32001D0844

L 317/1 *AZ EURÓPAI KÖZÖSSÉGEK HIVATALOS LAPJA* 2001.12.3.

A BIZOTTSÁG HATÁROZATA
(2001. november 29.)
eljárási szabályzatának módosításáról

(az értesítés a C(2001) 3031. számú dokumentummal történt)

(2001/844/EK, ESZAK, Euratom)

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre és különösen annak 218. cikke (2) bekezdésére,

tekintettel az Európai Szén- és Acélközösséget létrehozó szerződésre és különösen annak 16. cikkére,

tekintettel az Európai Atomenergia-közösséget létrehozó szerződésre és különösen annak 131. cikkére,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 28. cikke (1) bekezdésére és 41. cikke (1) bekezdésére,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A Bizottság biztonsági rendelkezéseit, amelyek szövegét e határozat melléklete tartalmazza, mellékletként csatolják a Bizottság eljárási szabályzatához.

2. cikk

Ez a határozat az *Európai Közösségek Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Ezt a határozatot 2001. december 1-jétől kell alkalmazni.

Kelt Brüsszelben, 2001. november 29-én.

a Bizottság részéről

az elnök

Romano PRODI

MELLÉKLET

A BIZOTTSÁG BIZTONSÁGI RENDELKEZÉSEI

mivel:

(1) A Bizottság tevékenységének a bizonyos fokú titoktartást igénylő területeken történő továbbfejlesztése érdekében helyénvaló, hogy egy átfogó, a Bizottságra, az EK-Szerződés vagy az Európai Unióról szóló szerződés által vagy alapján létesített egyéb intézményekre, szervekre, hivatalokra és ügynökségekre, a tagállamokra, valamint az Európai Unió minősített információinak (a továbbiakban: „EU minősített információk") egyéb címzettjeire alkalmazandó biztonsági rendszert hozzanak létre.

(2) Az így létrehozott biztonsági rendszer eredményességének biztosítása érdekében a Bizottság az EU minősített információkat csak olyan külső szervek számára teszi hozzáférhetővé, amelyek biztosítékot nyújtanak arra nézve, hogy meghozták az ezekkel a rendelkezésekkel szigorúan egyenértékű szabályok alkalmazásához szükséges valamennyi intézkedést.

(3) Ezek a rendelkezések nem érintik az Európai Atomenergia-közösséget létrehozó szerződés 24. cikkének végrehajtásáról szóló, 1958. július 31-i 3. Euratom-tanácsi rendeletet ([1]), a titoktartási kötelezettség hatálya alá tartozó statisztikai adatoknak az Európai Közösségek Statisztikai Hivatalához történő továbbításáról szóló, 1990. június 11-i 1588/90/EK tanácsi rendeletet ([2]) és az információs rendszerek védelméről szóló, 1995. november 23-i C (95) 1510 végleges bizottsági határozatot.

(4) Az uniós döntéshozatali folyamat zökkenőmentes működésének biztosítása érdekében a Bizottság biztonsági rendszerét a Tanács biztonsági szabályzatának elfogadásáról szóló, 2001. március 19-i 2001/264/EK tanácsi határozatban ([3]) megállapított elvekre alapozzák.

(5) A Bizottság hangsúlyozza annak fontosságát, hogy adott esetben a többi intézmény is átvegye azokat a titoktartásra vonatkozó szabályokat és normákat, amelyek az Unió és tagállamai érdekeinek védelme érdekében szükségesek.

(6) A Bizottság elismeri, hogy saját biztonsági koncepció kialakítására van szükség, a biztonság valamennyi elemének és a Bizottság mint intézmény sajátos jellegének figyelembevételével.

(7) Ezek a rendelkezések nem érintik a Szerződés 255. cikkét és a nyilvánosságnak az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz történő hozzáféréséről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti, tanácsi és bizottsági rendeletet ([4]).

1. cikk

A Bizottság biztonsági szabályait a melléklet tartalmazza.

2. cikk

(1) A Bizottságnak a biztonsági ügyekért felelős tagja meghozza a megfelelő intézkedéseket annak biztosítása érdekében, hogy az EU minősített információk kezelése során az 1. cikkben említett szabályzatot a Bizottságon belül, valamint a Bizottság valamennyi helyiségében, beleértve az Unióban található képviseleteit és irodáit, továbbá a harmadik országokban felállított kirendeltségeit is, a bizottsági tisztviselők és az egyéb alkalmazottak, a Bizottsághoz kirendelt személyzet és a Bizottság külső szerződéses megbízottai tiszteletben tartsák.

(2) A tagállamok, valamint a Szerződések által vagy alapján létrehozott egyéb intézmények, szervek, hivatalok és ügynökségek azzal a feltétellel juthatnak hozzá az EU minősített információkhoz, ha biztosítják, hogy az ilyen információk kezelése során az 1. cikkben említetteknek szigorúan megfelelő szabályokat szolgálataikon belül és helyiségeikben betartják, különösen a következők:

a) a tagállamok Európai Unió melletti állandó képviseleteinek tagjai, valamint a Bizottság vagy annak szervei ülésein megjelenő vagy egyéb bizottsági tevékenységben részt vevő nemzeti delegációk tagjai,

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

c) az EU minősített információkat kezelő külső szerződéses megbízottak és kirendelt személyzet.

([1]) HL L 17., 1958.10.6., 406/58. o.
([2]) HL L 151., 1990.6.15., 1. o.
([3]) HL L 101., 2001.4.11., 1. o.
([4]) HL L 145., 2001.5.31., 43. o.

3. cikk

Harmadik államok, nemzetközi szervezetek és egyéb szervek azzal a feltétellel juthatnak hozzá EU minősített információkhoz, ha biztosítják, hogy az ilyen információk kezelése során az 1. cikkben említett szabályokkal szigorúan egyenértékű szabályokat betartják.

4. cikk

A melléklet I. részében foglalt alapelvek és biztonsági minimumszabályok betartásával a Bizottság biztonsági ügyekért felelős tagja a melléklet II. részének megfelelően intézkedéseket hozhat.

5. cikk

Alkalmazásuk időpontjától kezdve ezek a rendelkezések a következők helyébe lépnek:

a) az Európai Unió tevékenységének keretében előállított vagy továbbított, minősített információkra alkalmazandó biztonsági intézkedésekről szóló, 1994. november 30-i C (94) 3282 bizottsági határozat;

b) az olyan eljárásokról szóló, 1999. február 25-i C (99) 423 bizottsági határozat, amelyek alapján az Európai Bizottság tisztviselői és egyéb alkalmazottai felhatalmazást kaphatnak a Bizottság birtokában lévő minősített információkhoz történő hozzáférésre.

6. cikk

E rendelkezések alkalmazásának időpontjától fogva az eddig az időpontig a Bizottság birtokában lévő valamennyi minősített információ, az Euratom minősített információk kivételével:

a) alapértelmezésben – amennyiben azt a Bizottság készítette – „EU KORLÁTOZOTT” körbe átminősítettnek tekintendő, hacsak kibocsátója úgy nem határoz, hogy 2002. január 31-ig az információt más minősítési fokozatba sorolja. Ebben az esetben a kibocsátó tájékoztatja az érintett dokumentum valamennyi címzettjét;

b) eredeti minősítését – amennyiben a Bizottságon kívüli kibocsátók készítették –megtartja, és ily módon a vele egyenértékű minősítésű EU információként kezelendő, hacsak a kibocsátó bele nem egyezik az információ minősítésének megszüntetésébe vagy visszaminősítésébe.

MELLÉKLET

BIZTONSÁGI SZABÁLYOK

Tartalom

I. RÉSZ: ALAPELVEK ÉS A BIZTONSÁG MINIMUMSZABÁLYAI

1. BEVEZETÉS

Ezek a rendelkezések állapítják meg azokat az alapelveket és biztonsági minimumszabályokat, amelyeket a Bizottságnak valamennyi munkahelyén, valamint az EU minősített információk valamennyi címzettjének megfelelő módon be kell tartania, hogy a biztonságot megőrizzék, és mindegyikük biztos lehessen afelől, hogy a védelem közös szintje megvalósul.

2. ÁLTALÁNOS ELVEK

A Bizottság biztonsági politikája a Bizottság általános belső igazgatási politikájának szerves részét képezi, és így alapjául az általános politikájára irányadó elvek szolgálnak.

Ezek az elvek a törvényességet, az átláthatóságot, az elszámolási kötelezettséget és a szubszidiaritást (arányosságot) foglalják magukban.

A törvényesség annak szükségességét jelenti, hogy a biztonsági feladatok ellátása során szigorúan a törvényes keretek között kell maradni, és eleget kell tenni a jogi követelményeknek. Azt is jelenti, hogy a biztonság terén a hatásköröket megfelelő jogi rendelkezésekre kell alapozni. A személyzeti szabályzat rendelkezései – különösen a bizottsági információk tekintetében a személyzet titoktartási kötelezettségéről szóló 17. cikk, valamint a fegyelmi intézkedésekről szóló VI. cím – maradéktalanul érvényesek. A törvényesség végezetül azt jelenti, hogy a biztonságnak a Bizottság felelősségi körén belül történő megsértésével úgy kell foglalkozni, hogy az megfeleljen a Bizottság fegyelmi intézkedésekkel kapcsolatos politikájának és a büntető igazságszolgáltatás terén a tagállamokkal folytatott együttműködéssel kapcsolatos politikájának.

Az átláthatóság annak szükségességét jelenti, hogy valamennyi biztonsági szabálynak és rendelkezésnek világosnak kell lennie, hogy a különböző szolgálatok és a különböző területek között (fizikai biztonság kontra információk védelme stb.) egyensúlynak kell lennie, továbbá hogy következetes és strukturált biztonságtudatossági politikát kell folytatni. Az átláthatóság magában foglalja a biztonsági intézkedések végrehajtására szolgáló világos írásos iránymutatások szükségességét is.

Az elszámolási kötelezettség azt jelenti, hogy a biztonság terén a hatáskörök világosan meghatározásra kerülnek, valamint azt, hogy rendszeresen ellenőrizni kell, hogy az ezekből a hatáskörökből következő feladatokat megfelelő módon hajtották-e végre.

A szubszidiaritás vagy arányosság azt jelenti, hogy a biztonságot a lehető legalacsonyabb szinten és a Bizottság Főigazgatóságaihoz és szolgálataihoz a lehető legközelebb szervezik meg, valamint hogy a biztonsági tevékenységeket csak azokra a területekre korlátozzák, amelyek azokat valóban igénylik. Végezetül a szubszidiaritás vagy arányosság azt is jelenti, hogy a biztonsági intézkedéseknek arányosaknak kell lenniük a védeni kívánt érdekekkel, valamint az ezeket az érdekeket fenyegető tényleges vagy lehetséges veszéllyel, olyan védelmet biztosítva, amely a lehető legkisebb zavart okozza.

3. A BIZTONSÁG ALAPJAI

A stabil biztonság alapjai a következők:

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

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

   2. tájékoztatás és tanácsadás a kormányuk és rajta keresztül a Bizottság számára a biztonságot fenyegető veszélyek jellegéről és a védelem velük szemben alkalmazandó eszközeiről.

b) Minden egyes tagállamban és a Bizottságon belül egy technikai INFOSEC-hatóság (IA), 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) Rendszeres együttműködés a kormányzati hatóságok és az európai intézmények megfelelő szolgálatai körében annak érdekében, hogy szükség szerint határozzák meg és tegyenek ajánlást arra, hogy:

   1. mely személyeket, információkat és erőforrásokat kell megvédeni; és

   2. melyek legyenek a védelem közös szabályai.

d) Szoros együttműködés a Bizottság Biztonsági Hivatala és a többi európai intézmény biztonsági szolgálatai között, valamint a NATO Biztonsági Hivatalával (NOS).

4. AZ INFORMÁCIÓBIZTONSÁG ELVEI

4.1. **Célok**

Az információbiztonság terén az elsődleges célok a következők:

a) az EU minősített információk (EUCI) 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 a titkosságukat, integritásukat és rendelkezésre állásukat fenyegető veszélyekkel szemben;

c) az EU-információknak helyet adó bizottsági helyiségek 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.

4.2. **Fogalommeghatározások**

E szabályok alkalmazásában:

a) Az „EU minősített információ” (EUCI) kifejezés 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.

b) 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.

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

d) A „szükséges ismeret” kifejezés azt jelenti, hogy az illető alkalmazottnak hozzá kell férnie az EU minősített információkhoz annak érdekében, hogy valamilyen funkciót vagy feladatot képes legyen ellátni.

e) A „felhatalmazás” azt jelenti, hogy a Bizottság elnökének határozatával valamely személy számára hozzáférést biztosítanak az EU minősített információkhoz egy meghatározott szintig, a nemzeti biztonsági hatóság által a nemzeti jog alapján lefolytatott biztonsági ellenőrzés (átvilágítás) kedvező eredménye alapján.

f) A „minősítés” kifejezés azt jelenti, hogy azokhoz az információkhoz, amelyek engedély nélküli kiszolgáltatása a Bizottság vagy a tagállamok érdekeit bizonyos mértékben sértheti, a biztonság megfelelő szintjét rendelik.

g) A „visszaminősítés” (downgrading) kifejezés a minősítés szintjének csökkentését jelenti.

h) A „minősítés megszüntetése” (declassification) kifejezés a minősítési jelölés törlését jelenti.

i) A „kibocsátó” kifejezés a minősített dokumentum kellő felhatalmazással rendelkező szerzőjét jelenti. A Bizottságon belül a szervezeti egységek vezetői engedélyezhetik beosztottjaik számára EU minősített információk készítését.

j) A „Bizottság szervezeti egysége” kifejezés a Bizottság szervezeti egységeit és szolgálatait jelenti, a kabineteket is beleértve, valamennyi munkahelyen, köztük a Közös Kutatóközpontban, az Unió területén található képviseleteken és irodákban, valamint a harmadik országokban létrehozott delegációkon.

4.3. **Minősítés**

a) A titkosság 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 információ és anyag biztonsági szempontból mennyire fontos. A zökkenőmentes információáramlás biztosítása érdekében lépéseket kell tenni annak érdekében, hogy elkerüljék mind a túlzottan magas, mind pedig a túlzottan alacsony minősítést.

b) A minősítési rendszer ezen elvek gyakorlatba való átültetésének eszköze. Hasonló minősítési rendszer alkalmazandó a kémkedés, a szabotázs, a terrorizmus és az egyéb fenyegető veszélyek elleni intézkedések megtervezése és megszervezése során, hogy a minősített információknak helyet adó legfontosabb helyiségek és azokon belül a legérzékenyebb pontok részesüljenek a legmagasabb szintű védelemben.

c) Az információ minősítése kizárólag az adott információ kibocsátójának a feladata.

d) A minősítés szintje kizárólag az adott információ tartalmára alapozható.

e) Ha különböző információk kerülnek egy anyagba, akkor az egész anyag tekintetében alkalmazandó minősítési szintnek legalább olyan magasnak kell lennie, mint a legmagasabb minősítésű alkotórész minősítése. Az információk gyűjteménye azonban magasabb minősítést is kaphat, mint az alkotórészei külön-külön.

f) Minősítés csak akkor és annyi időre adható, amikor és ameddig az szükséges.

4.4. **A biztonsági intézkedések céljai**

A biztonsági intézkedéseknek:

a) ki kell terjedniük mindazon személyekre, akik minősített információkhoz férnek hozzá, 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).

5. A BIZTONSÁGI SZERVEZET

5.1. **Közös minimumszabályok**

A Bizottság biztosítja, hogy a biztonság közös minimumszabályait az EU minősített információk valamennyi, mind az intézményen belül, mind annak hatáskörében alkalmazott címzettje – például az összes szervezeti egység és szerződéses megbízott – betartsa, hogy az EU minősített információkat annak tudatában lehessen továbbítani, hogy azokat mindenhol ugyanolyan gondossággal kezelik. Ezek a minimumszabályok tartalmazzák a személyzet biztonsági ellenőrzésének kritériumait és az EU minősített információk védelmére irányuló eljárásokat.

A Bizottság az EU minősített információkhoz való hozzáférést külső szervek számára csak azzal a feltétellel engedélyezi, ha azok biztosítják, hogy az EU minősített információk kezelése során olyan rendelkezések betartásával járnak el, amelyek ezekkel a minimumszabályokkal legalább szigorúan egyenértékűek.

5.2. **Szervezet**

A Bizottságon belül a biztonság két szinten szerveződik:

a) A Bizottság egészének szintjén található a Bizottság Biztonsági Hivatala a Biztonsági Akkreditációs Hatósággal (SAA), amely kriptográfiai hatóságként (CrA) és TEMPEST-hatóságként egyaránt eljár, valamint az INFOSEC-hatósággal (IA) és egy vagy több, EU minősített információkat nyilvántartó központi hivatallal, amelyek mindegyikénél egy vagy több, a nyilvántartó hivatalt ellenőrző tisztviselő (RCO) dolgozik.

b) A bizottsági szervezeti egységek szintjén a biztonságért egy vagy több helyi biztonsági tisztviselő (LSO), egy vagy több központi informatikai biztonsági tisztviselő (CISO), helyi informatikai biztonsági tisztviselő (LISO), továbbá egy vagy több, a nyilvántartó hivatalt ellenőrző tisztviselővel működő, EU minősített információkat nyilvántartó helyi hivatal felel.

c) A központi biztonsági szervek operatív iránymutatást adnak a helyi biztonsági szervek számára.

6. A SZEMÉLYZET BIZTONSÁGA

6.1. **Biztonsági ellenőrzés**

Minden olyan személyt, akinek EU BIZALMAS 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, akiknek feladatkörébe a minősített információkat tartalmazó kommunikációs és információs rendszerek technikai üzemeltetése vagy karbantartása 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) külföldről vagy más helyről kiinduló nyomásgyakorlás révén sebezhetők-e.

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

d) számára EU SZIGORÚAN TITKOS minősítésű információkhoz való hozzáférést kell biztosítani;

e) olyan beosztásban dolgoznak, ahol rendszeresen jelentős mennyiségű EU TITKOS minősítésű információhoz férnek hozzá;

f) feladataik ellátása során különleges hozzáféréssel rendelkeznek a biztonságos kommunikációs vagy információs rendszerekhez, így lehetőségük van arra, hogy illetéktelenül kerüljenek nagy mennyiségű EU minősített információ birtokába, illetve technikai szabotázscselekmények útján súlyosan veszélyeztessék a feladat ellátását.

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

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.

6.2. **A személyzeti biztonsági felhatalmazások nyilvántartása**

Valamennyi bizottsági szervezeti egység, amely EU minősített információkat kezel vagy ahol biztonságos kommunikációs vagy információs rendszerek vannak elhelyezve, nyilvántartást vezet az oda kinevezett személyzet biztonsági felhatalmazásáról. A biztonsági felhatalmazást szükség esetén ellenőrzik annak érdekében, hogy megfeleljen az adott személy pillanatnyi 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. Saját területén a bizottsági szervezeti egység helyi biztonsági tisztviselője vezeti a biztonsági felhatalmazások nyilvántartását.

6.3. **A személyzet biztonsági képzése**

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. E személyek számára előírás, hogy írásban igazolják, miszerint ezeket a biztonsági rendelkezéseket elolvasták és teljes mértékben megértették.

6.4. **A vezetők felelőssége**

A vezetők kötelezettsége, hogy ismerjék a minősített információkkal dolgozó vagy a 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.

6.5. **A személyzet biztonsági státusa**

Eljárások megállapítására kerül sor annak biztosítása érdekében, hogy – amikor egy személlyel kapcsolatosan kedvezőtlen információk válnak ismertté – meghatározzák, az illető személy dolgozik-e minősített információkkal vagy rendelkezik-e hozzáféréssel biztonságos kommunikációs vagy információs rendszerekhez, és erről tájékoztassák a Bizottság Biztonsági Hivatalát. 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.

7. FIZIKAI BIZTONSÁG

7.1. **A védelem szükségessége**

Az EU minősített információk védelmének biztosítása érdekében alkalmazandó fizikai biztonsági intézkedések mértékének arányosnak kell lennie a birtokolt információk és anyagok minősítésével, mennyiségével és veszélyeztetettségével. 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.

7.2. **Ellenőrzés**

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.

7.3. **Az épületek biztonsága**

Az EU minősített információk vagy a biztonságos kommunikációs és információs rendszerek elhelyezésére szolgáló épületeket az illetéktelen behatolás ellen védeni kell. Az EU minősített információk számára nyújtott védelem jellege – 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; továbbá

c) az épület fizikai jellemzői és elhelyezkedése.

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 a biztonság veszélyeztetése 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.

7.4. **Vészhelyzeti tervek**

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

8. AZ INFORMÁCIÓBIZTONSÁG

Az információbiztonság (INFOSEC) a kommunikációs, információs és egyéb elektronikus rendszerekben kezelt, tárolt vagy továbbított EU minősített információk titkosságának, integritásának vagy rendelkezésre állásának – véletlenszerű vagy szándékos cselekedet által okozott – sérülése elleni védelmét szolgáló biztonsági intézkedések megállapítására és alkalmazására vonatkozik. Megfelelő óvintézkedéseket kell tenni annak érdekében, hogy megelőzzék illetéktelen felhasználók hozzáférését az EU minősített információkhoz, illetve hogy az arra jogosult felhasználók esetében megelőzzék az EU minősített információkhoz való hozzáférés megtagadását, továbbá hogy megelőzzék az EU minősített információk megrongálódását, illetéktelen módosítását vagy törlését.

9. A SZABOTÁZS ÉS A SZÁNDÉKOS RONGÁLÁS EGYÉB FORMÁI ELLENI VÉDELEM

A szabotázzsal és a szándékos rongálással szembeni leghatásosabb biztosítékot a minősített információk elhelyezésére szolgáló fontos berendezések védelmére irányuló fizikai óvintézkedések jelentik, s ezeket a személyzet biztonsági ellenőrzése önmagában nem helyettesítheti. Az illetékes nemzeti szerv feladata, hogy bűnüldözési operatív információkat gyűjtsön a kémkedés, a szabotázs, a terrorizmus és az egyéb felforgató tevékenységek tekintetében.

10. MINŐSÍTETT INFORMÁCIÓK ÁTADÁSA HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE

A Bizottság mint testület határoz a Bizottságban keletkezett EU minősített információk harmadik állam vagy nemzetközi szervezet részére történő átadásáról. Ha az átadni kért információ kibocsátója nem a Bizottság, akkor a Bizottság először a kibocsátó beleegyezését kéri ki az információ átadásához. Ha a kibocsátó kiléte nem állapítható meg, helyette a Bizottság határoz.

Ha a Bizottság valamely harmadik államtól, nemzetközi szervezettől vagy más harmadik felektől kap minősített információt, akkor ez az információ a minősítésének megfelelő és az ezekben a rendelkezésekben 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.

A fenti elvek alkalmazása a II. rész 26. szakaszában, valamint a 3., 4. és 5. függelékben rögzített részletes rendelkezéseknek megfelelően történik.

II. RÉSZ: A BIZTONSÁGI SZERVEZET A BIZOTTSÁGNÁL

11. A BIZOTTSÁG BIZTONSÁGI ÜGYEKÉRT FELELŐS TAGJA

A Bizottság biztonsági ügyekért felelős tagja:

a) végrehajtja a Bizottság biztonsági politikáját;

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

c) a tagállamok nemzeti biztonsági (vagy egyéb illetékes) hatóságaival („NSA”) szoros kapcsolatot tartva megvizsgálja a Bizottság biztonsági politikájának megváltoztatását szükségessé tevő kérdéseket.

A Bizottság biztonsági ügyekért felelős tagja különösen az alábbiakért felel:

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

b) megkeresés intézése a tagállamok kijelölt hatóságaihoz, hogy a nemzeti biztonsági hatóság a 20. szakaszban foglaltaknak megfelelően végezze el a Bizottságnál alkalmazott személyzet biztonsági ellenőrzését;

c) olyan esetek kivizsgálása vagy kivizsgáltatása, amikor EU minősített információk szivárogtak ki, ha a jelek arra utalnak, hogy ennek oka a Bizottságon belül keresendő;

d) az illetékes biztonsági hatóságok felkérése vizsgálatok indítására, amikor EU minősített információk szivárogtak ki, de úgy tűnik, hogy nem a Bizottságon belülről, továbbá a vizsgálatok összehangolása, ha azokban több biztonsági hatóság is részt vesz;

e) az EU minősített információk védelmére irányuló biztonsági rendelkezések rendszeres ellenőrzése;

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

g) a Bizottság biztonsági politikájának és eljárásainak folyamatos felülvizsgálata, és szükség esetén megfelelő ajánlások kidolgozása. E tekintetben a Bizottság biztonsági ügyekért felelős tagja terjeszti a Bizottság elé a Bizottság Biztonsági Hivatala által elkészített éves ellenőrzési tervet.

12. A BIZOTTSÁG BIZTONSÁGI POLITIKAI TANÁCSADÓ CSOPORTJA

Létrejön a Bizottság biztonsági politikai tanácsadó csoportja. Ez a szerv az egyes tagállamok nemzeti biztonsági hatóságainak a képviselőiből áll, elnöki tisztét a Bizottság biztonsági ügyekért felelős tagja vagy helyettese látja el. Más európai intézmények képviselői is meghívást kaphatnak. A megfelelő EK és EU decentralizált szervek képviselői is meghívást kaphatnak, ha őket érintő kérdéseket vitatnak meg.

A Bizottság biztonsági politikai tanácsadó csoportja az elnök vagy bármelyik tag kérésére ülésezik. A csoportnak az a feladata, hogy megvizsgálja és értékelje az összes vonatkozó biztonsági kérdést és adott esetben ajánlásokat terjesszen a Bizottság elé.

13. A BIZOTTSÁG BIZTONSÁGI TANÁCSA

Létrejön a Bizottság biztonsági tanácsa. Ez a szerv az elnöki tisztet ellátó főtitkárból, a jogi szolgálat, a személyzeti és igazgatási ügyek, a külső kapcsolatok, az igazság- és belügyek, valamint a Közös Kutatóközpont főigazgatóiból, továbbá a Belső Ellenőrzési Szolgálatnak és a Bizottság Biztonsági Hivatalának a vezetőjéből áll. Más bizottsági tisztviselők is meghívást kaphatnak. A biztonsági tanács feladata a biztonsági intézkedések értékelése a Bizottságon belül, és e területen ajánlások készítése a Bizottság biztonsági ügyekért felelős tagja számára.

14. A BIZOTTSÁG BIZTONSÁGI HIVATALA

A 11. szakaszban említett feladatok teljesítése érdekében a Bizottság Biztonsági Hivatala a Bizottság biztonsági ügyekért felelős tagjának rendelkezésére áll a biztonsági intézkedések összehangolásához, felügyeletéhez és végrehajtásához.

Biztonsági ügyekben a Bizottság biztonsági ügyekért felelős tagjának legfontosabb tanácsadója és egyben a biztonsági politikai tanácsadó csoport titkára a Bizottság Biztonsági Hivatalának vezetője. E minőségében ő irányítja a biztonsági szabályok naprakésszé tételét, és összehangolja a biztonsági intézkedéseket a tagállamok illetékes hatóságaival és adott esetben azokkal a nemzetközi szervezetekkel, amelyek a Bizottsággal biztonsági megállapodást kötöttek. Ennek érdekében összekötő tisztviselőként jár el.

A Bizottság Biztonsági Hivatalának vezetője felelős a Bizottságon belüli IT-rendszerek és IT-hálózatok akkreditációjáért. A Bizottság Biztonsági Hivatalának vezetője az illetékes nemzeti biztonsági hatósággal egyetértésben határoz az olyan IT-rendszerek és -hálózatok akkreditációjáról, amelyek egyrészről a Bizottságot, másrészről pedig az EU minősített információk egyéb címzettjeit érintik.

15. BIZTONSÁGI ELLENŐRZÉSEK

A Bizottság Biztonsági Hivatala rendszeresen ellenőrzi az EU minősített információk védelmére irányuló biztonsági intézkedéseket.

A Bizottság Biztonsági Hivatalát e feladatának ellátásában támogathatják EU minősített anyagokat birtokukban tartó más EU-intézmények biztonsági szolgálatai vagy a tagállamok nemzeti biztonsági hatóságai ([1]).

Valamely tagállam kérésére annak nemzeti biztonsági hatósága, a Bizottság biztonsági szolgálatával közösen és kölcsönös egyetértésben, az EU minősített információkkal kapcsolatos ellenőrzést folytathat le a Bizottságon belül.

([1]) A diplomáciai kapcsolatokról szóló 1961. évi Bécsi Egyezmény és az Európai Közösségek kiváltságairól és mentességeiről szóló, 1965. április 8-i jegyzőkönyv sérelme nélkül.

16. MINŐSÍTÉSEK, BIZTONSÁGI AZONOSÍTÓK ÉS JELÖLÉSEK

16.1. **Minősítési szintek** ([1])

Az információk minősítése a következő szintek szerint történik (lásd még a 2. függeléket is):

EU SZIGORÚAN TITKOS: 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.

EU TITKOS: 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.

EU BIZALMAS: 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.

EU KORLÁTOZOTT: 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.

Egyéb minősítés nem engedélyezett.

16.2. **Biztonsági azonosítók**

A minősítés érvényességi idejének behatárolására (azaz a minősített információk automatikus visszaminősítése vagy a minősítésük automatikus megszüntetése időpontjának maghatározására) egyezményes biztonsági jelölés használható. Ez a jelölés a „(dátum/időpont) ……-IG” vagy az „(esemény) ……-IG” lehet.

Olyan kiegészítő biztonsági azonosítók, mint a CRYPTO vagy egyéb, az EU által elismert biztonsági jelölés akkor alkalmazandó, ha a biztonsági minősítés által meghatározott kezelés mellett korlátozott elosztásra és különleges kezelésre van szükség.

Biztonsági azonosítókat csak minősítéssel együtt lehet használni.

16.3. **Jelölések**

Jelölést lehet használni a dokumentum által érintett terület vagy valamilyen, a „szükséges ismeret” elve alapján történő elosztás meghatározására, illetve (a nem minősített információk esetében) a tilalom végének jelzésére.

A jelölés nem minősítés, ezért helyette nem használható.

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.

16.4. **A minősítés feltüntetése**

A minősítés feltüntetése a következő módon történik:

a) EU KORLÁTOZOTT dokumentumokon mechanikus vagy elektronikus eszközökkel;

b) EU BIZALMAS dokumentumokon mechanikus eszközökkel vagy előre lebélyegzett, regisztrált papíron kézírással, illetve nyomtatással;

c) EU TITKOS és EU SZIGORÚAN TITKOS dokumentumokon mechanikus eszközökkel és kézírással.

16.5. **A biztonsági azonosítók feltüntetése**

A biztonsági azonosítókat közvetlenül a minősítés alatt tüntetik fel ugyanazokkal az eszközökkel, mint amelyeket a minősítések feltüntetésénél használnak.

([1]) Lásd az 1. függelékben az EU, a NATO, a WEU és a tagállamok biztonsági minősítéseinek összehasonlító táblázatát.

17. A MINŐSÍTÉS SZABÁLYAI

17.1. **Általános ismertetés**

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.

Az információ minősítése és későbbi visszaminősítése vagy a minősítés megszüntetése kizárólag a kibocsátó feladata.

Az információk minősítését, visszaminősítését vagy a minősítés megszüntetését a Bizottság tisztviselői és egyéb alkalmazottai szervezeti egységük vezetőjének utasítására vagy vele egyetértésben végzik el.

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

Az EU SZIGORÚAN TITKOS dokumentumok készítésére felhatalmazott személyek számát a lehető legkisebbre kell korlátozni és nevükről listát kell összeállítani, amelyet a Bizottság Biztonsági Hivatala vezet.

17.2. **Minősítések alkalmazása**

Egy dokumentum minősítését aszerint kell meghatározni, hogy tartalma a 16. szakasz meghatározásának megfelelően milyen mértékű védelmet igényel. Fontos, hogy a minősítést szabályosan használják és csak akkor alkalmazzák, ha valóban szükséges. Ez különösen az EU SZIGORÚAN TITKOS minősítésre vonatkozik.

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

A minősítésre vonatkozó gyakorlati útmutatót a 2. függelék tartalmazza.

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.

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.

A nyilvános hozzáférésre nézve továbbra is az 1049/2001/EK rendelet az irányadó.

17.3. **Visszaminősítés és a minősítés megszüntetése**

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 kibocsátó feladata tájékoztatni a címzetteket a minősítés megváltozásáról, akiknek viszont azokat a további címzetteket kell tájékoztatniuk erről, akiknek ők a dokumentumot megküldték vagy lemásolták.

Ha lehetséges, a kibocsátók a minősített dokumentumokon meghatározzák azt az időpontot, határidőt vagy eseményt, amikortól vagy amelynek lejártát, illetve bekövetkezését 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.

18. FIZIKAI BIZTONSÁG

18.1. **Általános ismertetés**

A fizikai biztonsági intézkedések fő célja, hogy megakadályozzák illetéktelen személyek hozzáférését EU minősített információkhoz és/vagy anyagokhoz, hogy megakadályozzák a berendezések és egyéb vagyontárgyak ellopását és megrongálását, továbbá a személyzet, a többi alkalmazott és a látogatók zaklatását vagy a velük szembeni agresszió egyéb formáit.

18.2. **Biztonsági követelmények**

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.

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 fenyegetések, valamint különösen a szabotázs, a terrorizmus és az egyéb felforgató tevékenységek és/vagy bűncselekmények helyi értékelése.

Az alkalmazott fizikai biztonsági intézkedések a következőkre irányulnak:

a) illetéktelen személyek titokban történő vagy erőszakos behatolásának megakadályozása;

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

c) az EU minősített információkhoz való hozzáférés megakadályozása azok számára, akiknek azokat nem szükséges ismerniük.

18.3. **Fizikai biztonsági intézkedések**

18.3.1. *Biztonsági területek*

Azokat a területeket, ahol EU BIZALMAS 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 EU BIZALMAS 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 EU BIZALMAS vagy ennél szigorúbb minősítésű információkat kezelnek és tárolnak olyan módon, hogy belső ellenőrzésekkel meg lehessen védeni azokat illetéktelen személyek hozzáférésével szemben, például az olyan irodahelyiségeknek helyt adó épületek, ahol EU BIZALMAS 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.

18.3.2. *Igazgatási terület*

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 EU KORLÁTOZOTT és nem minősített információkat szabad kezelni és tárolni.

18.3.3. *A be- és kilépés ellenőrzése*

Az I. és II. osztályba tartozó biztonsági területekre való be- és kilépést az állandó személyzet vonatkozásában alkalmazandó belépővel vagy személyfelismerő rendszer segítségével ellenőrzik. A látogatók ellenőrzésére olyan rendszert kell kialakítani, amely megakadályozza az EU minősített információkhoz való jogosulatlan hozzáférést. A belépő felmutatásán alapuló beléptetőrendszereket 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.

18.3.4. *Őrjáratok*

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.

18.3.5. *Biztonsági tárolóeszközök és páncélszobák*

Az EU minősített információk tárolására háromféle tárolóeszköz-osztály használatos:

– A osztály: I. vagy II. osztályba tartozó biztonsági területen EU SZIGORÚAN TITKOS minősítésű információk tárolására nemzeti szinten jóváhagyott tárolóeszközök,

– B osztály: I. vagy II. osztályba tartozó biztonsági területen EU TITKOS és EU BIZALMAS információk tárolására nemzeti szinten jóváhagyott tárolóeszközök,

– C osztály: csak EU KORLÁTOZOTT információk tárolására alkalmas irodai bútorok.

Az I. vagy II. osztályba tartozó biztonsági területen kiépített páncélszobák, továbbá minden olyan, I. osztályba tartozó biztonsági terület esetében, ahol EU BIZALMAS és ennél szigorúbb minősítésű információkat szabad polcon tárolnak vagy ábrákon, térképeken stb. mutatnak be, egy SAA-nak igazolnia kell, hogy a falak, a padlózat és a mennyezet, a zárral (zárakkal) felszerelt ajtó (ajtók) az ugyanilyen minősítésű információk tárolására jóváhagyott biztonsági tárolóeszköz-osztállyal egyenértékű védelmet biztosítanak.

18.3.6. *Zárak*

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 bútorok esetében megfelelő.

18.3.7. *A kulcsok és kombinációk ellenőrzése*

A biztonsági tárolóeszközök kulcsait nem szabad kivinni a Bizottság épületeiből. A biztonsági tárolóeszközök kombinációit kívülről meg kell tanulniuk azoknak a személyeknek, akiknek azokat ismerniük kell. Vészhelyzet esetén való felhasználás érdekében a Bizottság érintett szervezeti egységének 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.

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.

18.3.8. *Behatolásjelző berendezések*

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.

18.3.9. *Jóváhagyott berendezések*

A Bizottság Biztonsági Hivatala típus és modell szerint naprakész listákat vezet azokról a biztonsági berendezésekről, amelyeket különböző meghatározott körülmények között és feltételek mellett minősített információk közvetlen vagy közvetett védelméhez jóváhagyott. A Bizottság Biztonsági Hivatala ezeket a listákat többek között a nemzeti biztonsági hatóságoktól kapott információk alapján vezeti.

18.3.10. *A másológépek és telefaxok fizikai védelme*

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

18.4. **Rálátás és lehallgatás elleni védelem**

18.4.1. *Rálátás*

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

18.4.2. *Lehallgatás*

Azokat a hivatali helyiségeket, illetve területeket, ahol EU TITKOS 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 a Bizottság Biztonsági Hivatalának feladata, szükség esetén a nemzeti biztonsági hatóságokkal folytatott konzultációt követően.

18.4.3. *Elektronikus és felvevőberendezések bevitele*

A Bizottság Biztonsági Hivatala vezetőjének előzetes engedélye nélkül mobiltelefon, saját tulajdonú számítógép, hangrögzítő berendezés, kamera és egyéb elektronikus, illetve felvevőkészülék bevitele a biztonsági vagy a technikailag védett területekre nem megengedett.

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 Bizottság Biztonsági Hivatala a nemzeti biztonsági hatóságok szakértőinek segítségét kérheti.

Hasonlóképpen, ha a körülmények indokolják, a Bizottság Biztonsági Hivatala vezetőjének kérésére a nemzeti biztonsági hatóságok technikai biztonsági szakemberei ellenőrizhetik a távközlési berendezéseket és az EU TITKOS és annál magasabb szintű ülések során használt bármilyen elektromos vagy elektronikus irodai berendezéseket.

18.5. **Technikailag biztonságos területek**

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.

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 a megfelelő hatóság előzetes engedélye nélkül nem telepíthetők.

19. A „SZÜKSÉGES ISMERET” ELVÉRE ÉS AZ EU-SZEMÉLYZET BIZTONSÁGI ELLENŐRZÉSÉRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK

19.1 **Általános ismertetés**

Az EU minősített információkhoz való hozzáférést csak azoknak engedélyezik, akiknek feladataik vagy megbízatásuk ellátásához az információkat ismerniük szükséges. Az EU SZIGORÚAN TITKOS, EU TITKOS és EU BIZALMAS információkhoz való hozzáférést csak azon személyek számára engedélyezik, akiknek a megfelelő biztonsági ellenőrzése megtörtént.

Annak megállapítása, hogy kinek mit szükséges ismernie, annak a szervezeti egységnek a feladata, ahol az érintett személyt alkalmazni kívánják.

A személyzet biztonsági ellenőrzésének kérelmezése az egyes szervezeti egységek feladata.

Az eljárás eredményeképpen kiállításra kerül az „EU személyi 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 EU személyi biztonsági tanúsítvány birtokosa számára a kevésbé szigorú minősítésű információkhoz is hozzáférést biztosíthat.

A tisztviselőkön és egyéb alkalmazottakon kívül az olyan személyeknek, akikkel esetleg EU minősített információkat kell megtárgyalni vagy akik számára ilyen információkba kell betekintést biztosítani – például külső szerződéses megbízottaknak, szakértőknek vagy tanácsadóknak – az EU minősített információk tekintetében EU biztonsági ellenőrzésen kell átesniük, és tájékoztatni kell őket a biztonsággal kapcsolatos kötelezettségeikről.

A nyilvános hozzáférésre nézve továbbra is az 1049/2001/EK rendelet az irányadó.

19.2. **Az EU SZIGORÚAN TITKOS minősítésű információkhoz való hozzáférés különös szabályai**

Mindazokat a személyeket, akiknek EU SZIGORÚAN TITKOS minősítésű információkhoz kell hozzáférniük, először biztonsági ellenőrzésnek kell alávetni az ilyen információkhoz való hozzáférés tekintetében.

Mindazokat a személyeket, akiknek EU SZIGORÚAN TITKOS minősítésű információkhoz kell hozzáférniük, a Bizottság biztonsági ügyekért felelős tagja jelöli ki, és nevüket a megfelelő EU SZIGORÚAN TITKOS nyilvántartó hivatalban nyilván kell tartani. Ezt a nyilvántartó hivatalt a Bizottság Biztonsági Hivatala hozza létre és vezeti.

Az EU SZIGORÚAN TITKOS minősítésű információkhoz való hozzáférés előtt minden személynek alá kell írnia egy nyilatkozatot arról, hogy kioktatták a Bizottság biztonsági eljárásairól és teljes egészében megértette az EU SZIGORÚAN TITKOS minősítésű információk megőrzésével kapcsolatos különleges felelősségét, valamint azokat a következményeket, amelyeket az EU szabályai, a nemzeti jog vagy a közigazgatási szabályok írnak elő, ha minősített információk szándékosan vagy gondatlanságból illetéktelen személyek kezébe kerülnek.

Olyan személy esetében, aki üléseken stb. jut EU SZIGORÚAN TITKOS 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.

Az EU SZIGORÚAN TITKOS listáról törölni kell azoknak a személyeknek a nevét, akiket a továbbiakban nem alkalmaznak EU SZIGORÚAN TITKOS minősítésű információkhoz való hozzáférést igénylő feladatokra. Ezen túlmenően ezeknek a személyeknek ismételten fel kell hívni a figyelmét az EU SZIGORÚAN TITKOS minősítésű információk megőrzésére irányuló különleges felelősségükre. Alá kell írniuk egy nyilatkozatot is, amelyben kijelentik, hogy nem használják fel és nem adják tovább a birtokukban lévő EU SZIGORÚAN TITKOS minősítésű információkat.

19.3. **Az EU TITKOS és EU BIZALMAS információkhoz való hozzáférés különös szabályai**

Mindazokat a személyeket, akiknek EU TITKOS vagy EU BIZALMAS információkhoz kell hozzáférniük, először megfelelő szintű biztonsági ellenőrzésnek kell alávetni.

Mindazokkal a személyekkel, akiknek EU TITKOS vagy EU BIZALMAS információkhoz kell hozzáférniük, meg kell ismertetni a megfelelő biztonsági rendelkezéseket, és tudatában kell lenniük a gondatlanság következményeinek.

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

19.4. **Az EU KORLÁTOZOTT információkhoz való hozzáférés különös szabályai**

Az EU KORLÁTOZOTT információkhoz hozzáféréssel rendelkező személyek figyelmét fel kell hívni ezekre a biztonsági szabályokra és a gondatlanság következményeire.

19.5. **Áthelyezések**

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.

Ha a személyi állomány valamely tagját olyan más beosztásba helyezik, amely EU minősített anyagok kezelésével jár, az illető a helyi biztonsági tisztviselőtől ennek megfelelő oktatásban részesül.

19.6. **Különleges utasítások**

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 és a különérdekeket védő csoportok képviselőivel 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.

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.

A Bizottságnak nincsenek biztonsági rendelkezései arra az esetre, ha EU minősített információkhoz való hozzáférésre felhatalmazott személy bárhová magánjellegű utazást tesz. A Bizottság Biztonsági Hivatala azonban a hatáskörébe tartozó tisztviselőket és egyéb alkalmazottakat tájékoztatja a rájuk vonatkozó utazási rendelkezésekről.

20. A BIZOTTSÁG TISZTVISELŐIRE ÉS EGYÉB ALKALMAZOTTAIRA VONATKOZÓ BIZTONSÁGI ELLENŐRZÉSI ELJÁRÁS

a) A Bizottság birtokában lévő minősített információkhoz a Bizottságnak csak azon tisztviselői és egyéb alkalmazottai, illetve a Bizottságban dolgozók közül csak azon személyek férhetnek hozzá, akiknek feladataik alapján és a szolgálat követelményei miatt ismerniük vagy használniuk szükséges azokat.

b) Ahhoz, hogy a fenti a) pontban említett személyek hozzáférhessenek az „EU SZIGORÚAN TITKOS", „EU TITKOS" és „EU BIZALMAS" minősítésű információkhoz, az e szakasz c) és d) bekezdésében említett eljárásnak megfelelően felhatalmazással kell rendelkezniük.

c) A felhatalmazást csak azok kaphatják meg, akiket a tagállamok illetékes nemzeti hatóságai (NSA) az i)–n) pontban említett eljárásnak megfelelően biztonsági ellenőrzésnek vetettek alá.

d) Az a), b) és c) pontban említett felhatalmazások megadásáért a Bizottság Biztonsági Hivatalának vezetője felel.

e) A biztonsági hivatal vezetője azt követően adja meg a felhatalmazást, hogy megkapta a tagállamok illetékes nemzeti hatóságainak véleményét az i)–n) pontban említett eljárásnak megfelelően lefolytatott biztonsági ellenőrzés alapján.

f) A Bizottság Biztonsági Hivatala naprakész listát vezet a megfelelő bizottsági szervezeti egységek által megadott valamennyi kényes beosztásról és mindazokról a személyekről, akiknek (ideiglenes) felhatalmazást adtak.

g) Az ötéves időtartamra érvényes felhatalmazás érvényét veszti, ha az érintett személy már nem látja el azokat a feladatokat, amelyek a felhatalmazás megadását indokolták. A felhatalmazás az e) pontban említett eljárásnak megfelelően megújítható.

h) A Bizottság Biztonsági Hivatalának vezetője visszavonja a felhatalmazást, ha úgy ítéli meg, hogy erre megfelelő oka van. A felhatalmazás visszavonásáról szóló határozatról értesíteni kell az érintett személyt, aki kérheti, hogy a Bizottság Biztonsági Hivatalának vezetője hallgassa meg, továbbá az illetékes nemzeti hatóságot.

i) A biztonsági ellenőrzést az érintett személy közreműködésével és a Bizottság Biztonsági Hivatala vezetőjének kérésére folytatják le. A biztonsági ellenőrzés tekintetében a felhatalmazandó személy állampolgársága szerinti tagállam nemzeti hatósága az illetékes. Ha az érintett személy nem valamelyik EU tagállam állampolgára, akkor a Bizottság Biztonsági Hivatalának vezetője attól az EU tagállamtól fogja kérni a biztonsági ellenőrzés végrehajtását, ahol a személy lakóhellyel rendelkezik vagy szokásosan tartózkodik.

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

k) A Bizottság Biztonsági Hivatalának vezetője 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.

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

m) Ha a tagállam illetékes nemzeti hatóságai kedvező véleményt adnak, a Bizottság Biztonsági Hivatalának vezetője megadhatja a felhatalmazást az érintett személynek.

n) Az illetékes nemzeti hatóságok elutasító véleményéről értesítik az érintett személyt, aki kérheti, hogy a Bizottság Biztonsági Hivatalának vezetője hallgassa meg. Ha szükségesnek tartja, a Bizottság Biztonsági Hivatalának vezetője az illetékes nemzeti hatóságoktól lehetőségeikhez mérten további tájékoztatást kérhet. Ha az elutasító véleményt a hatóságok megerősítik, akkor a felhatalmazást nem lehet megadni.

o) Mindazok, akik a d) és e) bekezdés értelmében felhatalmazást kaptak, a felhatalmazás megadásának időpontjában, majd azt követően rendszeres 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.

p) A Bizottság Biztonsági Hivatalának vezetője minden szükséges intézkedést megtesz az e szakaszban foglaltak végrehajtása érdekében, különösen a felhatalmazással rendelkező személyek listájához való hozzáférés vonatkozásában irányadó szabályok tekintetében.

q) Kivételes esetben – ha a szolgálat érdekei úgy kívánják – a Bizottság Biztonsági Hivatalának vezetője, miután az illetékes nemzeti hatóságokat értesítette és azok erre egy hónapon belül nem reagáltak, legfeljebb hat hónapos időtartamra ideiglenes felhatalmazást adhat, amíg az i) pontban említett biztonsági ellenőrzés eredményét meg nem kapja.

r) Az így megadott feltételes és ideiglenes felhatalmazások nem biztosítanak hozzáférést EU SZIGORÚAN TITKOS minősítésű információkhoz. A hozzáférés ezekhez az információkhoz csak azokra a tisztviselőkre korlátozódik, akik ténylegesen és kedvező eredménnyel estek át a biztonsági ellenőrzésen az i) pontban foglaltaknak megfelelően. Az biztonsági ellenőrzés eredményére várva azok a tisztviselők, akik vonatkozásában EU SZIGORÚAN TITKOS szintű ellenőrzést kértek, ideiglenesen és feltételesen felhatalmazást kaphatnak az EU TITKOS vagy annál alacsonyabb minősítésű információkhoz való hozzáférésre.

21. AZ EU MINŐSÍTETT DOKUMENTUMOK ELŐÁLLÍTÁSA, ELOSZTÁSA, TOVÁBBÍTÁSA, A FUTÁROK BIZTONSÁGA, VALAMINT A FORDÍTÁSOK ÉS KIVONATOK KÜLÖNPÉLDÁNYAI

21.1. **Elkészítés**

1. Az EU-minősítéseket a 16. szakaszban megállapított módon kell alkalmazni, és az EU BIZALMAS és annál magasabb szintű minősítések esetében minden oldal tetején és alján, középen kell feltüntetni, továbbá minden oldalt meg kell számozni. Minden EU minősített dokumentumot hivatkozási számmal és keltezéssel kell ellátni. Az EU SZIGORÚAN TITKOS és EU TITKOS 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. Az EU BIZALMAS és annál magasabb minősítésű dokumentumok első oldalán minden mellékletet és csatolmányt fel kell sorolni.

2. Az EU BIZALMAS és annál magasabb minősítésű dokumentumokat csak olyan személyek gépelhetik, fordíthatják, tárolhatják, fénymásolhatják, másolhatják mágneses úton vagy vehetik mikrofilmre, akiket az EU minősített információkhoz való hozzáférés szempontjából legalább a kérdéses dokumentum megfelelő biztonsági minősítési szintjéig ellenőriztek.

3. A minősített dokumentumok számítógépes elkészítését szabályozó rendelkezéseket a 25. szakasz tartalmazza.

21.2. **Elosztás**

1. 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.

2. Az EU SZIGORÚAN TITKOS dokumentumokat az EU SZIGORÚAN TITKOS nyilvántartó hivatalokon keresztül osztják el (lásd a 22.2. szakaszt). Az EU SZIGORÚAN TITKOS üzenetek esetében az illetékes nyilvántartó hivatal engedélyezheti a kommunikációs központ vezetője számára, hogy elkészítse a címzettek listáján meghatározott számú másolatot.

3. Az EU TITKOS 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.

4. A főigazgatósághoz vagy a szolgálathoz történő beérkezés és az onnan való távozás időpontjában minden EU BIZALMAS és annál magasabb minősítésű dokumentumot regisztrálni kell a szervezeti egységek EU minősített információkat nyilvántartó helyi hivatalában. A rögzítendő adatoknak (hivatkozási szám, keltezés, 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 (lásd a 22.1. szakaszt).

21.3. **Az EU minősített dokumentumok továbbítása**

21.3.1. *Csomagolás, átvételi elismervény*

1. Az EU BIZALMAS 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.

2. Csak a nyilvántartó hivatalt ellenőrző tisztviselő (lásd a 22.1. szakaszt) 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 (lásd a 22.1. szakaszt) feljegyzi a boríték beérkezését, és csak a címzett személy nyithatja fel a belső borítékot és adhat elismervényt a benne foglalt dokumentum átvételéről.

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

4. 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.

5. Az EU BIZALMAS és annál magasabb minősítésű dokumentumok esetében a futárok és a küldöncök a küldeményszám alapján kapják meg az átvételi elismervényt.

21.3.2. *Továbbítás épületen vagy épületegyüttesen belül*

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.

21.3.3. *Továbbítás egyazon országon belül*

1. Egyazon országon belül az EU SZIGORÚAN TITKOS dokumentumok továbbítását csak hivatalos futárszolgálat vagy az EU SZIGORÚAN TITKOS minősítésű információkhoz való hozzáférésre felhatalmazott személyek végezhetik.

2. Ha EU SZIGORÚAN TITKOS dokumentumok épületen vagy épületegyüttesen kívülre történő továbbítására futárszolgálatot vesznek igénybe, akkor az e fejezetben foglalt, csomagolással és átvétellel kapcsolatos rendelkezéseket be kell tartani. A kézbesítő szolgálatoknak elegendő személyzettel kell rendelkezniük, amely biztosítja, hogy az EU SZIGORÚAN TITKOS dokumentumokat tartalmazó csomagok mindenkor egy felelős tisztviselő közvetlen felügyelete alatt maradjanak.

3. EU SZIGORÚAN TITKOS 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 az EU SZIGORÚAN TITKOS dokumentumokhoz;

   b) a szállítás módja megfelel az EU SZIGORÚAN TITKOS dokumentumok továbbítására irányadó szabályoknak;

   c) a tisztviselő semmilyen körülmények között sem hagyja őrizetlenül az EU SZIGORÚAN TITKOS dokumentumokat;

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

4. Egyazon országon belül az EU TITKOS és EU BIZALMAS 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.

5. A Bizottság Biztonsági Hivatala e szabályok alapján kidolgozza az EU minősített dokumentumok személyes szállítására vonatkozó utasításokat. A dokumentumokat 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 18. 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.

21.3.4. *Továbbítás egyik államból a másikba*

1. Az EU BIZALMAS és annál magasabb minősítésű anyagokat egyik tagállamból a másikba diplomáciai vagy katonai futárszolgálat útján kell továbbítani.

2. Azonban az EU TITKOS és EU BIZALMAS minősítésű anyag személyes szállítása is engedélyezhető, amennyiben a szállításra vonatkozó rendelkezések biztosítják, hogy az anyag ne kerülhessen illetéktelen személy kezébe.

3. A Bizottság biztonsági ügyekért felelős tagja engedélyezheti 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. Az EU TITKOS vagy annál alacsonyabb minősítésű anyagok diplomáciai és katonai futárokon kívüli más személyek által történő nemzetközi személyes szállítására vonatkozó utasításokat a Bizottság Biztonsági Hivatala dolgozza ki. Ezeknek az utasításoknak a következőket kell tartalmazniuk:

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

   b) a megfelelő szervezeti egységnek 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, a kiválasztott útvonal és az igénybe venni kívánt szállítóeszköz tekintetében feleljen meg az EU szabályoknak, illetve ha e tekintetében a nemzeti szabályok szigorúbbak, ez utóbbiaknak;

g) az anyag nem kerülhet ki az azt szállító személy birtokából, kivéve ha azt a 18. 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;

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

4. 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.

21.3.5. *EU korlátozott dokumentumok továbbítása*

Attól eltekintve, hogy a szállítás során biztosítani kell, hogy a dokumentumok ne kerülhessenek illetéktelen személyek kezébe, az EU KORLÁTOZOTT dokumentumok szállítására nézve különleges rendelkezések nincsenek megállapítva.

21.4. **A futárok biztonsága**

Az EU TITKOS és EU BIZALMAS dokumentumok szállítására alkalmazott valamennyi futárnak és küldöncnek megfelelő biztonsági felhatalmazással kell rendelkeznie.

21.5. **A technikai továbbítás elektronikus és egyéb eszközei**

1. Az EU minősített információk biztonságos továbbítását a kommunikációs biztonságot szolgáló intézkedések hivatottak biztosítani. Az EU minősített információk továbbítására vonatkozó részletes szabályokat a 25. szakasz tartalmazza.

2. Csak akkreditált kommunikációs központok és hálózatok és/vagy terminálok és rendszerek továbbíthatnak EU BIZALMAS és EU TITKOS minősítésű információkat.

21.6. **Az EU minősített dokumentumok különpéldányai és fordításai, valamint a belőlük készített kivonatok**

1. EU SZIGORÚAN TITKOS dokumentumok másolását vagy fordítását csak a kibocsátójuk engedélyezheti.

2. Ha EU SZIGORÚAN TITKOS biztonsági felhatalmazással nem rendelkező személyek kérnek olyan információkat, amelyek – bár azokat EU SZIGORÚAN TITKOS dokumentumok tartalmazzák – nem rendelkeznek ilyen minősítéssel, akkor az EU SZIGORÚAN TITKOS nyilvántartó hivatal vezetője (lásd a 22.2. szakaszt) engedélyt kaphat arra, hogy az adott dokumentumból a szükséges számú kivonatot elkészítse. Egyidejűleg meg kell tennie a szükséges intézkedéseket annak biztosítására, hogy ezek a kivonatok megkapják a megfelelő biztonsági minősítést.

3. Az EU TITKOS és az annál alacsonyabb minősítésű dokumentumokat a címzett is sokszorosíthatja és lefordíthatja az itt részletezett biztonsági rendelkezések keretein belül, illetve azzal a feltétellel, hogy szigorúan betartja a „szükséges ismeret” elvét. Az eredeti dokumentumra vonatkozó biztonsági intézkedések a másolatokra és/vagy a fordításokra is vonatkoznak.

22. *AZ EU MINŐSÍTETT INFORMÁCIÓK NYILVÁNTARTÓ HIVATALAI, SZÁMBAVÉTELE, ELLENŐRZÉSE, ARCHÍV TÁROLÁSA ÉS MEGSEMMISÍTÉSE*

22.1. **Az EU minősített információk helyi nyilvántartó hivatalai**

1. Az EU TITKOS és az EU BIZALMAS minősítésű dokumentumok nyilvántartásba vételéért, sokszorosításáért, továbbításáért, archiválásáért és megsemmisítéséért a Bizottságon belül az egyes szervezeti egységekben az EU minősített információk – igények szerinti – egy vagy több helyi nyilvántartó hivatala felel.

2. Ha a szervezeti egység nem rendelkezik EU minősített információk helyi nyilvántartó hivatalával, akkor a főtitkárság EU minősített információk helyi nyilvántartó hivatala jár el a szervezeti egység EU minősített információinak nyilvántartó hivatalaként.

3. AZ EU minősített információk helyi nyilvántartó hivatalai azon szervezeti egység vezetőjének tartoznak jelentéstételi kötelezettséggel, akitől utasításaikat kapják. E nyilvántartó hivatalok vezetője a nyilvántartó hivatalt ellenőrző tisztviselő (RCO).

4. A nyilvántartó hivatalok az EU minősített dokumentumok kezelésére vonatkozó rendelkezések alkalmazását és a megfelelő biztonsági intézkedések betartását illetően a helyi biztonsági tisztviselő felügyelete alá tartoznak.

5. Az EU minősített információk helyi nyilvántartó hivatalaihoz kinevezett tisztviselők számára a 20. szakaszban foglaltaknak megfelelően engedélyezik az EU minősített információkhoz való hozzáférést.

6. A megfelelő szervezeti egység vezetőjének felügyelete alatt az EU minősített információk helyi nyilvántartó hivatalai:

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

   b) naprakészen tartják a minősített információkra vonatkozó adatok listáját;

   c) rendszeres időközönként rákérdeznek, hogy szükséges-e az információ minősítésének további fenntartása.

7. Az EU minősített információk helyi nyilvántartó hivatalai az alábbi adatokról vezetnek nyilvántartást:

   a) a minősített információ előállításának időpontja;

   b) a minősítés szintje;

   c) a minősítés lejártának időpontja;

   d) a kibocsátó neve és szervezeti egysége;

   e) a címzett vagy címzettek és sorszámuk;

   f) tárgy;

   g) szám;

   h) a szétosztott példányok száma;

   i) a szervezeti egységhez benyújtott minősített információk leltárának elkészítése;

   j) a minősített információk visszaminősítésének és minősítésük megszüntetésének nyilvántartása.

8. A 21. szakaszban előírt általános szabályok a Bizottság EU minősített információk helyi nyilvántartó hivatalaira is vonatkoznak, hacsak azokat az ebben a szakaszban megállapított különös szabályok nem módosítják.

22.2. **Az EU SZIGORÚAN TITKOS nyilvántartó hivatal**

22.2.1. *Általános ismertetés*

1. Az EU SZIGORÚAN TITKOS dokumentumok nyilvántartását, kezelését és elosztását ezeknek a biztonsági rendelkezéseknek megfelelően egy központi EU SZIGORÚAN TITKOS nyilvántartó hivatal biztosítja. Az EU SZIGORÚAN TITKOS nyilvántartó hivatal vezetője az EU SZIGORÚAN TITKOS nyilvántartó hivatalt ellenőrző tisztviselő.

2. A központi EU SZIGORÚAN TITKOS nyilvántartó hivatal jár el a Bizottságnál fő átvevő és elosztó hatóságként más olyan EU intézmények, tagállamok, nemzetközi szervezetek és harmadik államok tekintetében, amelyekkel a Bizottság minősített információk cseréjére irányuló biztonsági eljárásokról szóló megállapodást kötött.

3. Ha szükséges, alárendelt nyilvántartó hivatalokat hoznak létre, amelyek az EU SZIGORÚAN TITKOS dokumentumok belső igazgatásáért felelnek. Ezek naprakész nyilvántartást vezetnek a felelősségi körükbe tartozó minden dokumentum elosztásáról.

4. A hosszú távú igényekre reagálva a 22.2.3. szakaszban meghatározott módon EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatalokat hoznak létre, és ezeket a központi EU SZIGORÚAN TITKOS nyilvántartó hivatalhoz csatolják. Ha az EU SZIGORÚAN TITKOS dokumentumokba csak ideiglenesen és alkalmanként kell betekinteni, akkor ezeket a dokumentumokat EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatal létrehozása nélkül is ki lehet adni, feltéve hogy szabályokat állapítanak meg annak biztosítása érdekében, hogy a dokumentumok a megfelelő EU SZIGORÚAN TITKOS nyilvántartó hivatal ellenőrzése alatt maradjanak és az összes fizikai és személyzeti biztonsági intézkedést betartsák.

5. Az alárendelt nyilvántartó hivatalok közvetlenül nem továbbíthatnak EU SZIGORÚAN TITKOS dokumentumokat az ugyanazon központi EU SZIGORÚAN TITKOS nyilvántartó hivatalhoz tartozó többi alárendelt nyilvántartó hivatal számára az előbbi kifejezett engedélye nélkül.

6. A nem ugyanahhoz a központi nyilvántartó hivatalhoz tartozó alárendelt nyilvántartó hivatalok között az EU SZIGORÚAN TITKOS dokumentumok minden cseréjét a központi EU SZIGORÚAN TITKOS nyilvántartó hivatalon keresztül kell lebonyolítani.

22.2.2. *A központi EU SZIGORÚAN TITKOS nyilvántartó hivatal*

A központi EU SZIGORÚAN TITKOS nyilvántartó hivatal vezetője mint ellenőrző tisztviselő az alábbiakért felel:

a) az EU SZIGORÚAN TITKOS dokumentumok továbbítása a 21.3. szakaszban meghatározott rendelkezéseknek megfelelően;

b) lista vezetése az alá tartózó valamennyi EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatalról, a kinevezett ellenőrző tisztviselők és felhatalmazott helyetteseik nevével és aláírásával együtt;

c) a nyilvántartó hivataloktól kapott átvételi elismervények megőrzése a központi nyilvántartó hivatal által elosztott valamennyi EU SZIGORÚAN TITKOS dokumentum vonatkozásában;

d) nyilvántartás vezetése a birtokukban levő és az elosztott EU SZIGORÚAN TITKOS dokumentumokról;

e) naprakész lista vezetése az összes olyan központi EU SZIGORÚAN TITKOS nyilvántartó hivatalról, amellyel rendszeresen levelezésben áll, a kinevezett ellenőrző tisztviselők és felhatalmazott helyetteseik nevével és aláírásával együtt;

f) a nyilvántartó hivatal birtokában levő valamennyi EU SZIGORÚAN TITKOS dokumentum fizikai megőrzése a 18. szakaszban foglalt rendelkezéseknek megfelelően.

22.2.3. *EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatalok*

Az EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatal vezetője mint ellenőrző tisztviselő az alábbiakért felel:

a) az EU SZIGORÚAN TITKOS dokumentumok továbbítása a 21.3. szakaszban meghatározott rendelkezéseknek megfelelően;

b) naprakész lista vezetése az összes olyan személyről, aki felhatalmazással rendelkezik az ellenőrzése alá tartozó EU SZIGORÚAN TITKOS információkhoz való hozzáférésre;

c) az EU SZIGORÚAN TITKOS dokumentumok elosztása a kibocsátójuk utasításainak megfelelően vagy a „szükséges ismeret” elve alapján történjék, miután először ellenőrizte, hogy a címzett rendelkezik-e a megfelelő szintű biztonsági felhatalmazással;

d) naprakész nyilvántartás vezetése az ellenőrzése alá tartozó valamennyi birtokolt vagy elosztott, illetve más EU SZIGORÚAN TITKOS nyilvántartó hivataloknak átadott EU SZIGORÚAN TITKOS dokumentumról, továbbá az összes megfelelő átvételi elismervény megőrzése;

e) naprakész lista vezetése azokról az EU SZIGORÚAN TITKOS nyilvántartó hivatalokról, amelyekkel jogosult EU SZIGORÚAN TITKOS dokumentumokat kicserélni, az ellenőrző tisztviselők és felhatalmazott helyetteseik nevével és aláírásával együtt;

f) az alárendelt nyilvántartó hivatal birtokában levő valamennyi EU SZIGORÚAN TITKOS dokumentum fizikai megőrzése a 18. szakaszban megállapított szabályoknak megfelelően.

22.3. **Az EU minősített dokumentumok leltárai, számbavétele és ellenőrzése**

1. Az ebben a szakaszban említett minden egyes EU SZIGORÚAN TITKOS nyilvántartó hivatal évente tételes leltárt készít az EU SZIGORÚAN TITKOS dokumentumokról. Akkor tekinthető úgy, hogy egy dokumentummal elszámoltak, ha a nyilvántartó hivatalban fizikailag megtalálható vagy a hivatal rendelkezik annak az EU SZIGORÚAN TITKOS nyilvántartó hivatalnak az átvételi elismervényével, amelynek a dokumentumot továbbította, illetve ha birtokában van a dokumentum megsemmisítési jegyzőkönyve vagy az adott dokumentum visszaminősítését vagy minősítésének megszüntetését elrendelő utasítás. Az éves leltárok megállapításait legkésőbb minden év április 1-jéig kell eljuttatni a Bizottság biztonsági ügyekért felelős tagjának.

2. Az EU SZIGORÚAN TITKOS alárendelt nyilvántartó hivatalok az éves leltár megállapításait a felettes központi nyilvántartó hivatalnak azon a napon továbbítják, amelyet ez utóbbi megjelölt.

3. Az EU SZIGORÚAN TITKOS szint alatti EU minősített dokumentumokon kötelező belső ellenőrzéseket végeznek a Bizottság biztonsági ügyekért felelős tagja utasításainak megfelelően.

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

   a) egyes dokumentumok visszaminősítésének vagy minősítésük megszüntetésének lehetőségéről;

   b) a megsemmisítendő dokumentumokról.

22.4. **Az EU minősített dokumentumok irattári tárolása**

1 Az EU minősített információkat olyan feltételek mellett tárolják, amelyek megfelelnek a 18. szakaszban felsorolt valamennyi követelménynek.

2. Annak érdekében, hogy a tárolás minél kevesebb problémával járjon, az összes nyilvántartó hivatal ellenőrző tisztviselői felhatalmazást kapnak arra, hogy az EU SZIGORÚAN TITKOS, EU TITKOS és EU BIZALMAS dokumentumokat mikrofilmre vegyék vagy egyéb módon, mágneses vagy optikai adathordozón tárolják irattári megőrzés céljából, feltéve hogy:

   a) a mikrofilmre vétel/tárolás eljárását 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) az EU SZIGORÚAN TITKOS dokumentum mikrofilmre vételéről/tárolásáról kibocsátója értesítést kap;

   d) a filmtekercsek vagy más típusú adathordozók csak azonos EU SZIGORÚAN TITKOS, EU TITKOS, illetve EU BIZALMAS minősítésű dokumentumokat tartalmaznak;

   e) az EU SZIGORÚAN TITKOS vagy EU TITKOS dokumentum mikrofilmre vételét/tárolását világosan feltüntetik az éves leltárnál használt nyilvántartásban;

   f) a mikrofilmre vett vagy más módon tárolt dokumentumok eredetijét a 22.5. szakaszban rögzített szabályoknak megfelelően megsemmisítik.

3. Ezek a szabályok vonatkoznak a tárolás egyéb engedélyezett formáira, például az elektromágneses adathordozókra és az optikai lemezekre is.

22.5. **Az EU minősített dokumentumok megsemmisítése**

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

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

   c) Az EU SZIGORÚAN TITKOS dokumentumokat – az EU SZIGORÚAN TITKOS dokumentumok készítése során keletkezett valamennyi minősített hulladékot is beleértve, mint például a rontott példányok, piszkozatok, gépelt jegyzetek, flopilemezek – az EU SZIGORÚAN TITKOS nyilvántartó hivatalt ellenőrző tisztviselő felügyelete alatt elégetéssel, zúzással, felaprítással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tévő módszerrel kell megsemmisíteni.

2. Az EU TITKOS dokumentumokat az 1. c) pontban említett eljárások egyikét alkalmazva, egy biztonsági felhatalmazással rendelkező személy felügyelete alatt az a nyilvántartó hivatal semmisíti meg, amelyik felel értük. A megsemmisített EU TITKOS dokumentumokról aláírt megsemmisítési jegyzőkönyvet kell felvenni, amelyet a nyilvántartó hivatal az elosztóívekkel együtt legalább három évig megőriz.

3. Az EU BIZALMAS dokumentumokat az 1. c) pontban említett eljárások egyikét alkalmazva, egy biztonsági felhatalmazással rendelkező személy felügyelete alatt az a nyilvántartó hivatal semmisíti meg, amelyik felel értük. Megsemmisítésüket a Bizottság biztonsági ügyekért felelős tagjától kapott utasításoknak megfelelően kell nyilvántartani.

4. Az EU KORLÁTOZOTT dokumentumokat a Bizottság biztonsági ügyekért felelős tagjától kapott utasításoknak megfelelően vagy a felhasználó vagy az a nyilvántartó hivatal semmisíti meg, amelyik felel értük.

22.6. **Megsemmisítés vészhelyzetben**

1. A Bizottság szervezeti egységei a helyi feltételek alapján terveket dolgoznak ki az EU minősített anyagok válsághelyzetben történő védelmére, beleértve adott esetben a vészhelyzeti megsemmisítési és kiürítési terveket is. Kiadják az annak megakadályozására szükségesnek ítélt utasításokat, hogy az EU minősített információk illetéktelen személyek kezébe kerülhessenek.

2. Az EU TITKOS és EU BIZALMAS anyagok válsághelyzetben történő védelmére és/vagy megsemmisítésére irányuló intézkedések semmilyen körülmények között sem akadályozhatják az olyan EU SZIGORÚAN TITKOS anyagok – a kriptográfiai berendezéseket is beleértve – védelmét vagy megsemmisítését, amelyek ellátása minden más feladattal szemben elsőbbséget élvez.

3. A kriptográfiai berendezések vészhelyzetben történő védelmére és megsemmisítésére vonatkozó intézkedéseket különleges utasítások útján szabályozzák.

4. Az utasításokat a helyszínen, lepecsételt borítékban kell elhelyezni. A megsemmisítés eszközeinek/szerszámainak rendelkezésre kell állniuk.

23. A BIZOTTSÁG HELYISÉGEIN KÍVÜL MEGTARTOTT, EU MINŐSÍTETT INFORMÁCIÓKAT TÁRGYALÓ KÜLÖNLEGES ÜLÉSEK ESETÉBEN ALKALMAZANDÓ BIZTONSÁGI INTÉZKEDÉSEK

23.1. **Általános ismertetés**

Amennyiben a Bizottság üléseit vagy más fontos üléseket a Bizottság helyiségein kívül tartják meg, továbbá amennyiben ezt a megtárgyalt kérdések vagy információk fokozottan kényes természetével kapcsolatos különleges biztonsági követelmények indokolják, az alábbiakban ismertetett biztonsági intézkedéseket kell megtenni. Ezek az intézkedések csak az EU minősített információk védelmére vonatkoznak, így esetleg egyéb biztonsági intézkedéseket is szükséges lehet tervbe venni.

23.2. **Hatáskörök**

23.2.1. *A Bizottság Biztonsági Hivatala*

Annak érdekében, hogy biztosítsák a Bizottság ülésének vagy más fontos ülésnek, valamint a küldötteknek és munkatársaiknak a biztonságát, a Bizottság Biztonsági Hivatala együttműködik annak a tagállamnak az illetékes hatóságaival, amelynek területén az ülést tartják (fogadó tagállam). A biztonság védelmét illetően a hivatalnak 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 Bizottság kommunikációs rendszeréhez. A fogadó tagállamot szükség esetén felkéri, hogy biztosítson hozzáférést biztonságos telefonrendszerekhez.

A Bizottság Biztonsági Hivatala az ülés előkészítése során biztonsági tanácsadóként jár el. Az ülésen képviseltetnie kell magát, hogy szükség esetén segítse és tanácsokkal lássa el az ülés biztonsági tisztviselőjét (MSO) és a küldöttségeket.

Az ülésen részt vevő minden küldöttséget felkérnek arra, hogy jelölje ki biztonsági tisztviselőjét, aki a küldöttségén belül a biztonsági ügyek kezeléséért és az ülés biztonsági tisztviselőjével, valamint adott esetben a Bizottság Biztonsági Hivatalának képviselőjével való kapcsolattartásért felel.

23.2.2. *Az ülés biztonsági tisztviselője (MSO)*

Ki kell nevezni az ülés biztonsági tisztviselőjét, akinek feladata az általános belső biztonsági intézkedések általános kidolgozása és ellenőrzése, valamint a többi érintett biztonsági hatósággal folytatott egyeztetés. Az MSO által tett intézkedések általában az alábbiakra terjednek ki:

a) 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.

b) Az ülés helyszínére, a küldöttségek számára biztosított területekre és a konferenciatermekbe belépési engedéllyel rendelkező személyzet, valamint a berendezések ellenőrzése.

c) Állandó egyeztetés a fogadó tagállam illetékes hatóságaival és a Bizottság Biztonsági Hivatalával.

d) A biztonsági utasítások beillesztése az ülés dossziéjába, kellőképpen figyelembe véve az ezekben a biztonsági szabályokban rögzített követelményeket és minden egyéb, szükségesnek ítélt biztonsági utasítást.

23.3. **Biztonsági intézkedések**

23.3.1. *Biztonsági területek*

A következő biztonsági területeket kell kialakítani:

a) egy II. osztályba tartozó biztonsági terület, amely a szerkesztői szobát, a Bizottság irodáit és a reprográfiai berendezéseket, valamint adott estben 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.

23.3.2. *Belépők*

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

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.

A kitűzőt viselő résztvevők mellett az ülés helyszínére a lehető legkevesebb számú embert engedik be. Csak az MSO engedélyezheti a nemzeti küldöttségek számára, hogy kérésre az ülés alatt látogatókat fogadjanak. 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.

23.3.3. *Fényképezőgépek és hangrögzítő berendezések ellenőrzése*

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

23.3.4. *Aktatáskák, hordozható számítógépek és csomagok ellenőrzése*

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 MSO szükségesnek tartja, az aktatáskák és csomagok átvizsgálására szigorúbb intézkedéseket is hozhat.

23.3.5. *Technikai biztonság*

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

23.3.6. *A küldöttségek dokumentumai*

A küldöttségek felelnek az EU minősített dokumentumoknak az ülésekre és az onnan történő 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.

23.3.7. *A dokumentumok biztonságos megőrzése*

Ha 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.

23.3.8. *Az irodahelyiségek ellenőrzése*

Az ülés biztonsági tisztviselője gondoskodik arról, hogy a Bizottság 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.

23.3.9. *Az EU minősített hulladék ártalmatlanítása*

Minden hulladék EU minősített anyagként kezelendő és tárolásához szemeteskosarakat vagy -zsákokat kell biztosítani a Bizottság és a küldöttségek részére. A Bizottság és a küldöttségek tagjai a számukra kijelölt helyiségek elhagyása előtt átadják a hulladékot az ülés biztonsági tisztviselőjének, aki intézkedik az előírásszerű megsemmisítésről.

Az ülés végén a Bizottság és a küldöttségek birtokában levő, de már szükségtelen minden dokumentumot hulladékként kell kezelni. Az üléssel kapcsolatban hozott biztonsági intézkedések megszüntetése előtt a Bizottság és a küldöttségek helyiségeit alaposan át kell vizsgálni. Az átvételi elismervény ellenében átvett dokumentumokat, amilyen mértékben csak lehetséges, a 22.5. szakaszban előírtak szerint semmisítik meg.

24. A BIZTONSÁG MEGSÉRTÉSE ÉS AZ EU MINŐSÍTETT INFORMÁCIÓK ILLETÉKTELENEK TUDOMÁSÁRA JUTÁSA

24.1. **Fogalommeghatározások**

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

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.

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.

24.2. **A biztonság megsértésének jelentése**

Minden olyan személyt, akinek EU minősített információkat kell kezelnie, alaposan tájékoztatni kell az e területen fennálló felelősségéről. Azonnal jelenteniük kell, ha tudomást szereznek arról, hogy a biztonságot megsértették.

Ha a helyi biztonsági tisztviselő vagy az ülés biztonsági tisztviselője felfedezi, hogy az EU minősített információkra vonatkozó biztonságot megsértették vagy azt, hogy EU minősített anyagok vesztek vagy tűntek el, illetve erről tájékoztatást kap, akkor idejében intézkedéseket tesz:

a) a bizonyítékok megőrzésére;

b) a tényállás megállapítására;

c) az okozott kár felmérésére és minimalizálására;

d) az ismételt előfordulás megelőzésére; valamint

e) 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.

Az egyes biztonsági hatóságok, amint értesítést kaptak arról, hogy a biztonság megsértésére sor kerülhetett, haladéktalanul kötelesek jelenteni ezt a tényt a Bizottság Biztonsági Hivatalának.

Az EU KORLÁTOZOTT információkkal kapcsolatos eseteket csak akkor kell jelenteni, ha szokatlan jellemzőket mutatnak.

Miután a Bizottság biztonsági ügyekért felelős tagja értesült arról, hogy a biztonságot megsértették:

a) értesíti a kérdéses minősített információt kibocsátó hatóságot;

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.

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

24.3. **Jogi lépések**

Az EU minősített információk illetéktelenek tudomására jutásáért felelős személyt a vonatkozó szabályok és rendelkezések értelmében, különösen a személyzeti szabályzat VI. címének megfelelően fegyelmi eljárás alá vonhatják. Ez az eljárás nem érinti az esetleges bírósági eljárást.

Adott esetben a Bizottság biztonsági ügyekért felelős tagja a 24.2. szakaszban említett jelentés alapján minden szükséges lépést megtesz annak érdekében, hogy az illetékes nemzeti hatóságok büntetőeljárást indíthassanak.

25. AZ IT-RENSZEREKBEN ÉS KOMMUNIKÁCIÓS RENDSZEREKBEN KEZELT EU MINŐSÍTETT INFORMÁCIÓK VÉDELME

25.1. **Bevezetés**

25.1.1. *Általános ismertetés*

A biztonsági politika és a biztonsági követelmények minden olyan kommunikációs és információs rendszerre és hálózatra (a továbbiakban: rendszerek) vonatkoznak, amelyek EU BIZALMAS és annál magasabb minősítésű információkat kezelnek. Ezeket az informatikai rendszerek védelméről szóló, 1995. november 23-i C (95) 1510 végleges bizottsági határozat kiegészítéseként alkalmazzák.

Az ilyen információk titkosságának védelme érdekében az EU KORLÁTOZOTT információkat kezelő rendszerek esetében is szükség van biztonsági intézkedésekre. Minden rendszernél szükségesek biztonsági intézkedések maguknak a rendszereknek és a bennük található információk integritásának és rendelkezésre állásának a védelmében.

A Bizottság által alkalmazott információtechnológiai biztonsági politika a következő elemeket tartalmazza:

– az általános biztonság szerves részét képezi és kiegészíti az adatbiztonság, a személyzeti biztonság és a fizikai biztonság valamennyi elemét,

– a hatáskörök megosztása a technikai rendszerek tulajdonosai, a technikai rendszerekben kezelt vagy tárolt EU minősített információk tulajdonosai, az információtechnológiai biztonsági szakemberek és felhasználók között,

– az egyes IT-rendszerek biztonsági elveinek és követelményeinek a leírása,

– ezeknek az elveknek és követelményeknek a jóváhagyása a kijelölt hatóság által,

– az IT-terület sajátos fenyegetettségének és gyenge pontjainak figyelembevétele.

25.1.2. *A rendszerekkel szembeni fenyegetések és a rendszerek sebezhetősége*

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 határozható meg, amely megkönnyíti vagy lehetővé teszi a konkrét fenyegetés létrejöttét egy meghatározott tárggyal vagy céllal szemben.

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.

25.1.3. *A biztonsági intézkedések fő célja*

Az e szakaszban megállapított biztonsági intézkedések főként arra irányulnak, hogy védelmet nyújtsanak az EU minősített információk engedély nélküli kiszolgáltatásával (a titkosság elvesztésével), valamint az információk integritásának és rendelkezésre állásának elvesztésével szemben. Az EU minősített információkat kezelő rendszerek megfelelő biztonsági védelmének megvalósítása érdekében a Bizottság Biztonsági Hivatala – az egyes rendszerekre külön kidolgozott megfelelő biztonsági eljárások és technikák mellett – megállapítja a hagyományos biztonság vonatkozó szabályait.

25.1.4. *A rendszerspecifikus biztonsági követelmények megállapítása (SSRS)*

Az EU BIZALMAS és annál magasabb minősítésű információkat kezelő valamennyi rendszer esetében előírás, hogy a technikai rendszer tulajdonosa (TSO, lásd a 25.3.4. szakaszt) és az információ tulajdonosa (lásd a 25.3.5. szakaszt) elkészítse a rendszerspecifikus biztonsági követelmények megállapítását (SSRS), adott esetben a projekt személyzetének és a Bizottság Biztonsági Hivatalának (mint INFOSEC-hatóságnak – IA, lásd a 25.3.3. szakaszt) a részvételével és támogatásával, amelyet a biztonsági akkreditációs hatóság (SAA, lásd a 25.3.2. szakaszt) hagy jóvá.

Az SSRS-re akkor is szükség van, ha a biztonsági akkreditációs hatóság (SAA) az EU KORLÁTOZOTT vagy a nem minősített információk rendelkezésre állását vagy integritását elengedhetetlennek ítéli.

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.

25.1.5. *Biztonsági üzemmódok*

Az EU BIZALMAS 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.

25.2. **Fogalommeghatározások**

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 rendszer-erőforrások 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;

c) biztonsági üzemeltetési eljárások (SecOPs) a javasolt műveletek (például biztosítandó üzemmódok, szolgáltatások) részletes leírásával, 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.

A „központi informatikai biztonsági tisztviselő” (CISO) valamely központi IT-szolgálatnál azt a tisztviselőt jelenti, aki a központilag szervezett rendszereknél a biztonsági intézkedéseket összehangolja és felügyeli.

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.

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:

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.

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.

A „számítógépes biztonsági termék” olyan általános számítógépes biztonsági terméket jelent, amelyet egy IT-rendszerbe kívánnak beilleszteni azért, hogy ott fokozza, illetve biztosítsa a kezelt információk titkosságát, integritását vagy rendelkezésre állását.

A „KIZÁRÓLAGOS biztonsági üzemmód” olyan üzemmódot jelent, amelyben a rendszerhez hozzáférő MINDEN személy a rendszeren belül kezelt információk legmagasabb minősítési szintjének megfelelő biztonsági felhatalmazással rendelkezik, és minden személynek közösen szükséges ismernie a rendszeren belül 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 (például fizikai, személyzeti és eljárási) tulajdonságnak meg kell felelnie a rendszerben kezelt információk legmagasabb minősítési szintje és minden kategóriamegjelölése követelményeinek.

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.

Az „információ tulajdonosa” (IO) azt a hatóságot (szervezeti egység vezetőjét) jelenti, amelynek hatáskörébe tartozik az információk létrehozása, kezelése és felhasználása, beleértve annak eldöntését is, hogy ki kapjon engedélyt az ezen információkhoz való hozzáférésre.

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 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.

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.

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.

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.

Az „IT-hálózatbiztonsági tulajdonságok” a hálózatot alkotó egyes IT-rendszerek IT-rendszerbiztonsági 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.

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 TSO ellenőrzése alá tartozó elemek együtteseként határozhatók meg.

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

Az „IT-rendszerbiztonsági 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.

A „helyi informatikai biztonsági tisztviselő" (LISO) a Bizottság valamely szervezeti egységénél azt a tisztviselőt jelenti, aki a saját területén belül a biztonsági intézkedések összehangolásáért és felügyeletéért felel.

A „többszintű biztonsági üzemmód" olyan üzemmódot jelent, amelyben a rendszerhez hozzáféréssel rendelkező személyek közül NEM MINDENKI rendelkezik biztonsági felhatalmazással a rendszerben kezelt információk legmagasabb minősítési szintjéig, és amelyben a rendszerhez hozzáféréssel rendelkező személyek közül NEM MINDENKINEK 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.

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.

A „biztonsági üzemeltetési eljárások" a technikai rendszerek tulajdonosa által kialakított eljárásokat jelentik, amelyek meghatározzák a biztonsági ügyekben alkalmazandó elveket, a betartandó üzemeltetési eljárásokat és a személyzet hatáskörét.

A „DOMINÁNS biztonsági üzemmód" olyan üzemmódot jelent, amelyben a rendszerhez hozzáféréssel rendelkező MINDEN személy biztonsági felhatalmazással rendelkezik a rendszerben kezelt információk legmagasabb minősítési szintjéig, ugyanakkor az ilyen hozzáféréssel bíró személyek közül NEM MINDENKINEK 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 eljárási) 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.

A „rendszerspecifikus biztonsági követelmények megállapítása" (SSRS) a betartandó biztonsági elvek és a betartandó részletes biztonsági követelmények teljes és részletes meghatározása. A Bizottság 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 a 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.

A „technikai rendszerek tulajdonosa” (TSO) azt a hatóságot jelenti, amely valamely rendszer létrehozásáért, karbantartásáért, üzemeltetéséért és leállításáért felel.

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.

25.3. **Hatáskörök a biztonság terén**

25.3.1. *Általános ismertetés*

A Bizottság biztonsági politikai tanácsadó csoportjának a 12. szakaszban meghatározott tanácsadói feladatköre magában foglalja az INFOSEC-kérdéseket is. E csoportnak olyan módon kell megszerveznie tevékenységét, hogy a fenti kérdésekben szakértői tanácsot tudjon adni.

A Bizottság Biztonsági Hivatala felel a részletes INFOSEC-rendelkezések kiadásáért, amelyek alapját az ebben a fejezetben foglalt rendelkezések képezik.

A biztonsággal kapcsolatos problémák (váratlan események, a szabályok megsértése stb.) esetében a Bizottság Biztonsági Hivatala haladéktalanul intézkedik.

A Bizottság Biztonsági Hivatala INFOSEC-egységgel rendelkezik.

25.3.2. *A biztonsági akkreditációs hatóság (SAA)*

A Bizottság Biztonsági Hivatalának vezetője egyben a Bizottság biztonsági akkreditációs hatósága (SAA) is. Az SAA felel az általános biztonság területéért, illetve az INFOSEC speciális területeiért, azaz a kommunikációs biztonságért, a kriptográfiai biztonságért és a TEMPEST-biztonságért.

Az SAA felel annak biztosításáért, hogy a rendszerek megfeleljenek a Bizottság biztonsági politikájának. Egyik feladata az, hogy a rendszerek számára megadja a jóváhagyást EU minősített információk kezelésére a működési környezetükben meghatározott minősítési szintig.

A bizottsági SAA hatásköre kiterjed a Bizottság helyiségein belül működő valamennyi rendszerre. Ha egy rendszer különböző összetevői a bizottsági SAA és más SAA-k hatáskörébe tartoznak, akkor az érintett felek közös akkreditációs bizottságot jelölhetnek ki, amelynek koordinációját a bizottsági SAA biztosítja.

25.3.3. *Az INFOSEC-hatóság (IA)*

A Bizottság Biztonsági Hivatala INFOSEC-egységének vezetője egyben a Bizottság INFOSEC-hatósága. Az INFOSEC-hatóság a következőkért felel:

– technikai tanácsadás és támogatás nyújtása az SAA számára,

– részvétel az SSRS kidolgozásában,

– az SSRS felülvizsgálata annak érdekében, hogy összhangban legyen ezekkel a biztonsági szabályokkal, valamint az INFOSEC-politika és -architektúra dokumentumaival,

– adott esetben részvétel az akkreditációs testületekben/bizottságokban, és az akkreditációval kapcsolatban 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.

25.3.4. *A technikai rendszerek tulajdonosa (TSO)*

Valamely rendszer speciális biztonsági tulajdonságainak megvalósításáért és ellenőrzéséért az adott rendszer tulajdonosa, a technikai rendszer tulajdonosa (TSO) felel. A központilag irányított rendszerek esetében központi informatikai biztonsági tisztviselőt (CISO) kell kinevezni. Szükség esetén az egyes szervezeti egységek helyi informatikai biztonsági tisztviselőt (LISO) is kineveznek. A TSO hatásköre kiterjed a biztonsági üzemeltetési eljárások (SecOPs) kialakítására és a rendszer egész életciklusára, a projekt megtervezésének szakaszától a rendszer végleges ártalmatlanításáig.

A TSO határozza meg azokat a biztonsági normákat és eljárásokat, amelyeket a rendszer szállítóinak be kell tartaniuk.

A TSO adott esetben hatáskörének egy részét a helyi informatikai biztonsági tisztviselőre ruházhatja át. Egy személy különböző INFOSEC-feladatokat is elláthat.

25.3.5. *Az információk tulajdonosa (IO)*

Az információk tulajdonosa (IO) felel az EU minősített információkért (és más olyan információkért), amelyeket technikai rendszerekbe visznek be, ott kezelnek, illetve előállítanak. Meghatározza, hogy a rendszerekben tárolt ezen információkhoz milyen feltételekkel lehet hozzáférni. Ezt a feladatot saját területén az információmenedzserre vagy az adatbázis-kezelőre ruházhatja át.

25.3.6. *Felhasználók*

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

25.3.7. *INFOSEC-képzés*

INFOSEC-képzést és -oktatást kell biztosítani a személyi állomány minden olyan tagjának, akinek erre szüksége van.

25.4. **Nem technikai jellegű biztonsági intézkedések**

25.4.1. *Személyzeti biztonság*

A rendszer felhasználóinak az adott rendszeren belül 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 bizottsági eljárásoknak megfelelően megadott felhatalmazás szükséges.

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.

A RENDSZEREK meghatározása és tervezése úgy történik, hogy megkönnyítse a hatáskörök és a feladatok szétosztását a személyi állomány körében oly módon, hogy egy személyben teljeskörűen senki ne ismerhesse meg vagy ellenőrizhesse a kulcsfontosságú rendszerbiztonsági pontokat.

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 rendszer biztonsági beállításait csak legalább két, egymással együttműködő felhatalmazott személy változtathatja meg.

25.4.2. *Fizikai biztonság*

Szükség szerint EU I. osztályba tartozó vagy II. osztályba tartozó biztonsági területként kerülnek meghatározásra azok az IT-területek és távoli terminál/munkaállomás területek (a 25.2. szakaszban meghatározottak szerint), ahol információtechnológiai eszközök igénybevételével EU BIZALMAS és annál magasabb minősítésű információkat kezelnek, vagy ahol az ilyen információkhoz való hozzáférés lehetséges.

25.4.3. *A rendszerhez való hozzáférés ellenőrzése*

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

Ha a hozzáférés ellenőrzésére szolgáló információkat és anyagokat e célra a továbbiakban nem használják fel, akkor azokat a 25.5.4. szakasz rendelkezéseinek megfelelően meg kell semmisíteni.

25.5. **Technikai jellegű biztonsági intézkedések**

25.5.1. *Az információk biztonsága*

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.

A Bizottság szervezeti egységeinek 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.

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.

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.

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

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 az SAA által jóváhagyott eljárásnak megfelelően (lásd a 25.5.4. szakaszt) minősítését meg nem szüntetik vagy meg nem semmisítik.

25.5.2. *Az információk ellenőrzése és az azokkal való elszámolás kötelezettsége*

Az EU TITKOS és az annál magasabb minősítésű információkhoz történő hozzáférésről automatikus eseménynapló (audit trails) készül vagy azt kézzel vezetett naplóban kell nyilvántartani. E nyilvántartások megőrzése ezeknek a biztonsági szabályoknak megfelelően történik.

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.

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 és naplózására az SAA jóváhagyásával kialakított eljárások szolgálnak. Az EU TITKOS és az annál magasabb minősítésű anyagok esetében ezek az eljárások meghatározott utasításokat tartalmaznak az információkkal való elszámolás kötelezettségére vonatkozóan.

25.5.3. *Az eltávolítható számítógépes adathordozók kezelése és ellenőrzése*

Minden EU BIZALMAS 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.

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 szabályoknak megfelelően történjék.

25.5.4. *A számítógépes adathordozók minősítésének megszüntetése és az ilyen adathordozók megsemmisítése*

Az EU minősített információk rögzítésére szolgáló számítógépes adathordozókat az SAA által jóváhagyott eljárásnak megfelelően lehet visszaminősíteni vagy minősítésüket megszüntetni.

Nem lehet minősítésüket megszüntetni vagy újból felhasználni azokat a számítógépes adathordozókat, amelyeken korábban EU SZIGORÚAN TITKOS minősítésű vagy különleges kategóriájú információkat tároltak.

Ha egy számítógépes adathordozó minősítését nem lehet megszüntetni, illetve az nem használható fel újra, akkor azt a fent említett eljárásnak megfelelően meg kell semmisíteni.

25.5.5. *Kommunikációs biztonság*

A Bizottság Biztonsági Hivatalának vezetője a kriptográfiai hatóság.

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.

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

Továbbítás során az EU TITKOS és az annál magasabb minősítésű információk titkosságát a Bizottság biztonsági ügyekért felelős tagja által a Bizottság biztonsági politikai tanácsadó csoportjával folytatott konzultációt követően jóváhagyott kriptográfiai módszerekkel vagy termékekkel kell védeni. Továbbítás során az EU BIZALMAS vagy az EU KORLÁTOZOTT információk titkosságát a Bizottság kriptográfiai hatósága által a Bizottság biztonsági politikai tanácsadó csoportjával folytatott konzultációt követően jóváhagyott kriptográfiai módszerek vagy termékek igénybevételével kell védeni.

Az EU minősített információk továbbítására alkalmazandó részletes szabályokat a Bizottság Biztonsági Hivatala által, a Bizottság biztonsági politikai tanácsadó csoportjával folytatott konzultációt követően jóváhagyott különleges biztonsági utasítások rögzítik.

Kivételes működési körülmények között az EU KORLÁTOZOTT, az EU BIZALMAS és az EU TITKOS minősítésű információk rejtjelezés nélkül is továbbíthatók, feltéve hogy ezt az információk tulajdonosa minden egyes esetben kifejezetten engedélyezi és szabályszerűen nyilvántartásba veszi. 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.

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 termináljukon kategorikusan megtagadják a hozzáférést az EU minősített információkhoz.

25.5.6. *Telepítési és kisugárzási biztonság*

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.

Az EU BIZALMAS és az annál magasabb minősítésű információkat kezelő rendszerek olyan védelemben részesülnek, hogy biztonságukat ne fenyegethesse kompromittáló kisugárzás és/vagy konduktivitás, amelynek tanulmányozása és ellenőrzése a „TEMPEST” elnevezést kapta.

A TEMPEST-ellenintézkedéseket a TEMPEST-hatóság vizsgálja felül és hagyja jóvá (lásd a 25.3.2. szakaszt).

25.6. **Biztonság a kezelés során**

25.6.1. *Biztonsági üzemeltetési eljárások (SecOPs)*

A biztonsági üzemeltetési eljárások (SecOPs) határozzák meg a biztonsági ügyekben elfogadásra kerülő elveket, a követendő üzemeltetési eljárásokat és a személyzet hatáskörét. A SecOPs eljárások kidolgozásáért a technikai rendszerek tulajdonosa (TSO) felel.

25.6.2. *Szoftvervédelem és konfigurációkezelés*

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.

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

25.6.3. *Kártékony szoftverek és számítógépes vírusok kiszűrése*

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

A Bizottsághoz beérkező számítógépes adathordozókat csak azután lehet bármely RENDSZERBE bevinni, hogy a kártékony szoftverek vagy számítógépes vírusok kiszűrését szolgáló ellenőrzés megtörtént.

25.6.4. *Karbantartás*

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.

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.

25.7. **Beszerzés**

25.7.1. *Általános ismertetés*

Bármely biztonsági termék csak akkor használható a beszerzendő rendszerrel együtt, ha valamelyik EU-tagállam megfelelő értékelő vagy tanúsító szerve által nemzetközileg elismert kritériumok (mint például az Információtechnológia Biztonsági Értékelésének Közös Kritériumai, lásd ISO 15408) szerint végzett értékelésére és tanúsítására már sor került vagy az folyamatban van. Az ACPC-jóváhagyás megadásához különleges eljárás szükséges.

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.

25.7.2. *Akkreditáció*

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 Bizottságot és valamely más szervezetet, akkor a Bizottság és az érintett biztonsági hatóságok közös egyetértéssel állapodnak meg az akkreditációról.

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

25.7.3. *Értékelés és tanúsítás*

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.

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

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

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

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.

25.7.4. *A biztonsági tulajdonságok rendszeres ellenőrzése az akkreditáció fenntartása érdekében*

A TSO állapítja meg azokat a rendszeres ellenőrzési eljárásokat, amelyek biztosítják, hogy a rendszer valamennyi biztonsági tulajdonsága mindig fennálljon.

Az SSRS-ben világosan meg kell határozni és körül kell írni a változtatásoknak azokat a fajtáit, amelyek ismételt akkreditációt vonnának maguk után, illetve amelyekhez az SAA előzetes jóváhagyása szükséges. Olyan jellegű módosítás, javítás vagy üzemzavar után, amely kihatással lehetett a rendszer biztonsági tulajdonságaira, a TSO gondoskodik annak az ellenőrzésnek a végrehajtásáról, amellyel megállapítható a biztonsági tulajdonságok megfelelő működése. A rendszer akkreditációjának fennmaradása rendszerint az ellenőrzések kielégítő eredményétől függ.

Az SAA rendszeresen ellenőrzi vagy felülvizsgálja mindazokat a rendszereket, amelyekben biztonsági tulajdonságokat hoztak létre. Az EU SZIGORÚAN TITKOS minősítésű információkat kezelő rendszerek tekintetében az ellenőrzéseket évente legalább egyszer el végezni.

25.8. **Ideiglenes vagy alkalomszerű felhasználás**

25.8.1. *Mikroszámítógépek és személyi számítógépek biztonsága*

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.

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).

25.8.2. *Magántulajdonban lévő IT-berendezések felhasználása hivatalos bizottsági munkára*

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

A Bizottság Biztonsági Hivatala vezetőjének írásbeli engedélye nélkül magántulajdonban lévő hardvert, szoftvert és adathordozót nem lehet olyan I. vagy II. osztályba tartozó területre bevinni, ahol EU minősített információkat kezelnek. Ilyen engedély kivételesen, csak technikai okok alapján adható.

25.8.3. *Szerződéses megbízott tulajdonában lévő vagy egy tagállam által biztosított IT-berendezések felhasználása hivatalos bizottsági munkára*

A szerződéses megbízott tulajdonában álló IT-berendezéseket és szoftvereket csak a Bizottság Biztonsági Hivatala vezetőjének engedélyével lehet hivatalos bizottsági munkára használni. A valamely tagállam által biztosított IT-berendezések és szoftverek használata is engedélyezhető. Ebben az esetben az IT-berendezést a Bizottság 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.

26. EU MINŐSÍTETT INFORMÁCIÓK ÁTADÁSA HARMADIK ÁLLAMOK VAGY NEMZETKÖZI SZERVEZETEK RÉSZÉRE

26.1.1. *Az EU minősített információk átadását szabályozó elvek*

A Bizottság mint testület az alábbiak alapján határoz EU minősített információk átadásáról harmadik állam vagy nemzetközi szervezet részére:

– 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.

Ezeket a határozatokat eseti alapon hozzák az alábbiaktól függően:

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

– az irántuk 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 tekintetben a Bizottság biztonsági politikai tanácsadó csoportja ad szakvéleményt a Bizottság számára.

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 Bizottság által előírt védelmet.

26.1.2. *Szintek*

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

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.

Az együttműködés egyes szintjei határozzák meg az eljárásokat és a biztonsági rendelkezéseket, amelyeket a 3., 4. és 5. függelék részletez.

26.1.3. *Biztonsági megállapodások*

Ha a Bizottság úgy határozott, hogy tartós vagy hosszú távú igény van minősített információk cseréjére közte és harmadik államok vagy más nemzetközi szervezetek között, akkor „minősített információk cseréjére vonatkozó biztonsági eljárásokról szóló megállapodást" dolgoz ki velük, meghatározva az együttműködés célját és a kicserélt információk védelmére vonatkozó kölcsönös szabályokat.

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 EU KORLÁTOZOTT lehet.

A biztonsági eljárásokról szóló megállapodások vagy egyetértési megállapodások tervezetét a Bizottság biztonsági politikai tanácsadó csoportja megvitatja, mielőtt azokat a Bizottsághoz határozathozatalra benyújtják.

A Bizottság biztonsági ügyekért felelős tagja a tagállamok nemzeti biztonsági hatóságaitól minden szükséges támogatást megkér annak biztosítása érdekében, hogy az átadandó információkat a biztonsági eljárásokról szóló megállapodásokban vagy a vonatkozó egyetértési megállapodásokban foglalt rendelkezéseknek megfelelően használják fel és részesítsék védelemben.

1. függelék

A NEMZETI BIZTONSÁGI MINŐSÍTÉSEK ÖSSZEHASONLÍTÓ TÁBLÁZATA

EU-minősítés	EU SZIGORÚAN TITKOS	EU TITKOS	EU BIZALMAS	EU KORLÁTOZOTT
NATO-minősítés (1)				
WEU-minősítés	Központi szigorúan titkos	WEU TITKOS	WEU BIZALMAS	WEU KORLÁTOZOTT
EURATOM-minősítés (2)	EURATOM szigorúan titkos	EURATOM titkos	EURATOM bizalmas	EURATOM korlátozott
Ausztria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgium	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Dánia	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Egyesült Királyság	Top Secret	Secret	Confidential	Restricted
Finnország	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Franciaország	Très Secret Défense (3)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Görögország	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Hollandia	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Írország	Top Secret	Secret	Confidential	Restricted
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Németország	STRENG GEHEIM	GEHEIM	VS (4) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUH
Olaszország	Segretissimo	Segreto	Riservatissimo	Riservato
Portugália	Muito secreto	Secreto	Confidencial	Reservado
Spanyolország	Secreto	Reservado	Confidencial	Difusión limitada
Svédország	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig

(1) NATO – a NATO minősítési szinteknek való megfelelést akkor állapítják meg, amikor a Bizottság és a NATO közötti biztonsági megállapodást tárgyalják.

(2) Az Euratom minősített információk védelméről szóló, 1958. július 31-i 3. Euratom rendelet.

(3) Franciaország: a „Très Secret Défense” minősítés, amely a kormányzati prioritásokra vonatkozik, csak a miniszterelnök jóváhagyásával változtatható meg.

(4) Németország: VS = Verschlusssache.

2. függelék

GYAKORLATI MINŐSÍTÉSI ÚTMUTATÓ

Ez az útmutató csak indikatív jellegű, és nem értelmezhető úgy, mint amely a 16., 17., 20. és 21. szakaszban megállapított lényegi rendelkezéseket módosítja.

Minősítés	Mikor	Ki	Jelölés	Visszaminősítés/a minősítés megszüntetése/megsemmisítés	
				Ki	Mikor
EU SZIGORÚAN TITKOS: 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 [16.1.].	Az EU SZIGORÚAN TITKOS minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg: – közvetlenül veszélyeztetné az EU vagy egyik tagállama vagy az egyik baráti ország belső stabilitását, – rendkívül súlyos kárt okozna a baráti kormányokkal fenntartott kapcsolatokban, – közvetlenül nagyszámú emberi élet elvesztéséhez vezetne, – rendkívül súlyosan károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességének fenntartását, – súlyos, hosszú távú kárt okozna az EU vagy a tagállamok gazdaságának.	Szabályszerűen felhatalmazott személyek (kibocsátók), főigazgatók, szolgálatvezetők [17.1.]. A kibocsátók határozzák meg az időpontot, határidőt vagy eseményt, amikortól vagy amelynek lejártát, illetve bekövetkezését követően a tartalmat vissza lehet minősíteni vagy a minősítést meg lehet szüntetni [16.2.]. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [17.3.].	Az EU SZIGORÚAN TITKOS minősítést az EU SZIGORÚAN TITKOS dokumentumokon – adott esetben biztonsági jelöléssel és/vagy az EBVP védelmi jelöléssel együtt –mechanikus eszközökkel és kézírással kell elhelyezni [16.4., 16.5., 16.3.]. Az EU minősítéseket és biztonsági azonosítókat minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Az egyes dokumentumokat hivatkozási számmal és keltezéssel kell ellátni; a hivatkozási számnak minden oldalon szerepelnie kell. 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 [21.1.].	A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [17.3.]. Az EU SZIGORÚAN TITKOS dokumentumokat a központi nyilvántartó hivatal vagy a dokumentumokért felelős alárendelt nyilvántartó hivatal semmisíti meg. Az egyes megsemmisített dokumentumokat megsemmisítési jegyzőkönyvben kell felsorolni, amelyet az EU SZIGORÚAN TITKOS ellenőrző tisztviselő és a megsemmisítésnél tanúként jelen lévő tisztviselő ír alá, aki EU SZIGORÚAN TITKOS biztonsági felhatalmazással rendelkezik. A szolgálati naplóba ilyen értelmű bejegyzést kell tenni. A nyilvántartó hivatalnak a megsemmisítési jegyzőkönyveket az elosztóívvel együtt tíz évig kell megőriznie [22.5.].	A fölösleges példányokat és szükségtelenné vált dokumentumokat meg kell semmisíteni [22.5.]. Az EU SZIGORÚAN TITKOS dokumentumokat, beleértve az dokumentumok készítése során keletkezett minősített hulladékokat, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat is, egy EU SZIGORÚAN TITKOS ellenőrző tisztviselő felügyelete mellett elégetéssel, bezúzással, feldarabolással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [22.5.].

Minősítés	Mikor	Ki	Jelölés	Visszaminősítés/a minősítés megszüntetése/megsemmisítés	
				Ki	Mikor
EU TITKOS: 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 [16.1.].	Az EU TITKOS minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg: – nemzetközi feszültségeket okozna, – súlyos kárt okozna a baráti kormányokkal fenntartott kapcsolatokban, – közvetlenül emberi életeket veszélyeztetne vagy súlyosan károsítaná a közrendet, az egyéni biztonságot vagy szabadságot, – súlyosan károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességének fenntartását, – jelentős anyagi kárt okozna az EU vagy egyik tagállama pénzügyi, monetáris, gazdasági és kereskedelmi érdekeinek.	Felhatalmazott személyek (kibocsátók), főigazgatók, szolgálatvezetők [17.1.]. A kibocsátók határozzák meg azt az időpontot vagy határidőt, amikortól vagy amelynek lejártát követően a tartalmat vissza lehet minősíteni vagy minősítését meg lehet szüntetni [16.2.]. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [17.3.].	Az EU TITKOS minősítést az EU TITKOS dokumentumokon – adott esetben biztonsági jelöléssel és/vagy az EBVP védelmi jelöléssel együtt – mechanikus eszközökkel és kézírással kell elhelyezni [16.4., 16.5., 16.3.]. Az EU minősítéseket és biztonsági azonosítókat minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Az egyes dokumentumokat hivatkozási számmal és keltezéssel kell ellátni; a hivatkozási számnak minden oldalon szerepelnie kell. 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 [21.1.].	A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [17.3.]. Az EU TITKOS dokumentumokat az értük felelős nyilvántartó hivatal semmisíti meg egy biztonsági felhatalmazással rendelkező személy felügyelete alatt. A megsemmisített EU TITKOS dokumentumokat fel kell tüntetni az aláírt megsemmisítési jegyzőkönyvben, amelyet a nyilvántartó hivatalnak az elosztóívekkel együtt legalább három évig meg kell őriznie [22.5.].	A fölösleges példányokat és szükségtelenné vált dokumentumokat meg kell semmisíteni [22.5.]. Az EU TITKOS dokumentumokat, beleértve az EU TITKOS dokumentumok elkészítése során keletkezett valamennyi minősített hulladékot, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat is, elégetéssel, bezúzással, felaprítással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [22.5.].

Minősítés	Mikor	Ki	Jelölés	Visszaminősítés/a minősítés megszüntetése/megsemmisítés	
				Ki	Mikor
EU BIZALMAS: 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 [16.1.].	Az EU BIZALMAS minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg: – jelentős kárt okozna a diplomáciai kapcsolatokban, azaz hivatalos tiltakozást vagy egyéb szankciókat váltana ki, – sértené az egyének biztonságát vagy szabadságát, – károsítaná a tagállamok vagy más partnerek fegyveres erőinek bevethetőségét vagy biztonságát, illetve a különösen fontos biztonsági vagy hírszerzési műveletek eredményességét, – lényegesen gyengítené jelentős szervezetek pénzügyi életképességét, – súlyos bűncselekmények nyomozását akadályozná vagy azok elkövetését megkönnyítené, – erősen ártana az EU vagy a tagállamok pénzügyi, monetáris, gazdasági és kereskedelmi érdekeinek, – komolyan hátráltatná az EU főbb politikáinak kidolgozását vagy működését, – az EU jelentős tevékenységeit állítaná le vagy azokban jelentős fennakadást okozna.	Felhatalmazott személyek (kibocsátók), főigazgatók, szolgálatvezetők [17.1.]. 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 [17.3.].	Az EU BIZALMAS minősítést az EU BIZALMAS dokumentumokon – adott esetben biztonsági jelöléssel és/vagy az EBVP védelmi jelöléssel együtt – mechanikus eszközökkel és kézírással vagy előre lebélyegzett, regisztrált papírra való nyomtatással kell elhelyezni [16.4., 16.5., 16.3.]. Az EU minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Az egyes dokumentumokat hivatkozási számmal és keltezéssel kell ellátni. Minden mellékletet és csatolmányt fel kell sorolni az első oldalon [21.1.].	A minősítés megszüntetése vagy a visszaminősítés kizárólag a kibocsátó feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [17.3.]. Az EU BIZALMAS dokumentumokat az értük felelős nyilvántartó hivatal semmisíti meg egy biztonsági felhatalmazással rendelkező személy felügyelete alatt. Megsemmisítésüket a nemzeti rendelkezéseknek megfelelően, illetve a Bizottság vagy az EU decentralizált szervei esetében az elnöktől kapott utasításoknak megfelelően kell nyilvántartani [22.5.].	A fölösleges példányokat és szükségtelenné vált dokumentumokat meg kell semmisíteni [22.5.]. Az EU BIZALMAS dokumentumokat, beleértve az EU BIZALMAS dokumentumok elkészítése során keletkezett valamennyi minősített hulladékot, például a rontott példányokat, piszkozatokat, gépelt jegyzeteket és indigópapírokat, elégetéssel, bezúzással, felaprítással vagy egyéb, azok tartalmát felismerhetetlenné és rekonstruálhatatlanná tevő módszerrel kell megsemmisíteni [22.5.]

Minősítés	Mikor	Ki	Jelölés	Visszaminősítés/a minősítés megszüntetése/megsemmisítés	
				Ki	Mikor
EU KORLÁTOZOTT: 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 [16.1.].	Az EU KORLÁTOZOTT minősítésű anyagok illetéktelen személyek tudomására jutása valószínűleg: – ártana a diplomáciai kapcsolatoknak, – magánszemélyeknek jelentős szenvedést okozna, – megnehezítené a tagállamok vagy más partnerek fegyveres erői bevethetőségének vagy biztonságának fenntartását, – magánszemélyek vagy vállalkozások számára pénzügyi veszteséget okozna, illetve jogosulatlan nyereséget vagy előnyt biztosítana, – megsértené a harmadik felek által átadott információk titkosságának megőrzésére tett saját kötelezettségvállalásokat, – megsértené az információk kiszolgáltatására vonatkozó törvényi korlátozásokat, – bűncselekmények nyomozását akadályozná vagy azok elkövetését megkönnyítené, – hátrányos helyzetbe hozná az EU-t vagy tagállamait a másokkal folytatott kereskedelmi vagy általános politikai tárgyalások során, – hátráltatná az EU politikáinak eredményes kidolgozását vagy működését, – veszélyeztetné az EU-nak és tevékenységeinek megfelelő igazgatását.	Felhatalmazott személyek (kibocsátók), főigazgatók, szolgálatvezetők [17.1.]. A kibocsátók határozzák meg azt az időpontot, határidőt vagy eseményt, amikortól vagy amelynek lejártát, illetve bekövetkezését követően a tartalmat vissza lehet minősíteni vagy minősítését meg lehet szüntetni [16.2.]. Egyébként a dokumentumokat legkésőbb ötévente felül kell vizsgálni annak megállapítása céljából, hogy az eredeti minősítés továbbra is szükséges-e [17.3.].	Az EU KORLÁTOZOTT minősítést az EU KORLÁTOZOTT dokumentumokon – adott esetben biztonsági jelöléssel és/vagy az EBVP védelmi jelöléssel együtt – mechanikus vagy elektronikus eszközökkel kell elhelyezni [16.4., 16.5., 16.3.]. Az EU minősítéseket minden oldal tetején és alján, középen kell feltüntetni és minden egyes oldalt meg kell számozni. Az egyes dokumentumokat hivatkozási számmal és keltezéssel kell ellátni [21.1.].	A minősítés megszüntetése kizárólag a kibocsátó feladata, aki a változásról tájékoztatja azokat a későbbi címzetteket, akik számára a dokumentumot vagy annak másolatát megküldte [17.3.]. Az EU KORLÁTOZOTT dokumentumokat az értük felelős nyilvántartó hivatal vagy a felhasználó semmisíti meg az elnöktől kapott utasításoknak megfelelően [22.5.].	A fölösleges példányokat és szükségtelenné vált dokumentumokat meg kell semmisíteni [22.5.].

3. függelék

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához: 1. szintű együttműködés

ELJÁRÁSOK

1. A Bizottságot mint testületet illeti meg az a hatáskör, 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 biztonsági megállapodás megkötéséig a Bizottság biztonsági ügyekért felelős tagja illetékes elbírálni az EU minősített információk átadására irányuló kérelmeket.
3. Ennek során:
   – kikéri az átadandó EU minősített információk kibocsátóinak 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 rendelkezéseknek megfelelő védelmét,
   – kikéri a Bizottság biztonsági politikai tanácsadó csoportjának véleményét arról, hogy mennyiben lehet megbízni a kedvezményezendő államokban vagy nemzetközi szervekben.
4. A Bizottság biztonsági ügyekért felelős tagja a kérelmet és a Bizottság biztonsági politikai tanácsadó csoportjának véleményét határozathozatalra a Bizottság elé terjeszti.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI RENDELKEZÉSEK

5. A Bizottság biztonsági ügyekért felelős tagja értesíti a kedvezményezett államokat vagy nemzetközi szervezeteket a Bizottságnak arról a határozatáról, amellyel engedélyezi az EU minősített információk átadását.

6. 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 ezeknek a rendelkezéseknek megfelelően, és különösen az alábbiakban rögzített különleges szabályoknak 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) Az EU BIZALMAS 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) Megállapodás útján határozzák meg a dokumentumok továbbításának gyakorlati eljárását. E megállapodás megkötéséig a 21. szakasz rendelkezéseit kell alkalmazni. A megállapodás különösen azokat a nyilvántartó hivatalokat határozza meg, ahová az EU minősített információkat továbbítani kell.
   b) Ha a Bizottság által átadásra engedélyezett minősített információk EU SZIGORÚAN TITKOS anyagot is tartalmaznak, a kedvezményezett állam vagy nemzetközi szervezet központi EU nyilvántartó hivatalt és, ha szükséges, EU alárendelt nyilvántartó hivatalokat hoz létre. Ezekre a nyilvántartó hivatalokra a 22. szakaszban található biztonsági rendelkezések az irányadók.

9. Bejegyzés

   Amint valamely nyilvántartó hivatal EU BIZALMAS 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 ezen biztonsági rendelkezések 22. szakaszában rögzített utasításoknak megfelelően semmisítik meg. Az EU TITKOS és az EU SZIGORÚAN TITKOS 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**

EU BIZALMAS vagy EU TITKOS 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.

EU SZIGORÚAN TITKOS dokumentum sokszorosítását vagy fordítását csak a kibocsátó hatóság engedélyezheti, amely meghatározza a másolatok engedélyezett számát. Ha a kibocsátó hatóság kiléte nem határozható meg, a kérelmet a Bizottság 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) értesíteni kell a Bizottság Biztonsági Hivatalát, a megfelelő 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 a 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 Bizottság Biztonsági Hivatala által ajánlott intézkedéseket.

14. Ellenőrzések

Az érintett államokkal vagy nemzetközi szervezetekkel egyetértésben a Bizottság 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 ezeket a biztonsági rendelkezéseket betartották.

4. függelék

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához: 2. szintű együttműködés

ELJÁRÁSOK

1. A kibocsátó hatóság 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. A Bizottságot mint testületet illeti meg az a hatáskör, hogy a Bizottságon belül készített EU minősített információk átadását engedélyezze.
2. Az átadás főszabály szerint az EU TITKOS vagy annál alacsonyabb minősítésű információkra korlátozódik. A különleges biztonsági azonosítókkal vagy jelölésekkel védett minősített információk e körből ki vannak zárva.
3. A biztonsági megállapodás megkötéséig a Bizottság biztonsági ügyekért felelős tagja illetékes elbírálni az EU minősített információk átadására irányuló kérelmeket.
4. Ennek során:
   - kikéri az átadandó EU minősített információk kibocsátóinak 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,
   - intézkedik a Bizottság biztonsági politikai tanácsadó csoportja ülésének összehívásáról, vagy ha szükséges, egyszerűsített írásbeli eljárás keretében érdeklődik a tagállamok nemzeti biztonsági hatóságainál azért, hogy megszerezze a Bizottság biztonsági politikai tanácsadó csoportjának véleményét.
5. A Bizottság biztonsági politikai tanácsadó csoportja véleményében a következő 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,
   - visszaminősítés vagy a minősítés megszüntetése, mielőtt az információt átadják a kedvezményezett országok vagy nemzetközi szervezetek számára.
6. A Bizottság biztonsági ügyekért felelős tagja a kérelmet és a Bizottság biztonsági politikai tanácsadó csoportjának véleményét határozathozatalra a Bizottság elé terjeszti.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI SZABÁLYOK

7. A Bizottság biztonsági ügyekért felelős tagja értesíti a kedvezményezett államokat vagy nemzetközi szervezeteket a Bizottság határozatáról, amellyel engedélyezi az EU minősített információk átadását, továbbá az abban foglalt korlátozásokról.

8. 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 a Bizottság által megállapított szabályoknak megfelelően védik.

9. A következő védelmi szabályokat kell alkalmazni, hacsak a Bizottság – a Bizottság biztonsági politikai tanácsadó csoportjának technikai véleménye birtokában – úgy nem határoz, hogy különleges eljárást alkalmaz az EU minősített dokumentumok kezelésére (EU-minősítés, különleges jelölések stb. törlése).

10. 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) A Bizottság által átadott minősített információkhoz való 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 felhatalmazással kell rendelkeznie.
    c) Ezeket a nemzetbiztonsági tanúsítványokat vagy felhatalmazásokat az elnök számára tájékoztatásul továbbítják.

11. A dokumentumok továbbítása

Megállapodás útján határozzák meg a dokumentumok továbbításának gyakorlati eljárását. E megállapodás megkötéséig a 21. szakasz rendelkezéseit kell alkalmazni. A megállapodás különösen azokat a nyilvántartó hivatalokat határozza meg, ahová az EU minősített információkat továbbítani kell, valamint azokat a pontos címeket, ahová a dokumentumokat továbbítják, továbbá az EU minősített információk továbbításánál igénybe veendő futár- vagy postai szolgálatokat.

12. **Bejegyzés beérkezéskor**

A címzett állam nemzeti biztonsági hatósága vagy az annak megfelelő állami szerv, amely kormánya nevében a Bizottság által továbbított minősített információkat átveszi, illetve a címzett 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 számára, amikor a dokumentumot visszajuttatják az EU számára vagy megsemmisítik azt.

13. A dokumentumok visszajuttatása

Amikor az átvevő a Bizottság számára minősített dokumentumot juttat vissza, a fenti „A dokumentumok továbbítása" pontban jelzett módon kell eljárnia.

14. Védelem

a) Amikor a dokumentumokat nem használják a nemzetileg azonos szintűként minősített anyagok tárolására jóváhagyott biztonsági tárolóeszközökben kell elhelyezni őket. A tárolóeszközön nem szerepelhet a tartalmára vonatkozó jelzés, és 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) EU BIZALMAS vagy az annál magasabb minősítésű dokumentumokról nem lehet fénymásolatot, illetve e dokumentumokból kivonatokat készíteni a Bizottság Biztonsági Hivatalának engedélye nélkül.

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

15. 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.

16. A biztonság megsértése

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 Bizottság Biztonsági Hivatalának vagy a dokumentumok átadását kezdeményező tagállam nemzeti biztonsági hatóságának (ennek másolatát meg kell küldeni a Bizottság 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.

17. Ellenőrzések

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

18. 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 ezeket a biztonsági rendelkezéseket betartották.

5. függelék

Iránymutatások az EU minősített információk harmadik államok vagy nemzetközi szervezetek számára való átadásához: 3. szintű együttműködés

ELJÁRÁSOK

1. Esetenként előfordulhat, hogy a Bizottság bizonyos különleges körülmények között együtt kíván működni olyan államokkal vagy szervezetekkel, amelyek nem tudják megadni az e biztonsági szabályokban előírt biztosítékokat, de az együttműködés érdekében mégis szükségessé válhat EU minősített információk átadása.

2. A kibocsátót illeti meg az a hatáskör, 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. A Bizottságot mint testületet illeti meg az a hatáskör, hogy a Bizottságon belül készített EU minősített információk átadását engedélyezze.

   Az átadás főszabály szerint az EU TITKOS vagy annál alacsonyabb minősítésű információkra korlátozódik. Nem foglalja magában a különleges biztonsági azonosítókkal vagy jelölésekkel védett minősített információkat.

3. A Bizottság mérlegeli a minősített információk átadásának célszerűségét, értékeli, hogy a kedvezményezetteknek mennyiben szükséges azokat ismerniük, és meghatározza a közölhető minősített információk természetét.

4. Ha a Bizottság az átadást támogatja, a Bizottság biztonsági ügyekért felelős tagja:

   – kikéri az átadandó EU minősített információk kibocsátóinak véleményét,

   – intézkedik a Bizottság biztonsági politikai tanácsadó csoportja ülésének összehívásáról, vagy ha szükséges, egyszerűsített írásbeli eljárás keretében érdeklődik a tagállamok nemzeti biztonsági hatóságainál azzal a céllal, hogy megszerezze a Bizottság biztonsági politikai tanácsadó csoportjának véleményét.

5. A Bizottság biztonsági politikai tanácsadó csoportja véleményében a következő szempontokra tér ki:

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

   b) az átadható információk minősítési szintje;

   c) visszaminősítés vagy a minősítés megszüntetése az információk átadása előtt;

   d) az átadandó dokumentumok kezelésére irányuló eljárások (lásd az alábbi bekezdést);

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

6. 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 Bizottság biztonsági politikai tanácsadó csoportja 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.

7. Az elnök a Bizottság biztonsági politikai tanácsadó csoportjának véleményét határozathozatalra a Bizottsághoz továbbítja.

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

9. A Bizottság biztonsági ügyekért felelős tagja tájékoztatja a tagállamokat az információk természetéről és minősítéséről, felsorolva azokat a szervezeteket és országokat, amelyek számára azok a Bizottság határozatának megfelelően átadhatók.

10. A Bizottság Biztonsági Hivatala megtesz minden szükséges intézkedést annak érdekében, hogy a megkönnyítse az esetleges későbbi károk felmérését és az eljárások felülvizsgálatát.

    Ha az együttműködés feltételei megváltoznak, a Bizottság újból foglalkozik a kérdéssel.

A KEDVEZMÉNYEZETTEK ÁLTAL ALKALMAZANDÓ BIZTONSÁGI RENDELKEZÉSEK

11. A Bizottság biztonsági ügyekért felelős tagja értesíti a kedvezményezett államokat vagy nemzetközi szervezeteket a Bizottság határozatáról, amellyel engedélyezi az EU minősített információk átadását, valamint a Bizottság biztonsági politikai tanácsadó csoportja által javasolt és a Bizottság által jóváhagyott részletes védelmi szabályokról.

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

– az információkat csak a Bizottság által meghatározott együttműködés céljára használják fel,

– az információk számára biztosítják a Bizottság által előírt védelmet.

13. A dokumentumok továbbítása

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

b) Az EU BIZALMAS és az 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.

14. Bejegyzés beérkezéskor

A címzett állam nemzeti biztonsági hatósága vagy az annak megfelelő állami szerv, amely kormánya nevében a Bizottság 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 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.

15. A kicserélt minősített információk felhasználása és védelme

a) Az EU TITKOS 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. Az EU TITKOS minősítésű információkat diplomáciai futárcsomagban, biztonságos postaszolgálat vagy biztonságos távközlési eszközök útján továbbítják. Az EU TITKOS dokumentum csak a kibocsátó hatóság írásbeli beleegyezése alapján másolható. Minden másolatot nyilván kell tartani és ellenőrzés alatt kell tartani. Az EU TITKOS dokumentumokra vonatkozó valamennyi művelet esetében átvételi elismervényt kell kiállítani.

b) Az EU BIZALMAS 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.

Az EU BIZALMAS minősítésű információkat diplomáciai futárcsomagban, katonai postaszolgálat vagy biztonságos távközlési eszközök útján kell továbbítani. Az átvevő szerv másolatokat készíthet, azok számát és elosztását különleges nyilvántartásokba kell bejegyezni.

c) Az EU KORLÁTOZOTT 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.

16. Megsemmisítés

A szükségtelenné vált dokumentumokat meg kell semmisíteni. EU KORLÁTOZOTT és EU BIZALMAS minősítésű dokumentumok esetében megfelelő bejegyzést vezetnek be a különleges nyilvántartásokba. EU TITKOS dokumentumok esetében megsemmisítési jegyzőkönyvet kell felvenni, amelyet a megsemmisítésnél tanúként jelen lévő két személynek kell aláírnia.

17. A biztonság megsértése

Ha az EU BIZALMAS vagy EU TITKOS minősítésű információkkal kapcsolatos biztonságot megsértették vagy ennek gyanúja merül fel, az állam nemzeti biztonsági hatósága vagy a szervezet biztonsági vezetője köteles ennek körülményeit kivizsgálni. Az eredményről értesítik a Bizottság Biztonsági Hivatalát. Meg kell tenni a szükséges intézkedéseket a nem megfelelő eljárások vagy tárolási módszerek korrigálása érdekében, ha ezek vezettek a biztonság megsértéshez.

6. FÜGGELÉK

RÖVIDÍTÉSEK JEGYZÉKE

ACPC	Beszerzésekkel és szerződésekkel foglalkozó tanácsadó bizottság
CrA	Kriptográfiai hatóság
CISO	Központi informatikai biztonsági tisztviselő
COMPUSEC	Számítógépes biztonság
COMSEC	Kommunikációs biztonság
CSO	A Bizottság Biztonsági Hivatala
EBVP	Európai biztonsági és védelmi politika
EUCI	EU minősített információ
IA	INFOSEC-hatóság
INFOSEC	Információbiztonság
IO	Az információ tulajdonosa
ISO	Nemzetközi Szabványügyi Szervezet
IT	Információtechnológia
LISO	Helyi informatikai biztonsági tisztviselő
LSO	Helyi biztonsági tisztviselő
MSO	Az ülés biztonsági tisztviselője
NSA	Nemzeti biztonsági hatóság
PC	Személyi számítógép
RCO	A nyilvántartó hivatalt ellenőrző tisztviselő
SAA	Biztonsági akkreditációs hatóság
SecOPS	Biztonsági üzemeltetési eljárások
SSRS	Rendszerspecifikus biztonsági követelmények megállapítása
TA	TEMPEST-hatóság
TSO	A technikai rendszer tulajdonosa