A BIZOTTSÁG (EU, Euratom) 2018/559 HATÁROZATA

(2018. április 6.)

az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról szóló (EU, Euratom) 2017/46 határozat 6. cikkére vonatkozó végrehajtási szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 249. cikkére,

tekintettel az Európai Atomenergia-közösséget létrehozó szerződésre,

tekintettel az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról szóló, 2017. január 10-i (EU, Euratom) 2017/46 bizottsági határozatra ([1]) és különösen annak 6. cikkére,

mivel:

(1) Az (EU, Euratom) 2017/46 határozat elfogadásával szükség van arra, hogy a Bizottság felülvizsgálja, aktualizálja és egységesítse a Bizottság által használt kommunikációs és információs rendszerek biztonságáról szóló, hatályon kívül helyezett C(2006) 3602 bizottsági határozathoz kapcsolódó végrehajtási szabályokat.

(2) A Bizottság biztonságért felelős tagja – a belső eljárási szabályzat maradéktalan tiszteletben tartásával – felhatalmazást kapott a végrehajtási szabályok megállapítására, az (EU, Euratom) 2017/46 határozat ([2]) 13. cikkével összhangban.

(3) A C(2006) 3602 határozatban foglalt végrehajtási szabályokat ezért hatályon kívül kell helyezni,

ELFOGADTA EZT A HATÁROZATOT:

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy és hatály

(1) E határozat tárgyáról és hatályáról az (EU, Euratom) 2017/46 határozat 1. cikke rendelkezik.

(2) E határozat rendelkezései vonatkoznak minden kommunikációs és információs rendszerre (a továbbiakban: CIS). Az e határozatban meghatározott felelősségi területek azonban nem alkalmazandók az EU-minősített adatokat kezelő CIS-ekre. E rendszerek vonatkozó felelősségi területeit a rendszertulajdonos és a Bizottság Biztonsági Hatósága határozza meg az (EU, Euratom) 2015/444 bizottsági határozattal ([3]) összhangban.

(3) E határozat 2. fejezete áttekintést nyújt az informatikai biztonsággal kapcsolatos szervezés és feladatok gyakorlati végrehajtásáról. E határozat 3. fejezete áttekintést nyújt az (EU, Euratom) 2017/46 határozat 6. cikkével kapcsolatos eljárásokról.

2. cikk

Fogalommeghatározások

E határozat vonatkozásában az (EU, Euratom) 2017/46 határozat 2. cikkében foglalt meghatározások alkalmazandók. E határozat alkalmazásában az alábbi meghatározásokat kell még alkalmazni:

1. „kriptográfiai jóváhagyó hatóság (CAA)": a Bizottság Biztonsági Hatósága által betöltött funkció, amely a humánerőforrásügyi és biztonsági Főigazgató irányítása alá tartozik;

([1]) HL L 6., 2017.1.11., 40. o.
([2]) A Bizottság C(2017) 7428 final határozata (2017. november 8.) Európai Bizottság kommunikációs és információs rendszereinek biztonságával kapcsolatos végrehajtási szabályok, előírások és iránymutatások elfogadására adott felhatalmazásról.
([3]) A Bizottság (EU, Euratom) 2015/444 határozata (2015. március 13.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (HL L 72., 2015.3.17., 53. o.)

2. „külső hálózati kapcsolat”: a Bizottság belső hálózata és bármely más hálózat, köztük az internet közötti elektronikus hírközlési kapcsolat. E fogalommeghatározás nem terjed ki a harmadik fél olyan hálózatára, amelyet szerződés alapján biztosítanak a Bizottság belső hálózatának részeként.

3. „kulcs letétbe helyezése”: a kriptográfiai kulcsok másolatainak egy vagy több félnél történő tárolásának eljárása, amely biztosítja a feladatok elkülönítését, és lehetővé teszi a kulcsok lekérését abban az esetben, ha a műveleti másolat elveszett. A kulcsok két vagy több részre oszthatók, amelyek közül mindegyiket különböző félnél helyezik letétbe, annak biztosítása érdekében, hogy egyetlen fél se rendelkezzen a teljes kulccsal.

4. „RASCI”: a feladatkörök alábbi mutatók alapján történő kijelölésére utaló rövidítés:

   a) „felelős”: (Responsible) az elvárt eredmény elérése érdekében eljárni és döntéseket hozni köteles;

   b) „elszámoltatható”: (Accountable) tettekért, döntésekért és teljesítményért felelősségre vonható;

   c) „támogató”: (Supports) a feladat elvégzéséért felelős személlyel együttműködni köteles;

   d) „tanácsadó”: (Consulted) tanácsát vagy véleményét kérik;

   e) „tájékoztatott”: (Informed) naprakészen tájékoztatják a vonatkozó információkról.

2. FEJEZET

SZERVEZET ÉS FELADATKÖRÖK

3. cikk

Szerepek és feladatkörök

Az e határozat 4. és 8. cikkével kapcsolatos szerepeket és feladatköröket a RASCI modellnek megfelelően a melléklet határozza meg.

4. cikk

A Bizottság információbiztonsági politikájával való összhang

(1) A Humánerőforrásügyi és Biztonsági Főigazgatóság felülvizsgálja a Bizottság informatikai biztonsági politikáját, valamint a kapcsolódó standardokat és iránymutatásokat annak biztosítása érdekében, hogy azok összhangban legyenek a Bizottság általános biztonságpolitikájával, különösen az (EU, Euratom) 2015/443 bizottsági határozat ([1]) és az (EU, Euratom) 2015/444 határozat rendelkezéseivel.

(2) A Bizottság más szervezeti egységének kérésére a Humánerőforrásügyi és Biztonsági Főigazgatóság felülvizsgálhatja annak informatikai biztonsági politikáját vagy más informatikai biztonsági dokumentációját annak biztosítása érdekében, hogy az összhangban legyen a Bizottság információbiztonsági politikájával. Az érintett bizottsági szervezeti egység vezetője biztosítja, hogy a következetlenségeket megszüntetik.

(3) Az információbiztonsággal kapcsolatos feladatkörének megfelelően a Humánerőforrásügyi és Biztonsági Főigazgatóság együttműködik az Informatikai Főigazgatósággal annak biztosítása érdekében, hogy az informatikai biztonsági eljárások teljes mértékben figyelembe veszik az (EU, Euratom) 2015/443 határozatban és különösen annak 3. és 9. cikkében meghatározott minősítést és alapelveket.

3. FEJEZET

INFORMATIKAI BIZTONSÁGI ELJÁRÁSOK

5. cikk

Titkosítási technológiák

(1) A titkosítási technológiáknak az EU-minősített adatok védelmére való alkalmazása tekintetében eleget kell tenni az (EU, Euratom) 2015/444 határozatnak.

(2) A titkosítási technológiáknak a nem EU-minősített adatok védelmére való alkalmazásáról az egyes CIS-ek rendszertulajdonosai döntenek, figyelembe véve mind a titkosítás révén csökkentendő, mind pedig az általa jelentett kockázatokat.

(3) A kriptográfiai jóváhagyó hatóság előzetes jóváhagyására van szükség a titkosítási technológiák valamennyi alkalmazásához, kivéve, ha a titkosítást kizárólag a nem EU-minősített adatok bizalmas jellegének a továbbítás során történő védelmére használják és a titkosítás a standard hálózati kommunikációs protokollokat alkalmazza.

([1]) A Bizottság (EU, Euratom) 2015/443 határozata (2015. március 13.) a Bizottságon belüli biztonságról (HL L 72., 2015.3.17., 41. o.)

(4) Az e cikk (3) bekezdésében említett kivételek mellett a Bizottság szervezeti egységei biztosítják a visszafejtő kulcsok biztonsági másolatainak letéti őrzését a tárolt adatok lekérdezhetősége érdekében abban az esetben, ha a visszafejtő kulcs nem áll rendelkezésre. A titkosított adatoknak a visszafejtő kulcsok biztonsági másolatai alkalmazásával történő lekérdezésére csak akkor kerülhet sor, ha azt a kriptográfiai jóváhagyó hatóság által meghatározott előírásokkal összhangban engedélyezték.

(5) A titkosítási technológiák alkalmazása iránti kérelmeket hivatalosan dokumentálni kell, aminek ki kell terjednie a CIS-ekre és a védelmet igénylő adatok, az alkalmazandó technológia és a kapcsolódó biztonsági üzemeltetési eljárások részleteire. A jóváhagyás iránti kérelmet a rendszertulajdonos írja alá.

(6) A titkosítási technológiák alkalmazásának jóváhagyása iránti kérelmet a kriptográfiai jóváhagyó hatóság értékeli a közzétett standardoknak és követelményeknek megfelelően.

6. cikk

Informatikai biztonsági ellenőrzések

(1) A Humánerőforrásügyi és Biztonsági Főigazgatóság informatikai biztonsági ellenőrzéseket hajt végre, hogy megbizonyosodjon arról, hogy az informatikai biztonsági intézkedések megfelelnek-e a Bizottság informatikai biztonsági politikájának, és hogy megvizsgálja az ellenőrző intézkedések megbízhatóságát.

(2) A Humánerőforrásügyi és Biztonsági Főigazgatóság informatikai biztonsági ellenőrzést végezhet:

a) saját kezdeményezésére;

b) az információbiztonsági irányítóbizottság kérésére;

c) valamely rendszertulajdonos kérésére;

d) információbiztonsági incidenst követően; vagy

e) egy konkrét rendszert érintő magas kockázat azonosítását követően.

(3) Az adattulajdonosok informatikai biztonsági ellenőrzést kérhetnek, mielőtt az információikat egy CIS-nél tárolják.

(4) Az ellenőrzés eredményeit a rendszertulajdonos számára készített – a megállapításokat és a CIS informatikai biztonsági politikával való összhangja javítására vonatkozó ajánlásokat tartalmazó – hivatalos jelentésben kell dokumentálni, és annak másolatát meg kell küldeni helyi informatikai biztonsági tisztviselő számára. A Humánerőforrásügyi és Biztonsági Főigazgatóság a jelentős kérdésekről és ajánlásokról jelentést küld az információbiztonsági irányítóbizottságnak.

(5) A Humánerőforrásügyi és Biztonsági Főigazgatóság nyomon követi az ajánlások végrehajtását.

(6) Adott esetben az informatikai biztonsági ellenőrzések magukban foglalhatják a rendszertulajdonos számára biztosított szolgáltatások, helyszínek és berendezések ellenőrzését, egyaránt ideértve a belső és külső szolgáltatókat.

7. cikk

A külső hálózatokról való hozzáférés

(1) A Humánerőforrásügyi és Biztonsági Főigazgatóság ennek részletes szabályait a bizottsági kommunikációs és információs rendszerek és a külső hálózatok közötti hozzáférés engedélyezésére vonatkozó előírásban állapítja meg.

(2) A szabályoknak a külső hálózatokhoz való kapcsolódás különböző típusait kell megkülönböztetniük és a kapcsolódás minden egyes típusa esetében meg kell határozniuk a megfelelő biztonsági szabályokat, ideértve azt is, hogy szükséges-e a kapcsolódásnak az érintett hatóság általi előzetes engedélyezése, ahogy az e cikk (4) bekezdésében is szerepel.

(3) Szükség esetén az engedély hivatalos kérelmezési és engedélyezési eljárás alapján adható meg. Az engedély meghatározott időtartamra érvényes és azt a kapcsolat aktiválása előtt be kell szerezni.

(4) A Humánerőforrásügyi és Biztonsági Főigazgatóság viseli az általános felelősséget a kérelmek engedélyezéséért, azonban egyes kapcsolódási típusok esetében e hatáskörét saját döntése alapján átruházhatja, összhangban az (EU, Euratom) 2015/443 határozat 17. cikkének (3) bekezdésével, és a (8) bekezdésben meghatározott feltételek mellett.

(5) Az engedélyező szervezet további biztonsági követelményeket írhat elő az engedélyezés előfeltételeként, annak érdekében, hogy a Bizottság kommunikációs és információs rendszereit és hálózatait védje az adatokhoz való jogosulatlan hozzáférés vagy a biztonsági szabályok más megsértése kockázataival szemben.

(6) A Bizottság hálózati szolgáltatásait alapesetben az Informatikai Főigazgatóság nyújtja. Bármely olyan bizottsági szervezeti egységnek, amely nem az Informatikai Főigazgatóság által biztosított hálózatot üzemeltet, először be kell szereznie az információbiztonsági irányítóbizottság jóváhagyását. A Bizottság szervezeti egysége dokumentálja a kérelem üzleti indoklását és bizonyítja, hogy a hálózati ellenőrzések teljesítik a beérkező és kiáramló információk ellenőrzésével kapcsolatos követelményeket.

(7) A CIS rendszertulajdonosa meghatározza az CIS-hez való külső hozzáféréssel kapcsolatos biztonsági követelményeket, és – a helyi informatikai biztonsági tisztviselő támogatásával – biztosítja a CIS biztonságának védelmére irányuló megfelelő intézkedések végrehajtását.

(8) A belső hálózati kapcsolatok tekintetében végrehajtott biztonsági intézkedések a szükséges ismeret elvére és a legkisebb kiváltság elveire épülnek, amelyek biztosítják, hogy az egyének csak olyan információkat és hozzáférési jogosultságokat kapjanak, amelyek a Bizottságon belüli hivatali feladataik elvégzéséhez szükségesek.

(9) Valamennyi külső hálózati kapcsolatot szűrni kell és nyomon kell követni a biztonsági szabályok esetleges megsértésének felderítése érdekében.

(10) Amennyiben egy CIS kiszervezését lehetővé tevő kapcsolatokat hoznak létre, az engedély feltétele a 8. cikkben leírt eljárás sikeres lefolytatása.

8. cikk

A CIS-ek kiszervezése

(1) E határozat alkalmazásában egy CIS kiszervezettnek tekinthető, ha azt egy olyan harmadik személy vállalkozóval kötött szerződés alapján biztosítják, amely szerint a CIS nem a Bizottság létesítményeiben helyezkedik el. Mindez magában foglalja a Bizottság létesítményein kívüli, egyéni vagy több CIS-k vagy más informatikai szolgáltatások, adatközpontok kiszervezését, valamint a bizottsági adathalmazok külső szolgáltatók általi kezelését.

(2) Egy CIS kiszervezésekor figyelembe kell venni a kezelt információk érzékenységét vagy minősítését, az alábbiak szerint:

a) Az EU-minősített adatokat kezelő CIS-t az (EU, Euratom) 2015/444 határozattal összhangban kell akkreditálni, valamint előzetesen konzultálni kell a biztonsági akkreditációs hatósággal. Az EU-minősített adatokat kezelő rendszerek nem szervezhetők ki.

b) A nem EU-minősített adatokat kezelő CIS rendszertulajdonosa a vonatkozó jogi kötelezettségekkel vagy az információ érzékenységével arányos intézkedéseket tesz a biztonsági szükségletek kezelése érdekében, figyelembe véve a kiszervezéssel járó kockázatokat. A Humánerőforrásügyi és Biztonsági Főigazgatóság további követelményeket támaszthat.

c) A kiszervezett fejlesztési projekteknek figyelembe kell venniük a kifejlesztett kód és a fejlesztés során alkalmazott bármely tesztadat érzékenységét.

(3) A kiszervezett CIS-ekre az (EU, Euratom) 2017/46 határozat 3. cikkében meghatározottakon kívül az alábbi alapelvek alkalmazandók:

a) a kiszervezési megállapodásokat úgy kell kialakítani, hogy elkerüljék a konkrét szolgáltatóktól való függést;

b) a kiszervezés biztonságáról szóló megállapodásoknak minimalizálniuk kell annak lehetőségeit, hogy a harmadik fél alkalmazottai bizottsági információkhoz férjenek hozzá vagy módosítsák azokat;

c) a harmadig felek azon alkalmazottainak, akik hozzáféréssel rendelkeznek egy kiszervezett CIS-hez, titoktartási megállapodást kell bemutatniuk;

d) a CIS kiszervezését jelezni kell az CIS-ek leltárában.

(4) A rendszertulajdonos az adattulajdonos részvételével:

a) értékeli és dokumentálja a kiszervezéssel kapcsolatos kockázatokat;

b) meghatározza a vonatkozó biztonsági követelményeket;

c) konzultációt folytat valamennyi kapcsolódó CIS rendszertulajdonosaival annak biztosítása érdekében, hogy azok biztonsági követelményeit is beépítsék;

d) biztosítja, hogy a kiszervezési szerződés magában foglalja a megfelelő biztonsági követelményeket és jogokat;

e) teljesíti a részletes eljárásban foglalt minden egyéb követelményt, az e cikk (8) bekezdésében említettek szerint.

E lépéseket még az egy vagy több CIS kiszervezéséről szóló szerződés vagy más megállapodás aláírása előtt el kell végezni.

(5) A CIS élettartama során a rendszertulajdonosok kezelik a kiszervezéssel kapcsolatos kockázatokat annak érdekében, hogy teljesítsék a meghatározott biztonsági követelményeket.

(6) A rendszertulajdonosok biztosítják, hogy a harmadik személy vállalkozók kötelesek legyenek azonnal értesíteni a Bizottságot a kiszervezett bizottsági CIS-eket érintő valamennyi információbiztonsági incidensről.

(7) A rendszertulajdonos felel annak biztosításáért, hogy a CIS, a kiszervezési szerződés és a biztonságról szóló megállapodások megfeleljenek az információbiztonságról és informatikai biztonságról szóló bizottsági szabályoknak.

(8) A Humánerőforrásügyi és Biztonsági Főigazgatóság meghatározza az (1)–(7) pontokban foglalt feladatkörökkel és tevékenységekkel kapcsolatos részletes előírásokat, az alábbi 10. cikkel összhangban.

4. FEJEZET

VEGYES ÉS ZÁRÓ RENDELKEZÉSEK

9. cikk

Átláthatóság

Ezt a határozatot az Európai Bizottság személyzetének és a határozat hatálya alá tartozó minden személynek a tudomására kell hozni, és az Európai Unió Hivatalos Lapjában közzé kell tenni.

10. cikk

Standardok

(1) E határozat rendelkezéseit szükség esetén az (EU, Euratom) 2017/46 határozattal és a C(2017) 7428 határozattal összhangban elfogadott előírásokban és iránymutatásokban kell részletesebben meghatározni. Az informatikai biztonsággal kapcsolatos standardok és iránymutatások az ISO 27001:2013 szabvány A. melléklete szerinti konkrét biztonsági területek esetében további részletekkel szolgálnak e végrehajtási szabályok, valamint az (EU, Euratom) 2017/46 határozat tekintetében. Ezen standardok és iránymutatások az iparág bevált módszereire épülnek és a Bizottság IT környezetének megfelelően választották ki őket.

(2) A standardokat szükség esetén az ISO 27001:2013 szabvány A. mellékletének megfelelően az alábbi területeken kell fejleszteni:

1. az információbiztonság szervezése;
2. humánerőforrás-biztonság;
3. eszközkezelés;
4. hozzáférés szabályozása;
5. kriptográfia;
6. fizikai és környezeti biztonság;
7. üzembiztonság;
8. kommunikációs biztonság;
9. rendszerek beszerzése, fejlesztése és fenntartása;
10. kapcsolat a beszállítókkal;
11. információbiztonsági incidensek kezelése;
12. az üzletmenet-folytonosság kezelésének információbiztonsági szempontjai;
13. szabályszerűség.

(3) Az információbiztonsági irányítóbizottság az e cikk (1) és (2) bekezdésében említett standardokat azok elfogadását megelőzően jóváhagyja.

(4) Az e határozat alkalmazási körére vonatkozó C(2006) 3602 határozat végrehajtási szabályai hatályukat vesztik.

(5) A 2006. augusztus 16-i C (2006) 3602 határozat alapján elfogadott standardok és iránymutatások mindaddig hatályban maradnak, amíg az (EU, Euratom) 2017/46 határozat 13. cikke alapján elfogadandó standardok és iránymutatások a helyükbe nem lépnek.

11. cikk

Hatálybalépés

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Kelt Brüsszelben, 2018. április 6-án.

a Bizottság részéről,
az elnök nevében,
Günther OETTINGER
a Bizottság tagja

MELLÉKLET

SZEREPEK ÉS FELADATKÖRÖK (RASCI)

A RASCI modell a feladatkörök alábbi mutatókon alapuló kijelölésére utaló rövidítés:

a) R (Responsible) – felelős

b) A (Accountable) – elszámoltatható

c) S (Supporting) – támogató

d) C (Consulted) – tanácsadó

e) I (Informed) – tájékoztatott

Szerep / Eljárás	Információbiztonsági irányítóbizottság	HR (DS)	Bizottság Szervezeti egység	Rendszer Tulajdonos	Adattulajdonos	Helyi informatikai biztonsági tisztviselő	Informatikai Főigazgatóság	Szerződő vállalkozások
A Bizottság információbiztonsági politikájával való összhang		**R/A**	**S**				**S**	
Titkosítási technológiák		**C**	**A**	**R**	**I**	**C**		
Informatikai biztonsági ellenőrzések	**I**	**A/R**		**S**	**I**	**I**	**S**	
Külső hálózatokról való hozzáférés	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
A CIS-ek kiszervezése		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Az információbiztonsági irányítóbizottsággal konzultációt kell folytatni az Informatikai Főigazgatóságtól eltérő bármely bizottsági szervezeti egység által üzemeltetett belső hálózatok tekintetében.

[2] A kiszervezett CIS rendszertulajdonosa viseli a felelősséget, és minden olyan más CIS rendszertulajdonosával konzultálni kell, amely összekapcsolódik egy kiszervezett CIS-szel.