy SECRET UE minősítésű információt tartalmazó szerződésben vesz részt, nemzeti létesítménybiztonsági engedéllyel kell rendelkeznie (FSC). Az FSC-t a tagállam nemzeti/kijelölt biztonsági hivatala nyújtja annak megerősítése érdekében, hogy az adott létesítmény az EU minősített információnak – minősítési szintjének – megfelelő biztonsági védelmet tud biztosítani.

11. Az NSA/DSA felel valamennyi, e tagállamban bejegyzett ipari vagy egyéb szervezetben alkalmazott olyan személy – nemzeti jogszabályokkal összhangban történő – személyzeti biztonsági ellenőrzéséért, aki hivatalos feladatai ellátása során hozzáfér minősített szerződés alá tartozó, CONFIDENTIEL UE vagy SECRET UE minősítésű EU minősített információhoz.

12. A minősített szerződések magukban foglalják a fentiekben meghatározott SAL-t. A SAL magában foglalja az SCG-t.

13. A minősített szerződés megkötéséről szóló tárgyalás megkezdése előtt a Tanács Főtitkársága felveszi a kapcsolatot azon tagállam nemzeti/kijelölt biztonsági hatóságával, amelyben az érintett ipari vagy egyéb szervezetek be vannak jegyezve, annak érdekében, hogy meggyőződjön arról, hogy azok rendelkeznek a szerződés biztonsági minősítési szintjének megfelelő, érvényes létesítménybiztonsági engedéllyel.

14. A szerződő hatóság az érvényes FSC-re vonatkozó igazolás kézhezvételét megelőzően nem köthet minősített szerződést a megfelelőnek tartott ajánlattevővel.

15. A RESTREINT UE minősítésű információt magukban foglaló szerződések esetén az FSC nem kötelező, kivéve, ha a tagállam nemzeti törvényei és rendeletei azt megkövetelik.

16. A minősített szerződésekre vonatkozó ajánlattételek esetében a pályázati kiírásnak tartalmaznia kell egy olyan rendelkezést, amely szerint az ajánlattevő, amennyiben nem nyújt be ajánlatot, vagy nem nyeri el a pályázatot, köteles valamennyi dokumentumot meghatározott időn belül visszajuttatni.

17. Szükség lehet arra, hogy a vállalkozó különböző szinteken alvállalkozókkal kössön minősített alvállalkozói szerződést. A vállalkozó felel annak biztosításáért, hogy az alvállalkozói tevékenység az ebben a szakaszban foglalt közös minimumszabályokkal összhangban történjen. A vállalkozó azonban nem továbbíthat az alvállalkozónak EU minősített információt vagy anyagot a kibocsátó előzetes írásbeli beleegyezése nélkül.

18. A pályázati kiírás és a szerződés határozza meg azon feltételeket, amelyek szerint a vállalkozó alvállalkozói szerződést köthet. A Tanács Főtitkárságának határozott írásos beleegyezése nélkül alvállalkozói szerződés nem köthető olyan szervezetekkel, amelyek nem EU tagállamban vannak bejegyezve.

19. A szerződés valamennyi biztonsági rendelkezésének tiszteletben tartását a szerződés teljes időtartama alatt az érintett NSA/DSA ellenőrzi, a Tanács Főtitkárságával együttműködve. A biztonság megsértéséről az ezen biztonsági szabályzat II. részének X. szakaszában megállapított rendelkezésekkel összhangban kell jelentést tenni. Az FSC megváltoztatásáról vagy visszavonásáról azonnal tájékoztatni kell a Tanács Főtitkárságát, illetve bármely egyéb NSA/DSA-t, amelyet értesítettek arról.

20. A szerződések vagy alvállalkozói szerződések megszűnésekor a Tanács Főtitkársága és/vagy az NSA/DSA, adott esetben, azonnal értesíti annak a tagállamnak az NSA/DSA-ját, amelyben az érintett vállalkozó vagy alvállalkozó be van jegyezve.

21. Az e szakaszban foglalt közös minimumszabályokat a minősített szerződés vagy alvállalkozói szerződés megszűnését vagy felbontását követően is tiszteletben kell tartani, és a vállalkozók és alvállalkozók ezt követően is megőrzik a bizalmas minősített információt.

22. A SAL vagy egyéb, biztonsági követelményeket meghatározó vonatkozó rendelkezés egyedi rendelkezéseket tartalmaz a minősített információ szerződés lejártát követő kezelését illetően.

▼M3

LÁTOGATÁSOK

23. Az EU minősített szerződést teljesítő ipari vagy egyéb szervezetnél a Tanács Főtitkárságának személyzete által tett látogatást az érintett NSA/DSA-val kell megszervezni. Az ipari vagy egyéb szervezetek által az EU minősített szerződés teljesítésének keretében tett látogatásokat az érintett NSA-k/DSA-k között kell megszervezni. Az EU minősített szerződésben részt vevő NSA-k/DSA-k azonban megállapodhatnak egy olyan eljárást illetően, amely alapján az ipari vagy egyéb szervezetek által tett látogatásokat közvetlenül lehet megszervezni.

AZ EU MINŐSÍTETT INFORMÁCIÓ TOVÁBBÍTÁSA ÉS SZÁLLÍTÁSA

24. Az EU minősített információ továbbítására vonatkozóan a biztonsági szabályzat II. része VII. szakaszának II. fejezetét és, amennyiben vonatkozó, XI. szakaszát kell alkalmazni. Az ilyen rendelkezések kiegészítése érdekében a tagállamok között élő, hatályos eljárásokat kell alkalmazni.

25. A minősített szerződésekhez kapcsolódó EU minősített információ nemzetközi szállítását a tagállamok nemzeti eljárásaival összhangban kell végezni. A nemzetközi szállítás biztonsági előírásainak megvizsgálása során az alább elveket kell alkalmazni:

a) a szállítás valamennyi szakasza alatt és minden körülmények között garantált a biztonság, a származási helytől a végcélig;

b) egy adott szállítmányra megállapított védelmi szintet az abban foglalt anyag legmagasabb minősítési szintje határozza meg;

c) szükség esetén a szállítást végző vállalatok FSC-vel rendelkeznek. Ilyen esetben a szállítmányt kezelő személyzetet az e szakaszban foglalt közös minimumszabályoknak megfelelően biztonsági ellenőrzésnek kell alávetni;

d) az útvonalak lehetőség szerint közvetlenek, és a szállítást a körülmények engedte lehető leggyorsabban hajtják végre;

e) az útvonalak lehetőség szerint kizárólag EU tagállamokon keresztül vezetnek. Nem EU tagállamokon keresztül vezető útvonalakon kizárólag az átadó és az átvevő államának NSA/DSA-ja által kiadott engedélyt követően lehet haladni;

f) az EU minősített anyag szállítását megelőzően az átadó szállítási tervet készít, amelyet az érintett NSA-k/DSA-k jóváhagynak.

▼M2

*1. függelék*

**A nemzeti biztonsági hatóságok jegyzéke**

BELGIUM

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P&S 6
Rue des Petits Carmes 15
B-1000 Bruxelles
Telephone Secretariat: + 32/2/519 05 74
Telephone Presidency: + 32/2/501 82 20
+ 32/2/501 87 10
Fax: + 32/2/519 05 96

CSEH KÖZTÁRSASÁG

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DÁNIA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telephone: (45) 33 14 88 88
Fax: (45) 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 København Ø
Telephone: (45) 33 32 55 66
Fax: (45) 33 93 13 20

NÉMETORSZÁG

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49-1-888 681 15 26
Fax: + 49-1-888 681 558 06

ÉSZTORSZÁG

Eesti Vabariigi Kaitseministeerium
(Ministry of Defence, Republic of Estonia, Department of Security National Security Authority)
Sakala 1
EE-15094 Tallinn
Telephone:
+ 372/717 00 30
+ 372/717 00 31
+ 372/717 00 77
Fax: + 372/717 00 01

GÖRÖGORSZÁG

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)

▼M2

Διεύθυνση Ασφαλείας και Αντιπληροφοριών
GR-ΣΤΓ 1020 Χολαργός (Αθήνα)
Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)
Φαξ: (30-210) 642 64 32
(30-210) 652 76 12

[Hellenic National Defence General Staff (HNDGS)]
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Telephone: (30-210) 657 20 09 (office hours)
(30-210) 657 20 10 (office hours)
Fax: (30-210) 642 64 32
(30-210) 652 76 12

SPANYOLORSZÁG

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera nacional radial VI, km 8,5
E-28023 Madrid
Telephone:
+ 34/913 72 57 07
+ 34/913 72 50 27
Fax: + 34/913 72 58 08

FRANCIAORSZÁG

Secrétariat général de la défense nationale
Service de sécurité de défense (SGDN/SSD)
51, boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telephone: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

ÍRORSZÁG

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
IRL-Dublin 2
Telephone (353-1) 478 08 22
Fax (353-1) 478 14 84

OLASZORSZÁG

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-00187 Roma
Telephone: + 39/06/611 742 66
Fax: + 39/06/488 52 73

CIPRUS

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
CY-1432 Λευκωσία
Τηλέφωνα: 357-22) 80 75 69
(357-22) 80 75 19

▼**M2**

(357-22) 80 77 64
Φαξ: (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi Street
CY-1432 Nicosia
Telephone: 357-22) 80 75 69
(357-22) 80 75 19
(357-22) 80 77 64
Fax: (357-22) 30 23 51

LETTORSZÁG

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1013 Riga
Telephone: + 371/702 54 18
Fax: + 371/702 54 54

LITVÁNIA

Lithuanian National Security Authority
Gedimino ave. 40/1
LT-01110 Vilnius
Telephone: + 370/5/266 32 01
Fax: + 370/5/266 32 00

LUXEMBURG

Autorité nationale de sécurité
Ministère d'État
Boîte postale 23 79
L-1023 Luxembourg
Telephone: + 352/478 22 10 central
+ 352/478 22 35 direct
Fax:
+ 352/478 22 43
+ 352/478 22 71

MAGYARORSZÁG

National Security Authority Republic of Hungary
Nemzeti Biztonsági Felügyelet
Pf.: 2
HU-1352 Budapest
Telephone: + 361/346 96 52
Fax: + 361/346 96 58

MÁLTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telephone: + 356/21 24 98 44
Fax: + 356/21 23 53 00

HOLLANDIA

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Nederland
Telephone: (31-70) 320 44 00
Fax: (31-70) 320 07 33

▼M2

Ministerie van Defensie
Beveiligingsautoriteit (BA)
Postbus 20701
2500 ES Den Haag
Nederland
Telephone: (31-70) 318 70 60
Fax: (31-70) 318 75 22

AUSZTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43-1-531 15 23 96
Fax: + 43-1-531 15 25 08

LENGYELORSZÁG

Wojskowe Służby Informacyjne (Military Information Services
National Security Authority – Military Sphere)
PL-00-909 Warszawa 60
Telephone: + 48/22/684 13 62
Fax: + 48/22/684 10 76

Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency
National Security Authority – Civilian Sphere
Department for the Protection of Classified Information)
ul. Rakowiecka 2A
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60
Fax: + 48/22/585 85 09

PORTUGÁLIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (351) 21 301 17 10
Fax: (351) 21 303 17 11

SZLOVÉNIA

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information – NSA
Slovenska cesta 5
SI-1000 Ljubljana
Tel.: (386-1) 426 91 20
Faks: (386-1) 426 91 21

SZLOVÁKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
SK-851 05 Bratislava
Telephone: + 421/2/68 69 23 14
Fax: + 421/2/68 69 17 00

FINNORSZÁG

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu 22/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors

▼**M2**

Telephone: (358-9) 16 05 53 38
Fax: (358-9) 16 05 53 03

SVÉDORSZÁG

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telephone: + 46/8/405 54 44
Fax: + 46/8/723 11 76

EGYESÜLT KIRÁLYSÁG

UK National Security Authority
PO Box 49359
London, SW1P 1LU
United Kingdom
Telephone (44-207) 930 87 68
Fax (44-207) 821 86 04

▼M2

*2. Függelék*

**Biztonsági minősítések összehasonlító táblázata**

| EU- és EU-tagállami minősítés | TRÈS SECRET UE/EU TOP SECRET | SECRET UE | CONFIDENTIEL UE | RESTREINT UE |
|---|---|---|---|---|
| Euratom | *Eura — Top Secret* | *Eura — Secret* | *Eura — Confidential* | *Eura — Restricted* |
| Belgium | Très Secret<br>Zeer geheim | Secret<br>Geheim | Confidentiel<br>Vertrouwelijk | Diffusion restreinte<br>Beperkte verspreiding |
| Cseh Köztársaság | Přísně tajné | Tajné | Důvěrné | Vyhrazené |
| Dánia | Yderst hemmeligt | Hemmeligt | Fortroligt | Til tjenestebrug |
| Németország | Streng geheim | Geheim | VS (9) — Vertraulich | VS — Nur für den Dienstgebrauch |
| Észtország | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |
| Görögország | Άκρως Απόρρητο<br>Abr: ΑΑΠ | Απόρρητο<br>Abr: (ΑΠ) | Εμπιστευτικό<br>Abr: (ΕΜ) | Περιορισμένης Χρήσης<br>Abr: (ΠΧ) |
| Spanyolország | Secreto | Reservado | Confidencial | Difusión Limitada |
| Franciaország | Très Secret Défense (10) | Secret Défense | Confidentiel Défense | nota (11) |
| Írország | Top Secret | Secret | Confidential | Restricted |
| Olaszország | Segretissimo | Segreto | Riservatissimo | Riservato |
| Ciprus | Άκρως Απόρρητο | Απόρρητο | Εμπιστευτικό | Περιορισμένης Χρήσης |
| Lettország | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |
| Litvánia | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |
| Luxemburg | Très Secret | Secret | Confidentiel | Diffusion restreinte |

▼M2

| EU- és EU-tagállami minősítés | TRÈS SECRET UE/EU TOP SECRET | SECRET UE | CONFIDENTIEL UE | RESTREINT UE |
|---|---|---|---|---|
| Magyarország | Szigorúan titkos! | Titkos! | Bizalmas! | Korlátozott terjesztésű! |
| Málta | L-Ghola Segretezza | Sigriet | Kunfidenzjali | Ristrett |
| Hollandia | Zeer geheim | Geheim | Confidentieel | Vertrouwelijk |
| Ausztria | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Lengyelország | Ściśle Tajne | Tajne | Poufne | Zastrzeżone |
| Portugália | Muito Secreto | Secreto | Confidencial | Reservado |
| Szlovénia | Strogo tajno | Tajno | Zaupno | Interno |
| Szlovákia | Prísne tajné | Tajné | Dôverné | Vyhradené |
| Finnország | Erittäin salainen | Erittäin salainen | Salainen | Luottamuksellinen |
| Svédország | Kvalificerat hemlig | Hemlig | Hemlig | Hemlig |
| Egyesült Királyság | Top Secret | Secret | Confidential | Restricted |
| Nemzetközi szervezet minősítése | TRÈS SECRET UE/EU TOP SECRET | SECRET UE | CONFIDENTIEL UE | RESTREINT UE |
| NATO minősítés | COSMIC TOP SECRET | NATO SECRET | NATO CONFIDENTIAL | NATO RESTRICTED |
| NYEU minősítés | Focal Top Secret | WEU Secret | WEU Confidential | WEU Restricted |

([9]) Németország: VS = Verschlusssache.
([10]) Franciaország: a Trés Secret Défense minősítést, amely a kormány kiemelt kérdéseit érinti, kizárólag a miniszterelnök felhatalmazásával lehet módosítani.
([11]) Franciaország nem alkalmazza a „DIFFUSION RESTREINTE” minősítést nemzeti rendszerében. A „RESTREINT UE” minősítésű iratokat Franciaország hatályos nemzeti törvényeivel és rendeleteivel összhangban, a Tanács biztonsági szabályzatában előírtaknál semmivel sem kevésbé szigorúan kezeli és védi.

*3. függelék*

**Gyakorlati minősítési útmutató**

Ez az útmutató csak indikatív jellegű, és nem értelmezhető úgy, mint amely a II. és a III. szakaszban meghatározott lényegi rendelkezéseket módosítja.

| Minősítés | Mikor | Ki | Jelölés | Visszaminősítés/minősítés megszüntetése/megsemmisítés | |
|---|---|---|---|---|---|
| | | | | Ki | Mikor |
| TRÈS SECRET UE/EU TOP SECRET:<br>Ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása rendkívül súlyosan sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit [II. szakasz 1. pontja] | TRÈS SECRET UE/EU TOP SECRET minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg:<br>— közvetlenül veszélyeztetné az EU vagy egyik tagállama vagy az egyik baráti ország belső stabilitását,<br>— rendkívül súlyos kárt okozna a baráti kormányokkal fenntartott kapcsolatokban,<br>— közvetlenül nagyszámú emberi élet elvesztéséhez vezetne,<br>— rendkívül súlyosan károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességének fenntartását,<br>— súlyos, hosszú távú kárt okozna az EU vagy a tagállamok gazdaságának. | Tagállamok:<br>szabályszerűen felhatalmazott személyek (kibocsátók) [III. szakasz 4. pontja];<br>Főtitkárság:<br>szabályszerűen felhatalmazott személyek (kibocsátók) [III. szakasz 4. pontja], főtitkár/főképviselő, és főtitkárhelyettes.<br>A kibocsátók határozzák meg azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalmat vissza lehet minősíteni vagy a minősítést meg lehet szüntetni. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [III. szakasz 10. pontja]. | A TRÈS SECRET UE/EU TOP SECRET minősítést TRÈS SECRET UE/EU TOP SECRET dokumentumokon – adott esetben, az ESDP (EBVP) védelmi jelöléssel együtt – mechanikus eszközökkel és kézzel kell elhelyezni [II. szakasz 8. pontja].<br>Az EU-minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Minden dokumentumot hivatkozási számmal és keltezéssel kell ellátni; a hivatkozási számnak minden oldalon szerepelnie kell.<br>Ha több példányban kerülnek elosztásra, az egyes példányokat külön sorszámmal kell ellátni, amit az oldalak teljes számával együtt az első oldalon kell feltüntetni. Minden mellékletet és csatolmányt fel kell sorolni az első oldalon [VII. szakasz 1. pontja]. | A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó, illetve a főtitkár/főképviselő vagy a főtitkárhelyettes feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [III. szakasz 9. pontja].<br>A TRÈS SECRET UE/EU TOP SECRET dokumentumokat a központi nyilvántartó hivatal vagy a dokumentumokért felelős alárendelt nyilvántartó hivatal semmisíti meg. Minden megsemmisített dokumentumról megsemmisítési jegyzőkönyvet kell készíteni, melyet a TRÈS SECRET UE/EU TOP SECRET ellenőrző tisztviselőnek és a megsemmisítést tanúsító, TRÈS SECRET UE/EU TOP SECRET biztonsági felhatalmazással rendelkező tisztviselőnek kell aláírnia. A szolgálati naplóba ilyen értelmű bejegyzést kell tenni. A nyilvántartó hivatalnak a megsemmisítési jegyzőkönyveket az elosztóívvel együtt tíz évig kell megőriznie [VII. szakasz 31. pontja]. | A fölösleges példányokat és a szükségtelenné vált dokumentumokat meg kell semmisíteni [VII. szakasz 31. pontja].<br>A TRÈS SECRET UE/EU TOP SECRET dokumentumokat, beleértve a TRÈS SECRET UE/EU TOP SECRET dokumentumok készítése során keletkezett minősített hulladékot, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat is, egy TRÈS SECRET UE/EU TOP SECRET felhatalmazással rendelkező ellenőrző tisztviselő felügyelete mellett, elégetéssel, bezúzással, felaprítással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [VII. szakasz 31. pontja]. |

▼B

| Minősítés | Mikor | Ki | Jelölés | Visszaminősítés/minősítés megszüntetése/megsemmisítés | |
|---|---|---|---|---|---|
| | | | | Ki | Mikor |
| SECRET:<br>Ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása súlyosan sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit [II. szakasz 2. pontja]. | A SECRET UE minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg:<br>— nemzetközi feszültségeket okozna,<br>— súlyos kárt okozna a baráti kormányokkal fenntartott kapcsolatokban,<br>— közvetlenül emberi életeket veszélyeztetne vagy súlyosan károsítaná a közrendet, az egyéni biztonságot vagy szabadságot,<br>— súlyosan károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességének fenntartását,<br>— jelentős anyagi kárt okozna az EU vagy egyik tagállama pénzügyi, monetáris, gazdasági és kereskedelmi érdekeinek. | Tagállamok:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja];<br>Főtitkárság és az EU decentralizált szervei:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja], főigazgatók, főtitkár/főképviselő, és főtitkárhelyettes.<br>A kibocsátók határozzák meg azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalmat vissza lehet minősíteni vagy minősítését meg lehet szüntetni. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [III. szakasz 10. pontja]. | A SECRET UE minősítést az SECRET UE dokumentumokon – adott esetben az ESDP (EBVP) védelmi jelöléssel együtt – mechanikus eszközökkel és kézzel kell elhelyezni [III. szakasz 8. pontja].<br>Az EU minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Minden dokumentumot hivatkozási számmal és keltezéssel kell ellátni; a hivatkozási számnak minden oldalon szerepelnie kell.<br>Ha több példányban kerülnek elosztásra, az egyes példányokat külön sorszámmal kell ellátni, amit az oldalak teljes számával együtt az első oldalon kell feltüntetni. Minden mellékletet és csatolmányt fel kell sorolni az első oldalon [VII. szakasz 1. pontja]. | A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó, illetve a főtitkár/főképviselő vagy a főtitkárhelyettes feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [III. szakasz 9. pontja].<br>A SECRET UE dokumentumokat az ilyen dokumentumokért felelős nyilvántartó hivatal semmisíti meg egy biztonsági felhatalmazással rendelkező személy felügyelete alatt. A megsemmisített SECRET UE dokumentumokat fel kell tüntetni az aláírt megsemmisítési jegyzőkönyvben, melyet a nyilvántartó hivatalnak az elosztóívekkel együtt legalább három éven keresztül meg kell őriznie [VII. szakasz 32. pontja]. | A fölösleges példányokat és a szükségtelenné vált dokumentumokat meg kell semmisíteni [VII. szakasz 31. pontja].<br>A SECRET UE dokumentumokat, beleértve a SECRET UE dokumentumok készítése során keletkezett minősített hulladékot, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat is, elégetéssel, bezúzással, felaprítással vagy egyéb, azokat felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [VII. szakasz 31. és 32. pontja]. |

| Minősítés | Mikor | Ki | Jelölés | Visszaminősítés/minősítés megszüntetése/megsemmisítés | |
|---|---|---|---|---|---|
| | | | | Ki | Mikor |
| CONFIDENTIEL UE:<br>Ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása sérthetné az Európai Unió, illetve egy vagy több tagállama alapvető érdekeit [II. szakasz 3. pont]. | CONFIDENTIEL UE minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg:<br>— jelentős kárt okozna a diplomáciai kapcsolatokban, azaz hivatalos tiltakozást vagy egyéb szankciókat váltana ki,<br>— sértené az egyének biztonságát vagy szabadságát,<br>— károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességét,<br>— lényegesen gyengítené jelentős szervezetek pénzügyi életképességét,<br>— súlyos bűncselekmények nyomozását akadályozná vagy azok elkövetését megkönnyítené,<br>— erősen ártana az EU vagy a tagállamok pénzügyi, monetáris, gazdasági és kereskedelmi érdekeinek,<br>— komolyan hátráltatná az EU főbb politikáinak kidolgozását vagy működését,<br>— az EU jelentős tevékenységeit állítaná le vagy azokban jelentős fennakadást okozna. | Tagállamok:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja];<br>Főtitkárság és az EU decentralizált szervei:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja], főigazgatók, főtitkár/főképviselő, főtitkárhelyettes.<br>A kibocsátók határozzák meg azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalmat vissza lehet minősíteni vagy minősítését meg lehet szüntetni. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [III. szakasz 10. pontja]. | A CONFIDENTIEL UE minősítést a CONFIDENTIEL UE dokumentumokon – adott esetben az ESDP (EBVP) védelmi jelöléssel együtt – mechanikus eszközökkel és kézzel vagy előre lebélyegzett, regisztrált papírra való nyomtatással kell elhelyezni [II. szakasz 8. pontja].<br>Az EU-minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Minden dokumentumot hivatkozási számmal és keltezéssel kell ellátni. Minden mellékletet és csatolmányt fel kell sorolni az első oldalon [VII. szakasz 1. pontja]. | A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó, illetve a főtitkár/főképviselő vagy a főtitkárhelyettes feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [III. szakasz 9. pontja].<br>A CONFIDENTIEL UE dokumentumokat az ilyen dokumentumokért felelős nyilvántartó hivatal semmisíti meg egy biztonsági felhatalmazással rendelkező személy felügyelete alatt.<br>Megsemmisítésüket a nemzeti rendelkezések szerint, illetve a Főtitkárság vagy az EU decentralizált szervei esetében a főtitkár/főképviselő vagy a főtitkárhelyettes utasításai szerint kell nyilvántartani [VII. szakasz 33. pontja]. | A fölösleges példányokat és a szükségtelenné vált dokumentumokat meg kell semmisíteni [VII. szakasz 31. pontja].<br>A CONFIDENTIEL UE dokumentumokat, beleértve a CONFIDENTIEL UE dokumentumok készítése során keletkezett minősített hulladékot, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat is, elégetéssel, bezúzással, felaprítással vagy egyéb, azokat felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [VII. szakasz 31. és 33. pontja]. |

| Minősítés | Mikor | Ki | Jelölés | Visszaminősítés/minősítés megszüntetése/megsemmisítés | |
|---|---|---|---|---|---|
| | | | | Ki | Mikor |
| RESTREINT UE:<br>Ez a minősítés csak azokra az információkra és anyagokra alkalmazható, amelyek engedély nélküli kiszolgáltatása hátrányosan érinthetné az Európai Unió, illetve egy vagy több tagállama érdekeit [II. szakasz 4. pontja]. | A RESTREINT UE minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg:<br>— ártana a diplomáciai kapcsolatoknak,<br>— magánszemélyeknek jelentős szenvedést okozna,<br>— megnehezítené a tagállamok vagy más partnerek fegyveres erői bevethetőségének vagy biztonságának fenntartását,<br>— magánszemélyek vagy vállalkozások számára pénzügyi veszteséget okozna, illetve jogosulatlan nyereséget vagy előnyt biztosítana,<br>— megsértené a harmadik felek által átadott információk titkosságának megőrzésére tett saját kötelezettségvállalásokat,<br>— megsértené az információk kiszolgáltatására vonatkozó törvényi korlátozásokat,<br>— bűncselekmények nyomozását akadályozná vagy azok elkövetését megkönnyítené,<br>— hátrányos helyzetbe hozná az EU-t vagy tagállamait a másokkal folytatott kereskedelmi vagy általános politikai tárgyalások során,<br>— hátráltatná az EU politikáinak eredményes kidolgozását vagy működését,<br>— veszélyeztetné az EU-nak és tevékenységeinek megfelelő igazgatását. | Tagállamok:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja];<br>Főtitkárság és az EU decentralizált szervei:<br>felhatalmazott személyek (kibocsátók) [III. szakasz 2. pontja], főigazgatók, főtitkár/főképviselő, főtitkárhelyettes.<br>A kibocsátók határozzák meg azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalmat vissza lehet minősíteni vagy minősítését meg lehet szüntetni. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [III. szakasz 10. pontja]. | A RESTREINT UE minősítést RESTREINT UE dokumentumokon – adott esetben az ESDP (EBVP) védelmi jelöléssel együtt – mechanikus vagy elektronikus eszközökkel kell elhelyezni [II. szakasz 8. pontja].<br>Az EU minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Minden dokumentumot hivatkozási számmal és keltezéssel kell ellátni [VII. szakasz 1. pontja]. | Csak a minősített dokumentum kibocsátója, illetve a főtitkár/főképviselő vagy a főtitkárhelyettes részéről kerülhet sor visszaminősítésre vagy a minősítés megszüntetésére, aki a változásról értesíti azokat a további címzetteket, akik részére a dokumentumot vagy annak másolatát megküldte [III. szakasz 9. pontja].<br>A RESTREINT UE dokumentumokat az ilyen dokumentumokért felelős nyilvántartó hivatalnak kell megsemmisítenie a nemzeti rendelkezések, illetve a Főtitkárság vagy az EU decentralizált szervei esetében a főtitkár/főképviselő vagy a főtitkárhelyettes utasításainak megfelelően [VII. szakasz 34. pontja]. | A fölösleges példányokat és a szükségtelenné vált dokumentumokat meg kell semmisíteni [VII. szakasz 31. pontja]. |

▼B

*4. függelék*

**Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához**

**1. Szintű együttműködés**

ELJÁRÁSOK

1. A Tanács hatáskörébe tartozik, hogy EU minősített információkat adjon át az Európai Unióban nem tag országok vagy egyéb nemzetközi szervezetek számára, amelyek biztonsági politikája és rendelkezései összehasonlíthatóak az EU biztonsági politikájával és rendelkezéseivel.

2. A minősített információk átadására vonatkozó határozathozatali jogkört a Tanács átruházhatja. Az átruházáskor közölnie kell az átadható információk természetét és minősítési szintjét, amely rendszerint nem lehet magasabb a CONFIDENTIEL UE szintnél.

3. Külön biztonsági megállapodás megkötésére is figyelemmel az államok vagy nemzetközi szervezetek biztonsági hivatalainak a főtitkárhoz/főképviselőhöz kell benyújtaniuk EU minősített információk átadására vonatkozó kérelmüket, melyben közlik a szóban forgó átadás célját és az átadandó minősített információk természetét.

   A tagállamok és az EU decentralizált szervei ugyancsak benyújthatnak ilyen, az EU minősített információk átadását kívánatosnak tartó kérelmet, melyben közlik az átadás célját, az EU ebből származó előnyeit, illetve meghatározzák az átadandó információk természetét és minősítési szintjét.

4. A kérelmeket a Főtitkárság bírálja el és ehhez:

   — kikéri az átadandó dokumentumot kibocsátó tagállamnak, illetve adott esetben az EU decentralizált szervnek a véleményét,

   — kialakítja a szükséges kapcsolatokat a kedvezményezendő országok vagy nemzetközi szervezetek illetékes biztonsági szolgálataival annak megvizsgálása céljából, hogy azok biztonsági politikája és rendelkezései biztosítják-e az átadott minősített információk e biztonsági szabályzatnak megfelelő védelmét,

   — kikéri a tagállamok nemzeti biztonsági hatóságainak szakvéleményét, hogy mennyiben lehet megbízni a kedvezményezendő államokban vagy nemzetközi szervezetekben.

5. A Főtitkárság a kérelmet és a Biztonsági Hivatal ajánlását határozathozatal végett továbbítja a Tanácsnak.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI SZABÁLYOK

6. A főtitkár/főképviselő értesíti a kedvezményezett államokat vagy nemzetközi szervezeteket a Tanácsnak az EU minősített információk átadásáról szóló határozatáról, és továbbítja e biztonsági szabályzatot a szükségesnek ítélt példányszámban. Ha a kérelmet valamely tagállam nyújtotta be, ez az állam értesíti a kedvezményezettet az átadás engedélyezéséről.

   Az átadásról szóló határozat csak akkor lép hatályba, ha a kedvezményezettek írásban kötelezettséget vállalnak arra, hogy:

   — az információkat csak a megállapodás szerinti célokra használják fel,

   — az információkat e szabályzatnak megfelelően, és különösen az alábbiakban rögzített különleges rendelkezéseknek megfelelően védik.

7. *Személyzet*

   a) Az EU minősített információkhoz hozzáféréssel rendelkező tisztviselők száma a „szükséges ismeret” elve alapján szigorúan azokra a személyekre korlátozódik, akiknek erre a hozzáférésre feladataik alapján szükségük van.

▼B

b) A CONFIDENTIEL UE vagy az annál magasabb minősítésű információkhoz való hozzáférésre jogosult valamennyi tisztviselőnek vagy állampolgárnak a saját államának kormánya által kiadott megfelelő szintű biztonsági tanúsítvánnyal vagy ennek megfelelő biztonsági felhatalmazással kell rendelkeznie.

8. *Dokumentumok továbbítása*

a) A dokumentumok továbbításának gyakorlati eljárásait a Tanács biztonsági szabályzatának VII. szakaszában foglalt rendelkezések alapján létrejött megállapodásban kell meghatározni. Az eljárások különösen azt határozzák meg, hogy az EU minősített információkat mely nyilvántartó hivatalokba kell továbbítani.

b) Ha a Tanács által átadásra engedélyezett minősített információk TRÈS SECRET UE/EU TOP SECRET anyagot is tartalmaznak, a kedvezményezett állam vagy nemzetközi szervezet központi EU nyilvántartó hivatalt, és ha szükséges, EU alárendelt nyilvántartó hivatalokat hoz létre. Ezeknek a nyilvántartó hivataloknak a működését az e biztonsági szabályzat VIII. szakaszában foglalt rendelkezések szabályozzák.

9. *Bejegyzés*

Amint valamely nyilvántartó hivatal CONFIDENTIEL UE vagy annál magasabb minősítésű EU dokumentumot kap, a dokumentumot a szervezet által vezetett különleges nyilvántartásba bejegyzi, amelyben külön oszlopok vannak az átvétel időpontja, a dokumentum adatai (kelte, hivatkozási száma és a példány sorszáma), minősítése, címe, az átvevő neve vagy beosztása, az átvételi elismervény visszajuttatásának időpontja és annak az időpontnak a számára, amikor a dokumentumot az EU-beli kibocsátóhoz visszajuttatják vagy megsemmisítik.

10. *Megsemmisítés*

a) Az EU minősített dokumentumokat az e biztonsági szabályzat VI. szakaszában rögzített utasításoknak megfelelően semmisítik meg. A SECRET UE és a TRÈS SECRET UE/EU TOP SECRET dokumentumok vonatkozásában a megsemmisítési jegyzőkönyvek másolatait meg kell küldeni a dokumentumokat továbbító EU nyilvántartó hivatal számára.

b) Az EU minősített dokumentumokat bele kell foglalni a kedvezményezett szolgálatok saját minősített dokumentumaira vonatkozó vészhelyzeti megsemmisítési tervekbe.

11. *A dokumentumok védelme*

Minden intézkedést meg kell tenni annak megakadályozására, hogy illetéktelen személyek EU minősített információkhoz hozzáférjenek.

12. *Másolatok, fordítások és kivonatok*

CONFIDENTIEL UE vagy SECRET UE minősítésű dokumentumról nem lehet fénymásolatot vagy fordítást, illetve ezekből kivonatokat készíteni az érintett biztonsági szervezet vezetőjének engedélye nélkül, aki ezeket a másolatokat, fordításokat vagy kivonatokat nyilvántartja és ellenőrzi, és szükség szerint lepecsételi.

A TRÈS SECRET UE/EU TOP SECRET dokumentumok másolását vagy fordítását csak a kibocsátó hatóság engedélyezheti, amely meghatározza a másolatok engedélyezett számát; ha a kibocsátó hatóság kiléte nem határozható meg, a kérelmet a Főtitkárság Biztonsági Hivatalához kell benyújtani.

13. *A biztonság megsértése*

Ha a biztonságot EU minősített dokumentummal kapcsolatosan sértik meg vagy ennek gyanúja merül fel, a következő azonnali intézkedéseket kell megtenni a biztonsági megállapodás megkötésére is figyelemmel:

a) vizsgálatot kell lefolytatni a biztonság megsértése körülményeinek megállapítása céljából;

▼B

b) értesíteni kell a Főtitkárság Biztonsági Hivatalát, a nemzeti biztonsági hatóságot és a kibocsátó hatóságot, illetve adott esetben világosan közölni kell, hogy ez utóbbit nem értesítették;

c) intézkedéseket kell tenni annak érdekében, hogy a minimálisra korlátozzák biztonság megsértésének következményeit;

d) felül kell vizsgálni és végre kell hajtani az ismételt előfordulás megakadályozása érdekében szükséges intézkedéseket;

e) az ismételt előfordulás megakadályozása érdekében végre kell hajtani a Főtitkársági Biztonsági Hivatala által ajánlott intézkedéseket.

14. *Ellenőrzések*

Az érintett államokkal vagy nemzetközi szervezetekkel egyetértésben a Főtitkárság Biztonsági Hivatala jogosult értékelni az átadott EU minősített információk védelmére irányuló intézkedések eredményességét.

15. *Jelentéstétel*

A biztonsági megállapodás megkötésére is figyelemmel az államok vagy a nemzetközi szervezetek – mindaddig, amíg EU minősített információk birtokában vannak – az információ átadásának engedélyezésekor meghatározott időpontig minden évben jelentést nyújtanak be, amelyben megerősítik, hogy e biztonsági szabályzatot betartották.

▼B

*5. függelék*

**Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához:**

2. Szintű együttműködés

ELJÁRÁSOK

1. A Tanács hatáskörébe tartozik, hogy EU minősített információkat adjon át olyan harmadik országok vagy nemzetközi szervezetek számára, amelyek biztonsági politikája és rendelkezései jelentősen eltérnek az EU biztonsági politikájától és rendelkezéseitől. Az átadás főszabály szerint a SECRET UE és annál alacsonyabb minősítésű információkra korlátozódik; a kifejezetten a tagállamoknak fenntartott nemzeti információk és a külön jelöléssel védett, EU minősített információk e körből ki vannak zárva.

2. A minősített információk átadására vonatkozó határozathozatali jogkört a Tanács átruházhatja; az átruházáskor – az 1. pontban meghatározott korlátozások figyelembevételével – közölnie kell az átadható információk természetét és minősítési szintjét, amely nem lehet magasabb a RESTREINT UE szintnél.

3. Biztonsági megállapodás megkötésére is figyelemmel az államok vagy nemzetközi szervezetek biztonsági hivatalainak a főtitkárhoz/főképviselőhöz kell benyújtaniuk az EU minősített információk átadására vonatkozó kérelmüket, melyben közlik a szóban forgó átadás célját és az átadandó minősített információk természetét.

   A tagállamok és az EU decentralizált szervei ugyancsak benyújthatnak ilyen, az EU minősített információk átadását kívánatosnak tartó kérelmet, melyben közlik az átadás célját, az EU-nak ebből származó előnyét, illetve meghatározzák az átadandó információ természetét és minősítési szintjét.

4. A kérelmeket a Főtitkárság bírálja el és ehhez:

   — kikéri az átadandó dokumentumot kibocsátó tagállamnak, illetve adott esetben az EU decentralizált szervnek a véleményét,

   — kialakítja a szükséges kapcsolatokat a kedvezményezendő államok vagy nemzetközi szervezetek biztonsági szolgálataival, hogy információkhoz jusson azok biztonsági politikájával és rendelkezéseivel kapcsolatban, és különösen azért, hogy összehasonlító táblázatot készítsen az EU-ban és az érintett államban vagy nemzetközi szervezetben alkalmazott minősítésekről,

   — gondoskodik a Tanács Biztonsági Bizottságának összehívásáról vagy adott esetben egyszerűsített írásbeli eljárás keretében érdeklődik a tagállamok nemzeti biztonsági hatóságainál, hogy megszerezze a Biztonsági Bizottság szakvéleményét.

5. A Tanács Biztonsági Bizottsága szakvéleményében az alábbi szempontokra tér ki:

   — mennyiben lehet megbízni a kedvezményezendő államokban vagy nemzetközi szervezetekben, azaz azon biztonsági kockázatok értékelése, amelyeknek az EU vagy a tagállamai kiteszik magukat,

   — annak értékelése, hogy a kedvezményezettek képesek-e megvédeni az EU által átadott minősített információkat,

   — javaslatok az EU minősített információk (például a szöveg megtisztított változatának átadása) és a továbbított dokumentumok (EU minősítéseket tartalmazó azonosítók, különleges jelölések stb. megtartása vagy törlése) kezelésére irányuló gyakorlati eljárásokat illetően,

---

▼B

— a kibocsátó hatóság általi visszaminősítés vagy a minősítés megszüntetése, mielőtt a kedvezményezett országoknak vagy nemzetközi szervezeteknek az információkat átadják ([1]).

6. A főtitkár/főképviselő a kérelmet és a Főtitkárság Biztonsági Hivatala által a Tanács Biztonsági Bizottságától beszerzett szakvéleményt határozathozatalra a Tanács elé terjeszti.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI SZABÁLYOK

7. A főtitkár/főképviselő ismerteti a kedvezményezett államokkal vagy nemzetközi szervezetekkel a Tanácsnak az EU minősített információk átadásáról szóló határozatát, valamint az EU-ban és az érintett államokban vagy nemzetközi szervezetekben alkalmazandó minősítéseket összehasonlító táblázatot. Ha a kérelmet valamely tagállam nyújtotta be, ez az állam értesíti a kedvezményezettet az átadás engedélyezéséről.

Az átadásra vonatkozó határozat csak akkor lép hatályba, ha a kedvezményezettek írásban kötelezettséget vállalnak arra, hogy:

— az információkat csak a megállapodás szerinti célokra használják fel,

— az információkat a Tanács által megállapított szabályoknak megfelelően védik.

8. A következő védelmi szabályokat kell alkalmazni, hacsak a Tanács – a Tanács Biztonsági Bizottságának szakvéleménye birtokában – úgy nem határoz, hogy különleges eljárást alkalmaz az EU minősített dokumentumok kezelésére (EU-minősítés, különleges jelölések stb. törlése).

Ebben az esetben a szabályokat ki kell igazítani.

9. *Személyzet*

a) Az EU minősített információkhoz hozzáféréssel rendelkező tisztviselők száma a „szükséges ismeret” elve alapján szigorúan azokra a személyekre korlátozódik, akiknek erre a hozzáférésre feladataik alapján szükségük van.

b) Az EU által átadott minősített információkhoz hozzáférésre jogosult valamennyi tisztviselőnek vagy állampolgárnak az összehasonlító táblázatban meghatározottak szerinti megfelelő, az EU-éval azonos szintű minősített nemzeti információkhoz való hozzáférésre feljogosító nemzeti biztonsági tanúsítvánnyal vagy hozzáférési felhatalmazással kell rendelkeznie.

c) Ezeket a nemzeti biztonsági tanúsítványokat vagy felhatalmazásokat a főtitkár/főképviselő számára tájékoztatásul továbbítják.

10. *Dokumentumok továbbítása*

a) A dokumentumok továbbításának gyakorlati eljárásairól a Főtitkárság Biztonsági Hivatala és az átvevő államok vagy nemzetközi szervezetek biztonsági hivatalai állapodnak meg az e biztonsági szabályzat VII. szakaszában foglalt rendelkezések alapján. Az eljárások különösen azokat a pontos címeket határozzák meg, ahova a dokumentumokat továbbítani kell, illetve az EU minősített információk továbbításánál igénybe veendő futár- vagy postai szolgálatokat.

b) A CONFIDENTIEL UE vagy magasabb minősítésű dokumentumokat dupla borítékban kell továbbítani. A belső borítékon kell feltüntetni az „UE” jelölést és a biztonsági minősítés jelölését. Minden minősített dokumentumot átvételi elismervény kísér. Az átvételi elismervény, amely önmagában nem minősített, csak a dokumentum adatait (hivatkozási szám, keltezés, a példány sorszáma) és a nyelvét adja meg, de a címét nem.

([1]) Ez azzal jár, hogy a dokumentumot kibocsátó hatóságnak a III. szakasz 9. pontjában megállapított eljárást kell alkalmaznia minden, az EU-n belül köröztetett példány tekintetében.

▼B

c) Ezt követően a belső borítékot egy külső borítékba helyezik, amelyen az átvétel céljából csomagszámot tüntetnek fel. A külső borítékon nem szerepelhet a biztonsági minősítés.

d) A futároknak minden esetben meg kell kapniuk a csomagszámot feltüntető átvételi elismervényt.

11. Bejegyzés beérkezéskor

A címzett állam nemzeti biztonsági hatósága vagy a megfelelő állami szerv, amely az EU minősített információkat a kormány nevében átveszi, illetve a nemzetközi szervezet biztonsági hivatala külön nyilvántartást nyit, ahová átvételkor az EU minősített információkat bejegyzik. A nyilvántartásban külön oszlopok vannak az átvétel időpontja, a dokumentum adatai (keltezés, hivatkozási szám és a példány sorszáma), minősítése, címe, a címzett neve vagy beosztása, az elismervény visszajuttatásának időpontja és annak az időpontnak a számára, amikor a dokumentumot az EU számára visszajuttatják vagy megsemmisítik.

12. A dokumentumok visszajuttatása

Amikor az átvevő a Tanácsnak vagy az azt átengedő tagállamnak valamely minősített dokumentumot juttat vissza, a 10. pontban foglaltak szerint kell eljárnia.

13. Védelem

a) Amikor a dokumentumokat nem használják a nemzetileg azonos szintűként minősített anyagok tárolására jóváhagyott biztonsági tárolóeszközökben kell elhelyezni őket. A tartalmukra vonatkozó jelzés nem szerepelhet a tárolóeszközön, amelyekhez csak az EU minősített információk kezelésére felhatalmazott személyek férhetnek hozzá. Ha kombinációs zárat használnak, a kombinációt csak azok a személyek ismerhetik, akik az adott államban vagy szervezetnél engedéllyel rendelkeznek EU minősített információkhoz való hozzáféréshez; a kombinációt hathavonta meg kell változtatni, illetve ennél hamarabb, ha a kombinációt ismerő tisztviselőt áthelyezik vagy biztonsági felhatalmazását visszavonják, illetve ha a kombináció kitudódásának kockázata merül fel.

b) A biztonsági tárolóeszközből az EU minősített dokumentumokat az EU minősített dokumentumokhoz való hozzáférésre felhatalmazással rendelkező tisztviselők közül csak azok vehetik ki, akiknek a dokumentumokat ismerniük kell. Ők felelnek e dokumentumok biztonságos megőrzéséért mindaddig, amíg azok a birtokukban vannak, és különösen azért, hogy a dokumentumokhoz illetéktelen személyek ne férhessenek hozzá. Arról is kötelesek gondoskodni, hogy a dokumentumokat betekintés után vagy munkaidőn kívül biztonsági tárolóeszközben tárolják.

c) CONFIDENTIEL UE vagy az annál magasabb minősítésű dokumentumokról nem lehet fénymásolatot, illetve e dokumentumokból kivonatokat készíteni a Főtitkárság Biztonsági Hivatalának engedélye nélkül.

d) Ki kell dolgozni a dokumentumok vészhelyzetben történő gyors és teljes megsemmisítésére irányuló eljárást, amelyet a Főtitkárság Biztonsági Hivatala hagy jóvá.

14. Fizikai biztonság

a) Az EU minősített dokumentumok tárolására használt biztonsági tárolóeszközöket használaton kívül mindenkor zárva kell tartani.

b) Ha a karbantartó vagy takarító személyzetnek be kell lépnie vagy dolgoznia kell abban a helyiségben, ahol ezeket a biztonsági tárolóeszközöket tartják, őket mindenkor az állam vagy szervezet biztonsági szolgálata egy tagjának vagy a kifejezetten a helyiség biztonságának felügyeletéért felelős tisztviselőnek kell kísérnie.

c) A rendes munkaidőn túl (éjszaka, hétvégén és munkaszüneti napokon) az EU minősített dokumentumokat tartalmazó biztonsági tárolóeszközöket őr vagy automatikus riasztórendszer védi.

15. A biztonság megsértése

▼B

Ha a biztonságot EU minősített dokumentummal kapcsolatosan sértik meg, vagy ennek gyanúja merül fel, a következő azonnali intézkedéseket kell megtenni:

a) Haladéktalanul jelentést kell küldeni a Főtitkárság Biztonsági Hivatalának vagy a dokumentumok átadását kezdeményező tagállam nemzeti biztonsági hatóságának (ennek másolatát meg kell küldeni a Főtitkárság Biztonsági Hivatala számára).

b) Vizsgálatot kell lefolytatni, amelynek befejeztével részletes jelentést kell benyújtani a biztonsági szolgálathoz (lásd a fenti a) pontot). Ezt követően kell meghozni a szükséges intézkedéseket a helyzet orvoslására.

16. Ellenőrzések

Az érintett államokkal vagy nemzetközi szervezetekkel egyetértésben a Főtitkárság Biztonsági Hivatala jogosult értékelni az átadott EU minősített információk védelmére irányuló intézkedések eredményességét.

17. Jelentéstétel

Az államok vagy a nemzetközi szervezetek – mindaddig, amíg EU minősített információk birtokában vannak – az információ átadásának engedélyezésekor meghatározott időpontig minden évben jelentést nyújtanak be, amelyben megerősítik, hogy e biztonsági szabályzatot betartották.

▼B

*6. függelék*

**Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához**

3. szintű együttműködés

ELJÁRÁSOK

1. Esetenként előfordulhat, hogy a Tanács bizonyos különleges körülmények között együtt kíván működni olyan államokkal vagy szervezetekkel, amelyek nem tudják megadni az e biztonsági szabályzatban előírt biztosítékokat, de az együttműködés érdekében mégis szükségessé válhat EU minősített információk átadása. Az ilyen átadás nem terjedhet ki a kifejezetten a tagállamoknak fenntartott nemzeti információkra.

2. Ilyen különleges körülmények fennállása esetén a harmadik államoktól vagy nemzetközi szervezetektől érkező, vagy a tagállamok, illetve adott esetben az EU decentralizált szervei által javasolt, az EU-val való együttműködésre vonatkozó kéréseket először tartalmi szempontból vizsgálja meg a Tanács, amely szükség esetén kikéri az információt kibocsátó tagállam vagy decentralizált szerv véleményét. A Tanács mérlegeli a minősített információk átadásának célszerűségét, értékeli, hogy a kedvezményezetteknek mennyiben szükséges azokat ismerniük, és meghatározza a közölhető minősített információk természetét.

3. Ha a Tanács támogatja a kérést, a főtitkárnak/főképviselőnek kötelessége összehívni a Tanács Biztonsági Bizottságát vagy – esetlegesen egyszerűsített írásbeli eljárás keretében – érdeklődni a tagállamok nemzeti biztonsági hatóságainál, hogy megszerezze a Biztonsági Bizottság szakvéleményét.

4. A Tanács Biztonsági Bizottsága szakvéleményében az alábbi szempontokra tér ki:

   a) azon biztonsági kockázatok értékelése, amelyeknek az EU vagy a tagállamai kiteszik magukat;

   b) az átadható információk minősítési szintje, adott esetben azok természetére való tekintettel;

   c) az információknak a dokumentumot kibocsátó hatóság által végzett visszaminősítése vagy minősítésének megszüntetése, mielőtt azokat az érintett országoknak vagy nemzetközi szervezeteknek átadnák ([1]);

   d) az átadandó dokumentumok kezelésére irányuló eljárások (lásd az alábbi 5. pontot);

   e) a továbbítás lehetséges módszerei (nyilvános postaszolgálat, nyilvános vagy biztonsági távközlési rendszerek, diplomáciai futárcsomag, biztonsági szempontból ellenőrzött futárok stb. igénybevétele).

5. Az e függelék hatálya alá tartozó államok vagy szervezetek számára átadott dokumentumokat főszabály szerint a forrásra vagy az EU minősítésre való hivatkozás nélkül készítik el. A Tanács Biztonsági Bizottsága ajánlhatja:

   — különleges jelölés vagy fedőnév használatát,

   — a minősítés különös rendszerének használatát, amely összekapcsolja az információk érzékenységét azokkal az ellenőrzési intézkedésekkel, amelyeket a kedvezményezettnek a dokumentumok továbbítási módszerei alapján előírtak (lásd a 14. pontban található példákat).

6. A Főtitkárság Biztonsági Hivatala továbbítja a Tanácsnak a Biztonsági Bizottság szakvéleményét, adott esetben csatolva a feladat teljesítéséhez – különösen sürgős esetekben – szükséges hatáskörök átruházására vonatkozó javaslatokat.

([1]) Ez azzal jár, hogy a dokumentumot kibocsátó hatóságnak a III. szakasz 9. pontjában megállapított eljárást kell alkalmaznia minden, az EU-n belül köröztetett példány tekintetében.

▼B

7. Miután a Tanács jóváhagyta az EU minősített információk átadását és a gyakorlati végrehajtási eljárásokat, a Főtitkárság Biztonsági Hivatala kialakítja az ehhez szükséges kapcsolatokat az érintett állam vagy szervezet biztonsági szolgálatával, hogy megkönnyítse a tervezett biztonsági intézkedések alkalmazását.

8. A Főtitkárság Biztonsági Hivatala minden érintett tagállam – és adott esetben az EU érintett decentralizált szervei – részére tájékoztatás végett megküld egy táblázatot, amely összefoglalja az információk természetét és minősítését, és felsorolja, hogy a Tanács határozata alapján mely országoknak vagy szervezeteknek adhatók át.

9. Az átadó tagállam nemzeti biztonsági hatósága vagy a Főtitkárság Biztonsági Hivatala megtesz minden szükséges intézkedést annak érdekében, hogy megkönnyítse az esetleges későbbi károk felmérését és az eljárások felülvizsgálatát.

10. Ha az együttműködés feltételei megváltoznak, ismét a Tanácshoz kell fordulni.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI SZABÁLYOK

11. A főtitkár/főképviselő ismerteti a kedvezményezett államokkal vagy nemzetközi szervezetekkel a Tanácsnak az EU minősített információk átadásáról szóló határozatát, valamint a Tanács Biztonsági Bizottsága által javasolt és a Tanács által jóváhagyott részletes védelmi szabályokat. Ha a kérelmet valamely tagállam nyújtotta be, ez az állam értesíti a kedvezményezettet az átadás engedélyezéséről.

    Az átadásra vonatkozó határozat akkor lép hatályba, ha a kedvezményezettek írásban kötelezettséget vállalnak arra, hogy:

    — az információkat csak a Tanács által meghatározott együttműködés céljára használják fel,

    — az információk számára biztosítják a Tanács által előírt védelmet.

12. Dokumentumok továbbítása

    a) A dokumentumok továbbításának gyakorlati eljárásairól a Főtitkárság Biztonsági Hivatalának és az átvevő államok vagy nemzetközi szervezetek biztonsági szolgálatainak kell megállapodniuk. Különösen azokat a pontos címeket határozzák meg, ahova a dokumentumokat továbbítani kell.

    b) A CONFIDENTIEL UE vagy annál magasabb minősítésű dokumentumokat dupla borítékban kell továbbítani. A belső borítékot külön pecséttel vagy meghatározott fedőnévvel, valamint a dokumentum tekintetében elfogadott különleges minősítésre való utalással kell ellátni. Minden minősített dokumentumot átvételi elismervény kísér. Az átvételi elismervény, amely önmagában nem minősített, csak a dokumentum adatait (hivatkozási számát, keltét, a példány sorszámát) és nyelvét adja meg, de a címét nem.

    c) Ezt követően a belső borítékot egy külső borítékba helyezik, amelyen az átvétel céljából csomagszámot tüntetnek fel. A külső borítékon nem szerepelhet semmilyen biztonsági minősítés.

    d) A futároknak minden esetben meg kell kapniuk a csomagszámot feltüntető átvételi elismervényt.

13. Bejegyzés beérkezéskor

    A címzett állam nemzeti biztonsági hatósága vagy az annak megfelelő állami szerv, amely kormánya nevében az EU által továbbított minősített információkat átveszi, illetve az átvevő nemzetközi szervezet biztonsági hivatala különleges nyilvántartást nyit, ahová átvételkor az EU minősített információkat bejegyzik. A nyilvántartásban külön oszlopok vannak az átvétel időpontja, a dokumentum adatai (kelte, hivatkozási száma és a példány sorszáma), minősítése, címe, a címzett neve vagy beosztása, az átvételi elismervény visszajuttatásának időpontja és annak az időpontnak a

▼B

számára, amikor a dokumentumot az EU számára visszajuttatják vagy megsemmisítik.

14. A kicserélt minősített információk felhasználása és védelme

a) A SECRET UE minősítésű információkat csak a kifejezetten erre kijelölt tisztviselők kezelhetik, akik felhatalmazással rendelkeznek az ilyen minősítésű információkhoz való hozzáférésre. Ezeket az információkat olyan jó minőségű páncélszekrényekben tárolják, amelyeket csak a bennük tárolt információkhoz való hozzáférésre felhatalmazott személyek tudnak kinyitni. A területeket, ahol ezek a páncélszekrények találhatók, állandó jelleggel őrizni kell, és ellenőrző rendszert kell felállítani annak érdekében, hogy oda csak a szabályszerűen felhatalmazott személyek léphessenek be. A SECRET UE minősítésű információkat diplomáciai futárcsomagban, biztonságos postaszolgálat vagy biztonságos távközlési eszközök útján továbbítják. A SECRET UE dokumentum csak a kibocsátó hatóság írásbeli beleegyezése alapján másolható. Minden másolatot nyilván kell tartani, és ellenőrzés alatt kell tartani. A SECRET UE dokumentumokkal kapcsolatos valamennyi művelet esetében átvételi elismervényt kell kiállítani.

b) A CONFIDENTIEL UE minősítésű információkat csak a szabályszerűen kijelölt tisztviselők kezelhetik, akik felhatalmazással rendelkeznek arra, hogy a témában tájékozódjanak. A dokumentumokat ellenőrzött területen lévő zárt páncélszekrényben kell tárolni.

A CONFIDENTIEL UE információkat diplomáciai futárcsomagban, katonai postaszolgálat vagy biztonságos távközlési eszközök útján kell továbbítani. Az átvevő szerv másolatokat készíthet, ezek számát és elosztását különleges nyilvántartásokba kell bejegyezni.

c) A RESTREINT UE minősítésű információkat zárt tárolóeszközökben olyan helyiségekben kezelik, ahová illetéktelen személyek nem léphetnek be. A dokumentumok a nyilvános postaszolgálat útján dupla borítékban, ajánlott levélként, illetve sürgős esetekben a nem védett, nyilvános távközlési rendszereken keresztül is továbbíthatók. A címzettek másolatokat készíthetnek.

d) A nem minősített információk esetében nincsen szükség különleges védelmi intézkedésekre, ezek postai és nyilvános távközlési rendszerek útján továbbíthatók. A címzettek másolatokat készíthetnek.

15. Megsemmisítés

A szükségtelenné vált dokumentumokat meg kell semmisíteni. RESTREINT UE és CONFIDENTIEL UE minősítésű dokumentumok esetében megfelelő bejegyzést kell tenni a különleges nyilvántartásokban. SECRET UE dokumentumok esetében megsemmisítési jegyzőkönyvet kell felvenni, amelyet a megsemmisítésnél tanúként jelenlévő két személynek kell aláírnia.

16. A biztonság megsértése

Ha a CONFIDENTIEL UE vagy SECRET UE információkkal kapcsolatos biztonságot megsértették vagy ennek gyanúja merül fel, az állam nemzeti biztonsági hatósága vagy a szervezet biztonsági felelőse köteles ennek körülményeit kivizsgálni. Ha a vizsgálat során beigazolódik a biztonság megsértése, a kibocsátó hatóságot értesíteni kell. Meg kell tenni a szükséges intézkedéseket a nem megfelelő eljárások vagy tárolási módszerek korrigálása érdekében, ha ezek vezettek a biztonság megsértéshez. A Tanács főtitkára/főképviselője vagy az illetéktelenek tudomására jutott információkat továbbító tagállam nemzeti biztonsági hatósága kérheti a kedvezményezettől a vizsgálat részleteinek ismertetését.