Ez a dokumentum kizárólag tájékoztató jellegű és nem vált ki joghatást. Az EU intézményei semmiféle felelősséget nem vállalnak a tartalmáért. A jogi aktusoknak – ideértve azok bevezető hivatkozásait és preambulumbekezdéseit is – az Európai Unió Hivatalos Lapjában közzétett és az EUR-Lex portálon megtalálható változatai tekintendők hitelesnek. Az említett hivatalos szövegváltozatok közvetlenül elérhetők az ebben a dokumentumban elhelyezett linkeken keresztül

►**B**

A BIZOTTSÁG (EU, Euratom) 2017/46 HATÁROZATA

(2017. január 10.)

az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról

(HL L 6., 2017.1.11., 40. o.)

Helyesbítette:

►**C1** Helyesbítés, HL L 261., 2017.10.11., 31. o. (2017/46)

▼B

A BIZOTTSÁG (EU, Euratom) 2017/46 HATÁROZATA

(2017. január 10.)

az Európai Bizottság kommunikációs és információs rendszereinek biztonságáról

1. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

A rendelet tárgya és hatálya

1. Ez a határozat az Európai Bizottság által vagy nevében tulajdonolt, beszerzett, kezelt és üzemeltetett összes kommunikációs és információs rendszerre, valamint e rendszerek Bizottság általi mindennemű felhasználására vonatkozik.

2. Ez a határozat a kommunikációs és információs rendszerek biztonságával kapcsolatos alapelveket, célkitűzéseket, szervezetet és feladatokat határozza meg különösen azoknak a bizottsági szervezeti egységeknek a számára, amelyek ilyen rendszereket tulajdonolnak, beszereznek, kezelnek vagy üzemeltetnek, ideértve a belső informatikai szolgáltató által biztosított kommunikációs és információs rendszereket is. Amennyiben valamely kommunikációs és információs rendszert az Európai Bizottsággal kötött kétoldalú megállapodás vagy szerződés alapján külső fél szolgáltatja, tulajdonolja, kezeli vagy üzemelteti, akkor az ilyen megállapodás vagy szerződés feltételeinek összhangban kell lenniük e határozattal.

3. Ez a határozat minden bizottsági szervezeti egységre és végrehajtó ügynökségre vonatkozik. Amennyiben valamely bizottsági kommunikációs és információs rendszert az Európai Bizottsággal kötött kétoldalú megállapodás alapján más szervek és intézmények használják, akkor az ilyen megállapodás feltételeinek összhangban kell lenniük e határozattal.

4. A személyzet egyes csoportjaira vonatkozó konkrét utalások ellenére, ezen határozat a Bizottság tagjaira, az Európai Unió tisztviselőinek személyzeti szabályzata (a továbbiakban: személyzeti szabályzat) és az Európai Unió egyéb alkalmazottaira vonatkozó alkalmazási feltételek (a továbbiakban: alkalmazási feltételek) ([1]) hatálya alá tartozó bizottsági személyzetre, a Bizottsághoz kirendelt nemzeti szakértőkre ([2]), a külső szolgáltatókra és azok személyzetére, a gyakornokokra és a jelen határozat értelmében kommunikációs és információs rendszerhez hozzáféréssel rendelkező bármely személyre vonatkozik.

([1]) A Tanács 1968. február 29-i 259/68/EGK, Euratom, ESZAK rendelete tartalmazza (Személyzeti Szabályzat) (HL L 56., 1968.3.4., 1. o.).

([2]) A Bizottság 2008. november 12-i határozata a Bizottság szolgálataihoz kirendelt nemzeti szakértőkre és szakmai továbbképzésen részt vevő nemzeti szakértőkre vonatkozó alkalmazási feltételekről (C(2008) 6866 final).

▼B

5. Ez a határozat az Európai Csalás Elleni Hivatalra (OLAF) is vonatkozik, amennyiben összeegyeztethető az uniós jogszabályokkal és az 1999/352/EK, ESZAK, Euratom bizottsági határozattal [1]. Az e határozatban előírt rendelkezések, így az utasítások, az ellenőrzések, a vizsgálatok és más, azokkal egyenértékű intézkedések hatálya esetlegesen nem terjedhet ki az OLAF kommunikációs és információs rendszereire, ha az nem összeegyeztethető az OLAF vizsgálati feladatkörének függetlenségével, illetve az e feladatkör ellátása során az OLAF tudomására jutott információk titkosságának megőrzésével.

2. cikk

Fogalommeghatározások

E határozat alkalmazásában a következő fogalommeghatározásokat kell alkalmazni:

(1) „elszámoltathatóság”: tettekért, döntésekért és teljesítményért való felelősségre vonhatóság;

(2) „CERT-EU”: az uniós intézmények és ügynökségek hálózatbiztonsági vészhelyzeteket elhárító csoportja. Feladata, hogy támogatást nyújtson az uniós intézményeknek abban, hogy megvédjék magukat az informatikai eszközeik sértetlenségét fenyegető és az EU érdekeit sértő szándékos és rosszindulatú támadásokkal szemben. A CERT-EU tevékenységeinek köre a megelőzésre, az észlelésre, a válaszintézkedésekre és a helyreállításra terjed ki;

(3) „a Bizottság szervezeti egysége”: bármely bizottsági főigazgatóság vagy szolgálat vagy a Bizottság bármely tagjának kabinetje;

(4) „a Bizottság Biztonsági Hatósága”: az (EU, Euratom) 2015/444 bizottsági határozatban meghatározott szerepkör;

(5) „kommunikációs és információs rendszer”: az elektronikus formában történő információkezelést lehetővé tevő rendszer, ideértve a működéséhez szükséges valamennyi eszközt, valamint az infrastruktúrát, a szervezetet, a személyzetet és az információs forrásokat. Ez a fogalommeghatározás az üzleti alkalmazásokat, a megosztott informatikai szolgáltatásokat, a kiszervezett rendszereket és a végfelhasználói eszközöket is magában foglalja;

(6) „szervezetirányító tanács”: működési és igazgatási ügyekben a legmagasabb szintű szervezetirányítási ellenőrzést gyakorolja a Bizottságon belül;

(7) „adatbirtokos”: a kommunikációs és információs rendszer által kezelt konkrét adatkészlet védelméért és felhasználásáért felelős személy;

(8) „adatkészlet”: a Bizottság meghatározott működési folyamatának vagy tevékenységének céljára szolgáló információk együttese;

(9) „vészhelyzeti eljárás”: sürgős esetekben a Bizottság működésére gyakorolt súlyos hatások elkerülése érdekében végrehajtandó válaszintézkedésekhez előre meghatározott módszerek és feladatok összessége;

[1] A Bizottság 1999. április 28-i 1999/352/EK, ESZAK, Euratom határozata az Európai Csalászelleni Hivatal (OLAF) létrehozásáról (az értesítés a SEC(1999) 802. számú dokumentummal történt) (HL L 136., 1999.5.31., 20. o.).

▼B

(10) „információbiztonsági politika”: a meghatározott, végrehajtott és ellenőrzött, illetve meghatározandó, végrehajtandó és ellenőrzendő információbiztonsági célkitűzések összessége. Többek között az (EU, Euratom) 2015/444 és az (EU, Euratom) 2015/443 határozat tartozik ide;

(11) „információbiztonsági irányítóbizottság”: a szervezetirányító tanácsot az informatikai biztonsággal kapcsolatos feladatainak ellátásában támogató irányító szerv;

(12) „belső informatikai szolgáltató”: megosztott informatikai szolgáltatásokat nyújtó bizottsági szervezeti egység;

(13) „informatikai biztonság” vagy „a kommunikációs és információs rendszerek biztonsága”: a kommunikációs és információs rendszerek és az általuk feldolgozott adatkészletek titkosságának, sértetlenségének és rendelkezésre állásának megőrzése;

(14) „informatikai biztonsági iránymutatások”: ajánlott, de nem kötelező intézkedések, amelyek előmozdítják az informatikai biztonsági előírások teljesítésének támogatását, vagy vonatkozó szabványok hiányában alapul vehetők;

(15) „informatikai biztonsági incidens”: olyan esemény, amely valamely kommunikációs és információs rendszer titkosságát, sértetlenségét vagy rendelkezésre állását veszélyezteti;

(16) „informatikai biztonsági intézkedés”: az informatikai biztonsági kockázatok csökkentésére irányuló műszaki vagy szervezeti intézkedés;

(17) „informatikai biztonsági igény”: a titkosság, a sértetlenség és a rendelkezésre állás adott információra vagy informatikai rendszerre vonatkozó szintjének pontos és egyértelmű meghatározása a szükséges mértékű védelem megállapítása céljából;

(18) „informatikai biztonsági célkitűzés”: meghatározott fenyegetésekkel szembeni fellépés, illetve meghatározott szervezeti biztonsági követelmények vagy előfeltételek teljesítése iránti szándék kifejezése;

(19) „informatikai biztonsági terv”: a kommunikációs és információs rendszerek informatikai biztonsági igényeinek kielégítéséhez szükséges informatikai biztonsági intézkedések dokumentációja;

(20) „informatikai biztonsági politika”: a meghatározott, végrehajtott és ellenőrzött, illetve meghatározandó, végrehajtandó és ellenőrzendő informatikai biztonsági célkitűzések összessége. E határozat és annak végrehajtási szabályai tartoznak ide;

(21) „informatikai biztonsági követelmény”: előzetesen meghatározott folyamat keretében hivatalosan megfogalmazott informatikai biztonsági igény;

(22) „informatikai biztonsági kockázat”: informatikai biztonsági fenyegetés által kommunikációs és információs rendszeren sebezhetőség kihasználásával kiváltható hatás. Ennek megfelelően az informatikai biztonsági kockázat a következő két tényezővel jellemezhető: 1. bizonytalanság, vagyis informatikai biztonsági fenyegetés által előidézett nemkívánatos esemény bekövetkezésének valószínűsége, valamint 2. hatás, vagyis az ilyen nemkívánatos esemény esetleges következményei a kommunikációs és információs rendszerre nézve;

▼B

(23) „informatikai biztonsági előírások”: az informatikai biztonsági politika végrehajtását és támogatását elősegítő konkrét, kötelező erejű informatikai biztonsági rendelkezések;

(24) „informatikai biztonsági stratégia”: a Bizottság célkitűzéseinek elérése érdekében meghatározandó, végrehajtandó és ellenőrizendő projektek és tevékenységek összessége;

(25) „informatikai biztonsági fenyegetés”: olyan tényező, amely a kommunikációs és információs rendszerben esetlegesen károsodást eredményező nemkívánatos eseményhez vezethet. E fenyegetések lehetnek véletlenszerűek vagy szándékosak, és azokat fenyegető elemek, potenciális célpontok és támadási módszerek jellemezik;

(26) „helyi informatikai biztonsági tisztviselő”: egy adott bizottsági szervezeti egységen belül az informatikai biztonsági kapcsolattartásért felelős tisztviselő;

(27) „személyes adat”, „személyes adatok feldolgozása”, „adatkezelő” és „személyesadat-nyilvántartó rendszer”: jelentésük megegyezik a 45/2001/EK rendeletben és különösen annak 2. cikkében foglaltakkal;

(28) „információk feldolgozása”: a kommunikációs és információs rendszerek adatkészletekkel kapcsolatos összes funkciója, így információk létrehozása, módosítása, megjelenítése, tárolása, átvitele, törlése és archiválása. A kommunikációs és információs rendszer az információk feldolgozását a felhasználóknak funkciók, más kommunikációs és információs rendszereknek pedig informatikai szolgáltatások formájában kínálhatja;

(29) „szakmai titoktartás”: az EUMSZ 339. cikkében foglaltak szerinti szakmai titoktartási kötelezettség alá eső üzleti adatok, különösen a vállalkozásokra, az ezek üzleti kapcsolataira vagy költségösszetevőire vonatkozó információk védelme;

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

(31) „a Bizottságon belüli biztonság”: a személyek, eszközök és információk biztonsága a Bizottságbon belül, különösen a személyek testi épsége és az eszközök fizikai sértetlensége, az információk és a kommunikációs és információs rendszerek sértetlensége, titkossága és rendelkezésre állása, valamint a Bizottság tevékenységeinek zavartalansága;

(32) „megosztott informatikai szolgáltatás”: kommunikációs és információs rendszer által információk feldolgozásakor másik kommunikációs és információs rendszereknek nyújtott szolgáltatás;

(33) „rendszerfelelős”: kommunikációs és információs rendszer beszerzéséért, fejlesztéséért, integrálásáért, módosításáért, üzemeltetéséért, karbantartásáért és üzemen kívül helyezéséért általánosan felelős személy;

(34) „felhasználó”: a kommunikációs és információs rendszer által nyújtott szolgáltatást igénybe vevő, Bizottságon belüli vagy kívüli személy.

3. cikk

A Bizottságon belüli informatikai biztonságra vonatkozó alapelvek

1. A Bizottságon belüli informatikai biztonság a jogszerűség, átláthatóság, arányosság és elszámoltathatóság alapelveire épül.

▼B

2. Az informatikai biztonsági szempontokat már a bizottsági kommunikációs és információs rendszerek tervezésének és kiépítésének elején figyelembe kell venni. Ennek érdekében az Informatikai Főigazgatóságot és a Humánerőforrásügyi és Biztonsági Főigazgatóságot is be kell vonni a hatáskörükbe tartozó ügyekbe.

3. A hatékony informatikai védelem az alábbi tényezők megfelelő szintjét biztosítja:

a) hitelesség: annak garanciája, hogy az információ valódi és jóhiszemű forrásokból származik;

b) rendelkezésre állás: az engedéllyel rendelkező szervezet kérelemére megvalósuló hozzáférhetőség és felhasználhatóság;

c) titkosság: annak garanciája, hogy az információ nem hozzáférhető illetéktelen személy, szervezet vagy folyamat részére;

d) sértetlenség: az eszközök és információk pontosságának és teljességének védelme;

e) letagadhatatlanság: egy cselekmény vagy esemény megtörténtének bizonyíthatósága annak érdekében, hogy ezt a cselekedetet vagy eseményt később ne lehessen letagadni;

f) a személyes adatok védelme: a személyes adatok tekintetében megfelelő biztosítékok nyújtása a 45/2001/EK rendelettel teljes összhangban;

g) szakmai titoktartás: az EUMSZ 339. cikkében foglaltak szerint szakmai titoktartási kötelezettség alá eső adatok, különösen a vállalkozásokra, az ezek üzleti kapcsolataira vagy költségösszetevőire vonatkozó információk védelme.

4. Az informatikai biztonság kockázatkezelési eljáráson alapul. Ezen eljárás keretében az informatikai biztonsági kockázatok szintjét kell megállapítani, és az e kockázatok elfogadható költségek mellett megfelelő szintre való csökkentését szolgáló biztonsági intézkedéseket kell meghatározni.

5. Minden kommunikációs és információs rendszert azonosítani kell, rendszerfelelőshöz kell rendelni, és leltárba kell venni.

6. Mindegyik kommunikációs és információs rendszer biztonsági követelményeit az adott rendszer és az általa feldolgozott információk biztonsági igényei alapján kell megállapítani. A másik kommunikációs és információs rendszernek szolgáltatást nyújtó kommunikációs és információs rendszer kialakítható úgy, hogy meghatározott szintű biztonsági igényeket támogasson.

7. Az informatikai biztonsági terveknek és az informatikai biztonsági intézkedéseknek arányosnak kell lenniük a kommunikációs és információs rendszer biztonsági igényeivel.

▼C1

8. Az 1–7. bekezdésben meghatározott alapelvekhez és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

2. FEJEZET

SZERVEZET ÉS FELELŐSSÉGI KÖRÖK

4. cikk

Szervezetirányító tanács

A szervezetirányító tanács általános felelősséget vállal a Bizottságon belüli teljes körű informatikai biztonsági irányításért.

5. cikk

Információbiztonsági irányítóbizottság

1. Az információbiztonsági irányítóbizottság elnöki tisztét a Bizottságon belüli informatikai biztonsági irányításért felelős főtitkárhelyettes tölti be. Tagjai a Bizottság szervezeti egységein belüli üzleti, technológiai és biztonsági érdekeket képviselik, és az Informatikai Főigazgatóságból, a Humánerőforrásügyi és Biztonsági Főigazgatóságból, valamint a Költségvetési Főigazgatóságból, továbbá kétévente, rotációs rendszerben négy másik olyan szervezeti egységből kerülnek ki, ahol az informatikai biztonság a tevékenységek szempontjából kiemelt jelentőséggel bír. A tagság felső vezetőkből áll.

2. Az információbiztonsági irányítóbizottság támogatja a szervezetirányító tanácsot az informatikai biztonsággal kapcsolatos feladatainak ellátásában. Az információbiztonsági irányítóbizottság operatív felelősséget vállal a Bizottságon belüli teljes körű informatikai biztonsági irányításért.

3. Az információbiztonsági irányítóbizottság elfogadás céljából ajánlást tesz a Bizottságnak a bizottsági informatikai biztonsági politikára.

4. Az információbiztonsági irányítóbizottság megvizsgálja az irányítási ügyeket és az informatikai biztonsággal kapcsolatos problémákat, így a súlyos informatikai biztonsági incidenseket is, és kétévente jelentést nyújt be róluk a szervezetirányító tanácsnak.

5. Az információbiztonsági irányítóbizottság figyelemmel kíséri és felülvizsgálja e határozat általános végrehajtását, és erről jelentést készít a szervezetirányító tanácsnak.

6. Az információbiztonsági irányítóbizottság az Informatikai Főigazgatóság javaslatára felülvizsgálja, jóváhagyja és figyelemmel kíséri a folyamatosan megújuló informatikai biztonsági stratégia végrehajtását, és erről jelentést tesz a szervezetirányító tanácsnak.

7. Az információbiztonsági irányítóbizottság figyelemmel kíséri, értékeli és ellenőrzi az információkockázat-kezelési környezetet, és szükség esetén jogosult fejlesztés céljából hivatalos követelményeket megfogalmazni.

▼C1

8. Az 1–7. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

6. cikk

A Humánerőforrásügyi és Biztonsági Főigazgatóság

A Humánerőforrásügyi és Biztonsági Főigazgatóság feladatai az informatikai biztonsággal összefüggésben a következők:

▼B

(1) biztosítja az informatikai biztonsági politika és a bizottsági információbiztonsági politika összhangját;

(2) létrehozza a titkosítási technológiák kommunikációs és információs rendszerek által végzett tároláshoz és kommunikációhoz való felhasználásának engedélyezésére vonatkozó keretet;

(3) tájékoztatja az Informatikai Főigazgatóságot a konkrét fenyegetésekről, amelyek jelentős hatással lehetnek a kommunikációs és információs rendszerek és az általuk feldolgozott adatkészletek biztonságára;

(4) informatikai biztonsági ellenőrzéseket végez annak felmérése céljából, hogy a bizottsági kommunikációs és információs rendszerek megfelelnek-e a biztonsági politikában foglaltaknak, az ellenőrzések eredményéről pedig jelentésben számol be az információbiztonsági irányítóbizottságnak;

(5) meghatározza a bizottsági kommunikációs és információs rendszerekhez külső hálózatokból való hozzáférés engedélyezésének keretét és a kapcsolódó, megfelelő biztonsági szabályokat, valamint az Informatikai Főigazgatósággal szorosan együttműködve kidolgozza a vonatkozó informatikai biztonsági előírásokat és iránymutatásokat;

(6) a kommunikációs és információs rendszerek kiszervezésére vonatkozó alapelveket és szabályokat javasol az információk biztonsága feletti megfelelő ellenőrzés fenntartása érdekében;

▼C1

(7) az Informatikai Főigazgatósággal szorosan együttműködve kidolgozza az (1)–(6) pontban meghatározott informatikai biztonsági előírásokat és iránymutatásokat;

(8) az (1)–(7) pontban meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

7. cikk

Az Informatikai Főigazgatóság

Az Informatikai Főigazgatóság feladatai a Bizottság általános informatikai biztonságával összefüggésben a következők:

(1) a 6. cikkben foglalt kivételektől eltekintve a Humánerőforrásügyi és Biztonsági Főigazgatósággal szorosan együttműködve informatikai biztonsági előírásokat és iránymutatásokat dolgoz ki az informatikai biztonsági politika és a bizottsági információbiztonsági politika közötti összhang biztosítása érdekében, és ezeket az információbiztonsági irányítóbizottság elé terjeszti;

(2) értékeli az összes bizottsági szervezeti egység informatikai biztonsági kockázatkezelési módszereit, eljárásait és eredményeit, és erről rendszeresen jelentést tesz az információbiztonsági irányítóbizottságnak;

(3) folyamatosan megújuló informatikai biztonsági stratégiát javasol, amelyet az információbiztonsági irányítóbizottságnak kell felülvizsgálnia és jóváhagynia, a szervezetirányító tanácsnak pedig elfogadnia, továbbá az informatikai biztonsági stratégia végrehajtására irányuló projektek és tevékenységek tervezését is magában foglaló programra tesz javaslatot;

(4) figyelemmel kíséri a bizottsági informatikai biztonsági stratégia végrehajtását, és erről rendszeresen jelentésben számol be az információbiztonsági irányítóbizottságnak;

(5) figyelemmel kíséri az informatikai biztonsági kockázatokat és a kommunikációs és információs rendszereken belül végrehajtott informatikai biztonsági intézkedéseket, és erről rendszeresen jelentést nyújt be az információbiztonsági irányítóbizottságnak;

▼B

(6) rendszeresen jelentést tesz az információbiztonsági irányítóbizottságnak e határozat általános végrehajtásáról és betartásáról;

(7) a Humánerőforrásügyi és Biztonsági Főigazgatósággal folytatott egyeztetést követően felkéri a rendszerfelelősöket, hogy tegyenek konkrét informatikai biztonsági intézkedéseket a bizottsági kommunikációs és információs rendszereket érintő informatikai biztonsági kockázatok csökkentése érdekében;

(8) gondoskodik arról, hogy megfelelő jegyzék álljon a rendszerfelelősök és az adatbirtokosok rendelkezésére az Informatikai Főigazgatóság informatikai biztonsági szolgáltatásairól ahhoz, hogy teljesítsék informatikai biztonsági feladataikat, és betartsák az informatikai biztonsági politikában és előírásokban foglaltakat;

(9) kellő dokumentációt biztosít a rendszer- és az adatbirtokosok számára, és szükség szerint egyeztet velük az informatikai szolgáltatásaik esetében végrehajtott informatikai biztonsági intézkedésekről, hogy megkönnyítse az informatikai biztonsági politikában foglaltak betartását, és támogassa a rendszerfelelősöket az informatikai kockázatkezelésben;

(10) rendszeres üléseket szervez a helyi informatikai biztonsági tisztviselők hálózata számára, és támogatja a helyi informatikai biztonsági tisztviselőket feladataik ellátásában;

(11) a bizottsági szervezeti egységekkel együttműködve meghatározza az informatikai biztonsággal kapcsolatos képzési szükségleteket, és koordinálja a vonatkozó képzési programokat, továbbá a Humánerőforrásügyi és Biztonsági Főigazgatósággal együttműködve az informatikai biztonságra vonatkozó figyelemfelkeltő kampányokat szervez és koordinál;

(12) gondoskodik arról, hogy a rendszerfelelősök, az adatbirtokosok és a bizottsági szervezeti egységeken belül informatikai biztonsági feladatokkal rendelkező egyéb tisztviselők megismerjék az informatikai biztonsági politikát;

(13) tájékoztatja a Humánerőforrásügyi és Biztonsági Főigazgatóságot azokról a konkrét informatikai biztonsági fenyegetésekről, incidensekről és a rendszerfelelősök által bejelentett, a bizottsági informatikai biztonsági politika alóli kivételekről, amelyek jelentős hatást gyakorolhatnak a Bizottságon belüli biztonságra;

(14) belső informatikai szolgáltatói szerepkörére figyelemmel jegyzéket ad át a Bizottságnak a meghatározott szintű biztonságot nyújtó megosztott informatikai szolgáltatásokról. Ehhez az informatikai biztonsági kockázatok módszeres értékelésére, kezelésére és figyelemmel kísérésére van szükség, hogy végrehajthatók legyenek a meghatározott biztonsági szint elérésére irányuló biztonsági intézkedések;

▼C1

(15) az (1)–(14) pontban meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

8. cikk

A Bizottság szervezeti egységei

Mindegyik bizottsági szervezeti egység vezetője a következő, informatikai biztonsággal kapcsolatos feladatokat látja el a saját szervezeti egységén belül:

(1) mindegyik kommunikációs és információs rendszerhez hivatalosan kijelöl a tisztviselők vagy ideiglenes alkalmazottak közül egy rendszerfelelőst, aki az adott kommunikációs és információs rendszer informatikai biztonságáért felel, az egyes kommunikációs és információs rendszerek által kezelt adatkészletek tekintetében pedig hivatalosan kijelöl egy adatbirtokost, akinek ugyanannál az igazgatási egységnél kell dolgoznia, amely a 45/2001/EK rendelet hatálya alá tartozó adatkészletek tekintetében az adatkezelő;

(2) hivatalosan kijelöl egy helyi informatikai biztonsági tisztviselőt, aki a rendszerfelelőstől és az adatbirtokostól függetlenül látja el feladatait. Egy helyi informatikai biztonsági tisztviselő egy vagy több bizottsági szervezeti egység számára is kijelölhető;

(3) gondoskodik arról, hogy a szükséges informatikai biztonsági kockázatértékelések és informatikai biztonsági tervek elkészüljenek és teljesüljenek;

(4) gondoskodik arról, hogy rendszeresen készüljenek összefoglaló jelentések az Informatikai Főigazgatóság számára az informatikai biztonsági kockázatokról és intézkedésekről;

(5) az Informatikai Főigazgatóság támogatásával gondoskodik arról, hogy megfelelő folyamatok, eljárások és megoldások álljanak rendelkezésre a szervezeti egység kommunikációs és információs rendszereit érintő informatikai biztonsági incidensek hatékony észleléséhez, bejelentéséhez és elhárításához;

(6) informatikai biztonsági vészhelyzet esetén vészhelyzeti eljárást indít;

(7) végső felelősséget visel az informatikai biztonságért, ideértve a rendszerfelelős és az adatbirtokos feladatait is;

(8) felel a szervezeti egység kommunikációs és információs rendszereit és adatkészleteit érintő kockázatokért;

(9) megkísérli rendezni az adatbirtokosok és a rendszerfelelősök közötti nézetkülönbségeket, és amennyiben ez nem sikerül, az információbiztonsági irányítóbizottság elé terjeszti az ügyet rendezésre;

(10) gondoskodik az informatikai biztonsági tervek és az informatikai biztonsági intézkedések végrehajtásáról, és a kockázatok megfelelő kezeléséről;

▼C1

(11) az (1)–(10) pontban meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

9. cikk

Rendszerfelelősök

1. A rendszerfelelős a kommunikációs és információs rendszer informatikai biztonságáért felel, és a bizottsági szervezeti egység vezetőjének tartozik beszámolási kötelezettséggel.

▼B

2. Az informatikai biztonsággal összefüggésben a következő feladatokat látja el:

a) gondoskodik arról, hogy a kommunikációs és információs rendszer eleget tegyen az informatikai biztonsági politikában foglaltaknak;

b) gondoskodik a kommunikációs és információs rendszer pontos leltárba vételéről;

c) az adatbirtokosokkal együttműködve és az Informatikai Főigazgatósággal egyeztetve felméri az informatikai biztonsági kockázatokat, és meghatározza az informatikai biztonsági igényeket az egyes kommunikációs és információs rendszerek esetében;

d) biztonsági tervet dolgoz ki, amely adott esetben tartalmazza a felmért kockázatok részleteit és a szükséges kiegészítő biztonsági intézkedéseket;

e) az azonosított informatikai biztonsági kockázatokkal arányosan végrehajtja a kellő informatikai biztonsági intézkedéseket, és követi az információbiztonsági irányítóbizottság által elfogadott ajánlásokat;

f) feltárja a más kommunikációs és információs rendszerektől vagy megosztott informatikai szolgáltatásoktól való esetleges függést, és szükség esetén biztonsági intézkedéseket hajt végre az e kommunikációs és információs rendszerek vagy megosztott informatikai szolgáltatások esetében javasolt biztonsági szintek alapján;

g) kezeli és figyelemmel kíséri az informatikai biztonsági kockázatokat;

h) rendszeresen jelentést tesz a bizottsági szervezeti egység vezetőjének a kommunikációs és információs rendszer informatikai biztonsági kockázati profiljáról, az Informatikai Főigazgatóságnak pedig a vonatkozó kockázatokról, kockázatkezelési tevékenységekről és végrehajtott biztonsági intézkedésekről;

i) informatikai biztonsági vonatkozású ügyekben egyeztet az érintett bizottsági szervezeti egység(ek) helyi informatikai biztonsági tisztviselőjével;

j) utasításokat ad a felhasználóknak a kommunikációs és információs rendszer és a kapcsolódó adatok felhasználásáról, valamint a felhasználók kommunikációs és információs rendszerrel kapcsolatos feladatairól;

k) engedélyt kér a kriptográfiai hatóságként eljáró Humánerőforrásügyi és Biztonsági Főigazgatóságtól minden olyan kommunikációs és információs rendszerre, amely titkosítási technológiát használ;

l) előzetesen egyeztet a Bizottság Biztonsági Hatóságával minden olyan rendszerről, amely EU-minősített adatokat dolgoz fel;

m) gondoskodik a visszafejtő kulcsok biztonsági másolatainak letéti őrzéséről. A titkosított adatok kizárólag a Humánerőforrásügyi és Biztonsági Főigazgatóság által meghatározott keret szerint engedélyezett esetben alakíthatók vissza.

n) teljesíti a személyes adatok védelmével és az adatfeldolgozás biztonságára vonatkozó adatvédelmi szabályok alkalmazásával kapcsolatosan az illetékes adatkezelő(k)től kapott utasításokat;

o) tájékoztatja az Informatikai Főigazgatóságot a bizottsági informatikai biztonsági politika alóli kivételekről, azok megfelelő indoklásával együtt;

▼B

p) jelenti az adatbirtokos és a rendszerfelelős közötti feloldhatatlan nézetkülönbségeket a bizottsági szervezeti egység vezetőjének, az informatikai biztonsági incidensekről pedig azok súlyosságához mérten időben értesíti az érintetteket a 15. cikkben foglaltak szerint;

q) kiszervezett rendszerek esetében gondoskodik arról, hogy a kiszervezési szerződések megfelelő informatikai biztonsági rendelkezéseket tartalmazzanak, valamint hogy a kiszervezett kommunikációs és információs rendszerben bekövetkező informatikai biztonsági incidenseket a 15. cikknek megfelelően bejelentsék;

r) megosztott informatikai szolgáltatásokat nyújtó kommunikációs és információs rendszer esetében gondoskodik arról, hogy a meghatározott biztonsági szintet közöljék, egyértelműen dokumentálják, és az adott kommunikációs és információs rendszerben való eléréséhez szükséges biztonsági intézkedéseket végrehajtsák.

3. A rendszerfelelősök informatikai biztonsági feladataikat részben vagy egészben formálisan átruházhatják, de kommunikációs és információs rendszerük informatikai biztonságáért változatlanul ők viselik a felelősséget.

▼C1

4. Az 1–3. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

10. cikk

Adatbirtokosok

1. Az adatbirtokos felelősséggel tartozik a bizottsági szervezeti egység felé egy meghatározott adatkészlet informatikai biztonságáért, és az adatkészlet titkossága, sértetlensége és rendelkezésre állása tekintetében elszámoltatható.

2. Az adatkészlettel összefüggésben az adatbirtokos a következő feladatokat látja el:

a) biztosítja, hogy a felelősségi körébe tartozó összes adatkészlet az (EU, Euratom) 2015/443 és az (EU, Euratom) 2015/444 határozat szerint megfelelően minősített legyen;

b) meghatározza az információbiztonsági igényeket, és ezekről tájékoztatja az érintett rendszerfelelősöket;

c) közreműködik a kommunikációs és információs rendszer kockázatértékelésében;

d) jelenti az adatbirtokos és a rendszerfelelős közötti feloldhatatlan nézetkülönbségeket a bizottsági szervezeti egység vezetőjének;

e) a 15. cikkben foglaltak szerint bejelenti az informatikai biztonsági incidenseket.

3. Az adatbirtokosok informatikai biztonsági feladataikat részben vagy egészben formálisan átruházhatják, de az e cikkben meghatározott felelősségi körük változatlanul fennáll.

▼C1

4. Az 1–3. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

11. cikk

Helyi informatikai biztonsági tisztviselők

▼C1

1. A helyi informatikai biztonsági tisztviselő az informatikai biztonsággal összefüggésben a következő feladatokat látja el:

a) proaktívan azonosítja a rendszerfelelősöket, az adatbirtokosokat és a bizottsági szervezeti egységeken belül informatikai biztonsági feladatokkal rendelkező egyéb tisztviselőket, és tájékoztatja őket az informatikai biztonsági politikáról;

b) a bizottsági szervezeti egység(ek)en belül az informatikai biztonságot érintő kérdésekben kapcsolatot tart az Informatikai Főigazgatósággal a helyi informatikai biztonsági tisztviselők hálózatának tagjaként;

c) részt vesz a helyi informatikai biztonsági tisztviselők rendszeres ülésein;

d) folyamatosan fenntartja és felügyeli az információbiztonsági kockázatkezelési folyamatot, valamint az információs rendszerek biztonsági terveinek kidolgozását és végrehajtását;

e) az informatikai biztonsággal kapcsolatos kérdésekben tanácsot ad az adatbirtokosoknak, a rendszerfelelősöknek és a bizottsági szervezeti egységek vezetőinek;

f) együttműködik az Informatikai Főigazgatósággal a bevált informatikai biztonsági gyakorlatok terjesztésében, és javaslatot tesz konkrét figyelemfelkeltő és képzési programokra;

g) jelentést tesz az informatikai biztonságról, valamint meghatározza a hiányosságokat és a fejlesztési lehetőségeket a bizottsági szervezeti egység(ek) vezetője számára.

2. Az 1. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

12. cikk

Felhasználók

1. Az informatikai biztonsággal összefüggésben a felhasználónak a következő feladatai vannak:

a) eleget tesz az informatikai biztonsági politikában foglaltaknak és a rendszerfelelős által az egyes kommunikációs és információs rendszerek használatáról adott utasításoknak;

b) a 15. cikkben foglaltak szerint bejelenti az informatikai biztonsági incidenseket.

2. A bizottsági kommunikációs és információs rendszereknek az informatikai biztonsági politikával vagy a rendszerfelelős által adott utasításokkal ellentétes használata fegyelmi eljárást vonhat maga után.

▼C1

3. Az 1. és a 2. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

3. FEJEZET

BIZTONSÁGI KÖVETELMÉNYEK ÉS KÖTELEZETTSÉGEK

13. cikk

E határozat végrehajtása

1. ►C1 A 6. cikk (2) pontjában említett végrehajtási szabályok, valamint a kapcsolódó előírások és iránymutatások elfogadásához a Bizottság biztonsági ügyekért felelős tagjának adott felhatalmazásról szóló bizottsági határozat lehet szükséges. ◄

2. ►C1 Az e határozattal összefüggő minden egyéb végrehajtási szabály, valamint a kapcsolódó informatikai biztonsági előírások és iránymutatások elfogadásához a Bizottság informatikáért felelős tagjának adott felhatalmazásról szóló bizottsági határozat lehet szükséges. ◄

3. A fenti (1) és (2) bekezdésben említett végrehajtási szabályokat, előírásokat és irányelveket azok elfogadása előtt az információbiztonsági irányítóbizottságnak jóvá kell hagynia.

14. cikk

Betartási kötelezettség

1. Az informatikai biztonsági politikában és előírásokban foglalt rendelkezések betartása kötelező.

2. Az informatikai biztonsági politika és előírások be nem tartása a Szerződésekkel, a személyzeti szabályzattal és az alkalmazási feltételekkel összhangban fegyelmi eljárást, szerződéses szankciókat, illetve a nemzeti jogszabályok és előírások értelmében jogi lépéseket vonhat maga után.

3. Az Informatikai Főigazgatóságot az informatikai biztonsági politika alóli összes kivételről értesíteni kell.

4. Amennyiben az információbiztonsági irányítóbizottság úgy határoz, hogy a Bizottság valamely kommunikációs és információs rendszerét tartós, elfogadhatatlan kockázat fenyegeti, akkor az Informatikai Főigazgatóság a rendszerfelelőssel együttműködve kockázatcsökkentő intézkedéseket javasol az információbiztonsági irányítóbizottságnak elfogadásra. Ilyen intézkedés lehet egyebek mellett a fokozott megfigyelés és jelentés, a szolgáltatáskorlátozás és a kapcsolat bontása.

5. Az információbiztonsági irányítóbizottság szükség esetén előírhatja a jóváhagyott kockázatcsökkentő intézkedések végrehajtását. Az információbiztonsági irányítóbizottság ajánlhatja közigazgatási vizsgálat indítását a Humánerőforrásügyi és Biztonsági Főigazgatóság főigazgatójának. Az Informatikai Főigazgatóság minden olyan helyzetet jelent az információbiztonsági irányítóbizottságnak, amikor kockázatcsökkentő intézkedéseket írtak elő.

▼C1

6. Az 1–5. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

15. cikk

Az informatikai biztonsági incidensek kezelése

1. Az Informatikai Főigazgatóság feladata, hogy a Bizottságon belül biztosítsa az informatikai biztonsági incidensekkel szembeni operatív válaszintézkedés képességét.

2. Az informatikai biztonsági incidensekkel szembeni válaszintézkedésekben közreműködő érdekelt félként a Humánerőforrásügyi és Biztonsági Főigazgatóság:

a) jogosult betekinteni az incidensek nyilvántartásának kivonatába, kérésre pedig a teljes nyilvántartásba;

b) részt vesz az informatikai biztonsági incidensekkel foglalkozó válságkezelő csoportokban és az informatikai biztonsági vészhelyzeti eljárásokban;

c) ápolja a kapcsolatokat a bűnüldöző és a hírszerző szolgálatokkal;

d) a kiberbiztonságra vonatkozó igazságügyi szakértői elemzést végez az (EU, Euratom) 2015/443 rendelet 11. cikke szerint;

e) határoz arról, hogy szükséges-e hivatalos vizsgálatot indítani;

f) tájékoztatja az Informatikai Főigazgatóságot a más kommunikációs és információs rendszereket esetlegesen veszélyeztető informatikai biztonsági incidensekről.

3. Az Informatikai Főigazgatóságnak és a Humánerőforrásügyi és Biztonsági Főigazgatóságnak rendszeresen egyeztetnie kell egymással információcsere és a biztonsági incidensek – különösen a hivatalos vizsgálatot igénylő informatikai biztonsági incidensek – kezelésének összehangolása céljából.

4. Az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportjának (CERT-EU) incidensekkel kapcsolatos koordinációs szolgáltatásai szükség esetén igénybe vehetők az incidenskezelési eljárás támogatása és az ismeretek más, esetlegesen érintett uniós intézményekkel és hivatalokkal való megosztása érdekében.

5. Az informatikai biztonsági incidensekben érintett rendszerfelelősök feladatai a következők:

a) minden jelentős, különösen az adatok titkosságának megsértésével járó informatikai biztonsági incidensről haladéktalanul értesítik szervezeti egységük vezetőjét, az Informatikai Főigazgatóságot, a Humánerőforrásügyi és Biztonsági Főigazgatóságot, a helyi informatikai biztonsági tisztviselőt és adott esetben az adatbirtokost;

b) az incidensek bejelentésével, a válaszintézkedésekkel és a helyreállítással összefüggésben együttműködnek az illetékes bizottsági hatóságokkal, és követik azok utasításait.

▼B

6. A felhasználóknak minden tényleges vagy feltételezett informatikai biztonsági incidenst a lehető leghamarabb jelenteniük kell az illetékes informatikai ügyfélszolgálatnak.

7. Az adatbirtokosoknak minden tényleges vagy feltételezett informatikai biztonsági incidenst a lehető leghamarabb jelenteniük kell az illetékes, informatikai biztonsági incidenseket elhárító csoportnak.

8. Az Informatikai Főigazgatóság feladata, hogy más közreműködő érdekeltek támogatásával kezelje a nem kiszervezett bizottsági kommunikációs és információs rendszerekkel összefüggésben felmerülő informatikai biztonsági incidenseket.

9. Az Informatikai Főigazgatóságnak az érintett bizottsági szervezeti egységeket, az illetékes helyi informatikai biztonsági tisztviselőket és adott esetben, a szükséges mértékig a CERT-EU-t kell tájékoztatnia az informatikai biztonsági incidensekről.

10. Az Informatikai Főigazgatóság rendszeresen jelentést készít az információbiztonsági irányítóbizottságnak a bizottsági kommunikációs és információs rendszereket érintő súlyos informatikai biztonsági incidensekről.

11. Az illetékes helyi informatikai biztonsági tisztviselőnek kérésre betekintést kell engedni a bizottsági szervezeti egység kommunikációs és információs rendszerét érintő informatikai biztonsági incidensekre vonatkozó nyilvántartásba.

12. Súlyos informatikai biztonsági incidens bekövetkeztekor az Informatikai Főigazgatóság a válsághelyzetek kezelése tekintetében kapcsolattartóként szolgálva összehangolja az informatikai biztonsági incidensekkel foglalkozó válságkezelő csoportok tevékenységeit.

13. Vészhelyzet esetén az Informatikai Főigazgatóság főigazgatója határozhat úgy, hogy informatikai biztonsági vészhelyzeti eljárást indít. Az Informatikai Főigazgatóságnak vészhelyzeti eljárásokat kell kidolgoznia, és jóváhagyás céljából az információbiztonsági irányítóbizottság elé terjesztenie.

14. Az Informatikai Főigazgatóságnak jelentést kell készítenie az információbiztonsági irányítóbizottság és az érintett bizottsági szervezeti egységek vezetői számára a vészhelyzeti eljárások végrehajtásáról.

▼C1

15. Az 1–14. bekezdésben meghatározott feladatokhoz és tevékenységekhez kapcsolódó eljárások részleteit végrehajtási szabályokban kell meghatározni, a 13. cikknek megfelelően.

▼B

4. FEJEZET

ZÁRÓ RENDELKEZÉSEK

16. 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.

▼B

17. cikk

Más jogi aktusokkal való kapcsolat

E határozat rendelkezései nem érintik az (EU, Euratom) 2015/443 határozatot, az (EU, Euratom) 2015/444 határozatot, a 45/2001/EK európai parlamenti és tanácsi rendeletet, az 1049/2001/EK európai parlamenti és tanácsi rendeletet ([1]), a 2002/47/EK, ESZAK, Euratom bizottsági határozatot ([2]), a 883/2013/EU, Euratom európai parlamenti és tanácsi rendeletet ([3]) és az 1999/352/EK, ESZAK, Euratom határozatot.

18. cikk

Hatályon kívül helyezés és átmeneti intézkedések

A 2006. augusztus 16-i C(2006) 3602 határozat hatályát veszti.

Amennyiben nem ellentétesek e határozat rendelkezéseivel, a C(2006) 3602 határozat 10. cikke alapján elfogadott végrehajtási szabályok és informatikai biztonsági előírások mindaddig hatályban maradnak, amíg az e határozat 13. cikke alapján elfogadandó végrehajtási szabályok és előírások a helyükbe nem lépnek. A C(2006) 3602 határozat 10. cikkére történő bármilyen hivatkozást e rendelet 13. cikkére történő hivatkozásként kell értelmezni.

19. cikk

Hatálybalépés

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

([1]) Az Európai Parlament és a Tanács 2001. május 30-i 1049/2001/EK rendelete az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről (HL L 145., 2001.5.31., 43. o.).

([2]) A Bizottság 2002. január 23-i 2002/47/EK, ESZAK, Euratom határozata eljárási szabályzatának módosításáról (az értesítés a C(2002)99. számú dokumentummal történt) (HL L 21., 2002.1.24., 23. o.).

([3]) Az Európai Parlament és a Tanács 2013. szeptember 11-i 883/2013/EU, Euratom rendelete az Európai Csalás Elleni Hivatal (OLAF) által lefolytatott vizsgálatokról, valamint az 1073/1999/EK európai parlamenti és tanácsi rendelet és az 1074/1999/Euratom tanácsi rendelet hatályon kívül helyezéséről (HL L 248., 2013.9.18., 1. o.).