HIVATALOS ÉRTESÍTŐ

60. szám

A MAGYAR KÖZLÖNY MELLÉKLETE
2019. november 8., péntek

Tartalomjegyzék

I. Utasítások

II. Nemzetközi szerződésekkel kapcsolatos közlemények

III. Közlemények

I. Utasítások

A miniszterelnök kabinetfőnöke 7/2019. (XI. 8.) MK utasítása a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 5/2018. (XI. 30.) MK utasítás módosításáról

A kormányzati igazgatásról szóló 2018. évi CXXV. törvény 19. § (3) bekezdésében meghatározott hatáskörömben eljárva – a jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontjára figyelemmel – a következő utasítást adom ki:

1. § A Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 5/2018. (XI. 30.) MK utasítás 1. melléklete (a továbbiakban: SZMSZ) az 1. melléklet szerint módosul.

2. § Ez az utasítás a közzétételét követő napon lép hatályba.

Rogán Antal s. k.,
a miniszterelnök kabinetfőnöke

Jóváhagyom:

Orbán Viktor s. k.,
miniszterelnök

1. melléklet a 7/2019. (XI. 8.) MK utasításhoz

1. § Az SZMSZ 6. §-a a következő (6a) bekezdéssel egészül ki:
„(6a) A minisztert az Országgyűlés munkájával összefüggő miniszteri hatáskörök gyakorlása tekintetében a miniszter és a parlamenti államtitkár együttes akadályoztatása vagy távolléte esetén a nemzetközi kommunikációért és kapcsolatokért felelős államtitkár helyettesíti.”

A büntetés-végrehajtás országos parancsnokának 15/2019. (XI. 8.) BVOP utasítása a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról

A jogalkotásról szóló 2010. évi CXXX. törvény 23. § (4) bekezdés c) pontja, továbbá az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdés f) pontja alapján, a büntetés-végrehajtás elektronikus információs rendszereinek védelme érdekében a következő utasítást adom ki:

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Hatály

1. Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) hatálya a Büntetés-végrehajtás Országos Parancsnokságára (a továbbiakban: BVOP), a büntetés-végrehajtási intézetekre és intézményekre, a fogvatartottak kötelező foglalkoztatására létrehozott gazdasági társaságokra (a továbbiakban: bv. szerv) (a továbbiakban együtt: bv. szervezet), valamint ezek személyi állományára terjed ki.
2. Az IBSZ rendelkezéseit a BVOP-val vagy a bv. szervvel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és egyéb szervezetek (a továbbiakban: külső támogatók) vonatkozásában is érvényesíteni kell. Ennek érdekében biztosítani kell, hogy a külső támogatók az IBSZ-t vagy annak kivonatát megismerjék, amelynek megtörténtét a BVOP-val vagy a bv. szervvel szerződő külső támogató a szerződés aláírásával igazolja. E körben Az informatikai tárgyú szerződéses jogviszonyokra vonatkozó rendelkezések fejezetben foglaltakra is figyelemmel kell lenni.
3. Az IBSZ tárgyi hatálya kiterjed
   a) a bv. szervezet működése során használt elektronikus információs rendszerekre (a továbbiakban: rendszer), rendszerelemekre, infokommunikációs eszközökre, adathordozókra és a rendszerekben kezelt, feldolgozott, tárolt adatokra,
   b) az előzőekben felsoroltakkal kapcsolatos felhasználói, infokommunikációs és információbiztonsági tevékenységre, továbbá
   c) a fentiek működési környezetére.
4. A bv. szervezet által kezelt minősített adatokra, valamint az azokat kezelő, feldolgozó, tároló rendszerekre, rendszerelemekre, infokommunikációs eszközökre és adathordozókra vonatkozó előírásokat a büntetés-végrehajtási szervezet minősített adatainak Biztonsági Szabályzatának kiadásáról szóló 39/2016. (IX. 1.) OP szakutasítás tartalmazza.

2. Az IBSZ célja

5. Az IBSZ célja a bv. szervezet működése során használt rendszerek rendeltetésszerű működését és biztonságát garantáló előírások és eljárások egységes, magas szintű szabályozási keretbe foglalása a rendszerek sértetlensége és rendelkezésre állása, valamint az rendszerekben kezelt, feldolgozott, tárolt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosításához szükséges intézkedések meghatározása érdekében.
6. Az IBSZ a fenti cél teljesülése érdekében rögzíti a rendszerekre és a rendszerekkel kapcsolatos tevékenységekre vonatkozó adminisztratív, fizikai és logikai követelmények teljesítésével összefüggő feladatokat, folyamatokat és felelősségeket.

3. Értelmező rendelkezések

7. Az IBSZ alkalmazása során:
   a) *adatgazda:* az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) alapján a BVOP azon szervezeti egységének a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik, az adatgazda egyben a rendszer működtetéséért felelős személy;
   b) *archiválás:* speciális mentési eljárás, amelynek során az adatokat, adatállományokat a rendszerből törlik, és a rendszertől független adathordozóra, adattárolóra helyezik át, célja a napi tevékenység során már nem szükséges, de megőrzendő adatok, adatállományok biztonságos, hosszú távú, visszakereshető formában történő tárolásának biztosítása;

c) *biztonsági esemény:* az Ibtv. alapján nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

d) *informatikai szakterület:* a BVOP Informatikai Főosztálya (a továbbiakban: INFO) és a bv. szerv informatikai feladatokat ellátó szervezeti egysége vagy munkatársa;

e) *elektronikus információs rendszer biztonságáért felelős személy (a továbbiakban: IBF):* az Ibtv. 11. § (1) bekezdés c) alpontja szerinti személy;

f) *felhasználó:* az Ibtv. alapján a rendszert igénybe vevő személy;

g) *gépterem:* a rendszer központi rendszerelemeit befogadó, speciális üzemeltetési és védelmi feltételeket, működési környezetet biztosító helyiség vagy helyiségcsoport, amelyben a tevékenységek végzése is speciális szabályokhoz kötött;

h) *gépterem-üzemeltetés:* a gépterem mint fizikai létesítmény és az abban üzemeltetett rendszerek (infrastruktúra) fizikai működésének biztosítása; a létesítménymenedzsment a fizikai környezet minden vonatkozására kiterjed (pl. áramellátás, hűtés, belépés ellenőrzése stb.);

i) *hálózati tárhely:* hálózatban működő szervereken létrehozott, többszintű hierarchiába szervezett elektronikus tárolókból álló háttérkapacitás;

j) *jogosultság:* elemi jogok halmaza, amely a rendszerben meghatározott tevékenységek ellátásához szükséges (adatokra, adatállományokra, informatikai objektumokra irányuló hozzáférési vagy végrehajtási jog: olvasás, írás, módosítás, törlés, aktivitás kezdeményezése, döntés munkafolyamat továbbviteléről stb.); a jogosultság lehet lekérdező, amely az olvasási elemi jogot tartalmazza, ügyintéző, amely az elemi jogok bármelyikét tartalmazhatja, beleértve a munkafolyamatok továbbvitelére vonatkozó döntési jogot is;

k) *jogosultságkezelés:* a tevékenységhez szükséges jogosultságok szervezeti egység, szakterület vezetője általi igénylése, engedélyezése, felülvizsgálata, visszavonása, továbbá a jogosultságadminisztrátor általi technikai kialakítása, beállítása, törlése, nyilvántartása;

l) *jogosultság-nyilvántartás:* a felhasználók részére igényelt, engedélyezett és beállított, továbbá törölt jogosultságok egységes szempontok szerinti nyilvántartása, amely a felülvizsgálat és az ellenőrzés kiindulópontjaként is szolgál;

m) *katasztrófaterv (DRP, disaster recovery plan):* a szolgáltatások és/vagy rendszerek működő állapotának visszaállításához, ezen túlmenően gyakran az érintett rendszerekben tárolt adatok visszaállításához szükséges lépéseket is tartalmazó dokumentum;

n) *mentés:* biztonsági másolat készítése a rendszerben tárolt adatokról, adatállományokról, illetve a rendszerben használt alkalmazásokról, célja az adatok, adatállományok helyreállíthatóságának biztosítása az elsődleges adattároló megsérülése esetére;

o) *mobil adathordozó:* elektronikus adatok tárolására szolgáló eszköz, különösen: CD/DVD/BD-lemez, pendrive, eSATA, mágnesszalagos adattároló, merevlemez, okostelefon, tablet, digitális fényképezőgép/videókamera belső memóriája, külső memóriakártyája;

p) *napló:* a rendszerben bekövetkező eseményeket, felhasználói és adminisztrátori tevékenységeket, továbbá ezek időpontját rögzítő, a rendszer által automatikusan létrehozott adatállomány, amely a változások észlelését és a számonkérhetőséget biztosítja;

q) *naplózás:* a rendszerben bekövetkező események, a rendszerben végrehajtott tevékenységek, továbbá ezek időpontjának automatikus rögzítése a változások észlelése és a számonkérhetőség biztosítása érdekében;

r) *privilegizált felhasználó:* a felhasználói jogosultságot meghaladó, jellemzően meghatározott szerepkört (adminisztrátor, rendszergazda, root, superuser stb.) betöltő személyeknek biztosított speciális jogosultság, amellyel rendelkezve a rendszer- és adathozzáférés, a különböző aktivitások kezdeményezése és a további hozzáférési jogosultságok beállítása vagy törlése a rendszer működése, valamint a rendszer és az abban kezelt, feldolgozott és tárolt adatok biztonsága szempontjából kiemelt jelentőségű;

s) *privilegizált jogosultság:* a felhasználói jogosultságot meghaladó, jellemzően meghatározott szerepkört (adminisztrátor, rendszergazda, root, superuser stb.) betöltő személyeknek biztosított speciális jogosultság, amellyel rendelkezve a rendszer- és adathozzáférés, a különböző aktivitások kezdeményezése és a további hozzáférési jogosultságok beállítása vagy törlése a rendszer működése, valamint a rendszer és az abban kezelt, feldolgozott és tárolt adatok biztonsága szempontjából kiemelt jelentőségű;

t) *rendszerdokumentáció:* a rendszer üzemeltetésével összefüggő, infokommunikációs szakmai és információbiztonsági előírásokat, folyamatokat, feladatokat, feladatköröket és felelősségeket rögzítő

dokumentumok összessége, amelynek intraneten kialakított Dokumentumtárában történő őrzéséről, az érintettek számára elérhetővé tételéről és folyamatos frissítéséről az INFO gondoskodik;

u) *távoli hozzáférés:* a bv. szervezet által üzemeltetett rendszerhez nem a bv. szervezet által felügyelt hálózaton keresztül, a bv. szervezet által felügyelt eszközön, VPN kliens használatával megvalósított üzemeltetési, tesztelési, fejlesztési, illetve felhasználói célú hozzáférés;

v) *üzletmenet-folytonossági terv (business continuity plan) (a továbbiakban: BCP):* az üzleti folyamatok megszakadását követően azok helyreállításának lépéseit meghatározó dokumentum, amely tartalmazza az elindítását kiváltó eseményeket, a bevonandó személyeket, a kommunikáció módját stb.

II. A SZABÁLYOZÁS ALAPELVEI, RENDSZERE

4. Alapelvek

8. A rendszerekkel, infokommunikációs eszközökkel és adathordozókkal kapcsolatos fejlesztői, üzemeltetői, biztonsági, továbbá felhasználói tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, üzemeltetési és védelmi előírásokat úgy kell meghatározni és dokumentálni, hogy azok a biztonsági osztályozási előírások figyelembevételével garantálják az információbiztonság szükséges és elégséges szintjét.
9. Kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.
10. A fenti tevékenységek szabályozását úgy kell kialakítani, hogy a tevékenységek megtervezéséért és végrehajtásáért való felelősséget minden esetben meg lehessen állapítani.

5. A szabályozás rendszere

11. Az információbiztonsági szabályozás alapdokumentuma az IBSZ, amely átfogóan és keretjelleggel szabályozza az információbiztonsági szempontból releváns kérdéseket, területeket.
12. Az IBSZ előkészítéséért, kiadmányozásra felterjesztéséért – az INFO vezetőjével együttműködve – az IBF felelős.
13. Az IBSZ-t minden év február 28-áig – dokumentáltan – felül kell vizsgálni, szükség szerint aktualizálni kell. Az IBSZ-t aktualizálni kell különösen, ha a jogszabályi környezet megváltozik, továbbá ha a bv. szervezet informatikai biztonságát, illetve az IBSZ tartalmát érintő jelentős változás következik be.
14. A felülvizsgálat, aktualizálás elvégzéséért az IBF – az INFO vezetője bevonásával – felelős.
15. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: BM rendelet) foglalt részletes eljárásrendeket az Informatikai Biztonsági Kézikönyv (a továbbiakban: IBK) tartalmazza.
16. Az IBK-t az INFO készíti el az IBF közreműködésével, és az országos parancsnok gazdasági és informatikai helyettese hagyja jóvá.
17. A szabályozás egységességének biztosítása érdekében az információbiztonsági tárgykört érintő szabályozó eszközök tervezetét az IBF-nek és az INFO vezetőjének, az informatikai tárgykört érintő szabályozó eszközök tervezetét az INFO vezetőjének véleményezésre meg kell küldeni.
18. Az informatikai szakterületi munkafolyamatok leírását, valamint a rendszerekre vonatkozó speciális tartalmat a rendszerdokumentáció tartalmazza.
19. A szabályozó eszközök kidolgozására vonatkozó részletes előírásokat a büntetés-végrehajtási szervezet belső szabályozási tevékenységéről szóló 2/2013. (IX. 13.) BVOP utasítás tartalmazza.

6. A bv. szervezet biztonsági szintje

20. A BM rendelet 2. melléklete szerint a BVOP biztonsági szintje 4-es. A BM rendelet 2. melléklete szerint a bv. szerv biztonsági szintje 2-es, tekintettel arra, hogy a bv. szerv önállóan nem fejleszt és üzemeltet rendszert.
21. A biztonsági szintet az informatikai szakmai és a funkcionális területek adatai alapján az IBF és az INFO vezetője állapítja meg, és az országos parancsnok az IBSZ kiadmányozásával hagyja jóvá.
22. Amennyiben a bv. szervezet biztonsági szintjének meghatározását befolyásoló körülményekben, feltételekben változás következik be, a biztonsági szint megállapítását soron kívül ismételten el kell végezni. A biztonsági szintbe

sorolással összefüggő körülményeket, feltételeket és megállapításokat az IBSZ felülvizsgálata során is értékelni, szükség esetén módosítani kell.

7. A rendszerek biztonsági osztályba sorolása

23. A bv. szervezet működése során használt, a bv. szervezet mint adatkezelő ellenőrzése alatt álló, az Ibtv. hatálya alá tartozó rendszerek biztonsági osztályba sorolására Az adatgazda részben foglaltak irányadók.
24. Amennyiben a bv. szervezet mint adatkezelő ellenőrzése alatt álló, az Ibtv. hatálya alá tartozó rendszerek osztályba sorolását befolyásoló körülményekben, feltételekben változás következik be, a biztonsági osztályba sorolást soron kívül ismételten el kell végezni. A biztonsági osztályba sorolással összefüggő körülményeket, feltételeket és megállapításokat az IBSZ felülvizsgálata során is értékelni, szükség esetén módosítani kell.
25. Az egyes rendszerek biztonsági osztályba sorolását – az Ibtv. 8. § (1) bekezdése szerint – legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.
26. Az egyes rendszerek biztonsági osztályba sorolására vonatkozó adatokat az EIR-alapnyilvántartás tartalmazza, amelyet az INFO az IBF közreműködésével állít össze. Az EIR-alapnyilvántartás intraneten történő közzététele az INFO feladata. Az EIR-alapnyilvántartás – a rendszer nyilvántartás szerinti sorszámát, besorolási osztályát, speciális minősítését tartalmazó – kivonata az IBSZ 1. melléklete.
27. A biztonsági osztályba sorolással összefüggésben elvégzendő feladatokat tartalmazó Cselekvési tervet az INFO készíti el és tartja nyilván, teljesülését nyomon követi, és elérhetővé teszi az érintettek számára.

8. Információbiztonsági kockázatfelmérés és -kezelés

28. A bv. szervezet működése során használt és a bv. szervezet mint adatkezelő ellenőrzése alatt álló, az Ibtv. hatálya alá tartozó rendszerek esetében megfelelő kockázatkezelési rendszerről gondoskodni kell. A kockázatkezelési rendszert az INFO – az IBF bevonásával – működteti.
29. Az információbiztonsági kockázatkezelési rendszer magában foglalja a kockázatok felmérését, elemzését és szükség esetén az intézkedési terv alapján történő kezelését.
30. A bv. szervezet valamennyi elektronikus információs rendszeréről az EIR-alapnyilvántartást kell vezetni.
31. A kockázatfelmérésről – az IBF bevonásával – az INFO vezetője gondoskodik, az EIR-alapnyilvántartásban szereplő adatok alapján, a Nemzeti Elektronikus Információbiztonsági Hatóság honlapján elérhető Osztályba sorolás és védelmi intézkedés űrlap (a továbbiakban: OVI űrlap) kitöltésével.
32. A kockázatfelmérés eredménye alapján a biztonsági osztályba sorolásra vonatkozó javaslatot – az INFO bevonásával – az IBF állítja össze.
33. Amennyiben az OVI űrlapon megfogalmazott követelményeknek nem felel meg teljeskörűen a bv. szervezet, a 27. pontban foglaltak szerint kell eljárni.
34. Az osztályba sorolási javaslatot és hiányosság esetén a Cselekvési tervet az INFO vezetője terjeszti fel jóváhagyásra az országos parancsnok részére.
35. Amennyiben a bv. szervezet mint adatkezelő ellenőrzése alatt álló, az Ibtv. hatálya alá tartozó rendszerekre vonatkozó kockázatkezelést befolyásoló körülményekben, feltételekben változás következik be, a fejezetben foglaltakat soron kívül ismételten el kell végezni. A kockázatkezeléssel összefüggő körülményeket, feltételeket és megállapításokat az IBSZ felülvizsgálata során is értékelni, szükség esetén módosítani kell.

9. Információbiztonsági tervezés, elemzés és értékelés

36. Az információbiztonsági tervezés szervezeti elemeit az INFO vezetője által előkészített és az országos parancsnok által jóváhagyott informatikai fejlesztési dokumentumok tartalmazzák.
37. Az egyes rendszerekre vonatkozó információbiztonsági tervezés keretében az INFO vezetője köteles gondoskodni
    a) a rendszer tervezése, fejlesztése, kivitelezése és módosítása során alkalmazandó biztonságtervezési elvek kidolgozásáról,
    b) a biztonságtervezési elvek megvalósítását biztosító folyamatok kialakításáról és működtetéséről.
38. Új fejlesztések és meglevő rendszereket érintő továbbfejlesztések információbiztonsági elemeinek, alrendszereinek tervezésekor és megvalósításakor az alábbi szempontokat kell kiemelten figyelembe venni:
    a) a vonatkozó jogszabályok és a bv. szervezet által alkalmazott és alkalmazandó szabványok előírásai következetesen és maradéktalanul megvalósításra kerüljenek,

b) a fejlesztések eredményeként önmagukban is teljes rendszerek jöjjenek létre, de mindegyik illeszthető legyen az egységes koncepció alapján felépülő központi biztonsági rendszerhez és szervezetrendszerhez.

39. Meglevő rendszerek továbbfejlesztése során a fenti rendelkezések irányadóak, mind funkcionális továbbfejlesztés vagy rendszerelem-csere, mind információbiztonsági okból (pl. sérülékenység, jogszabályi előírás, így biztonsági osztály módosulása miatt) indokolt fejlesztés esetében is.
40. A dokumentálási követelmények meghatározásakor és teljesítésekor az Adminisztratív biztonsági követelmények és az Informatikai fejlesztések fejezetekben rögzítettekre is figyelemmel kell lenni.
41. A további részletszabályokat az IBK tartalmazza.

10. A védelmi intézkedések

42. A rendszer biztonsági osztályához rendelt védelmi intézkedések tervezése és teljesítése az Ibtv. és végrehajtási rendeletei alapján történik.
43. Az egyes rendszerek esetében a speciális, rendszerszintű védelmi intézkedésekre vonatkozó előírásokat a rendszerdokumentáció tartalmazza.
44. A védelmi intézkedések megfelelőségét rendszeres időközönként – a tervezett belső és külső auditok során, illetve amennyiben szükséges, belső értékelések keretében – felül kell vizsgálni. A felülvizsgálatra az Ellenőrzés és értékelés részben leírtak irányadók.

11. Ellenőrzés és értékelés

45. Az információbiztonsági helyzet és a védelmi intézkedések megfelelőségének ellenőrzése, értékelése érdekében szükséges feladatokat a bv. szervezet vezetői és szervezeti egységei vonatkozásában Az informatikai biztonság szervezete fejezet tartalmazza.
46. Az egyes rendszerek esetében a folyamatba épített ellenőrzésekre vonatkozó előírásokat a rendszerdokumentáció tartalmazza.
47. Az INFO vezetője az általa előterjesztett és az országos parancsnok által jóváhagyott éves ellenőrzési terv alapján, indokolt esetben az országos parancsnok vagy a bv. szerv vezetője által soron kívüli elrendelés alapján hajt végre ellenőrzést. Az ellenőrzésről az ellenőrzött bv. szerv vagy szervezeti egység vezetőjét 30 nappal korábban – az ellenőrzési program megküldésével – írásban tájékoztatni kell, kivéve, ha a tájékoztatás az ellenőrzés eredményességét veszélyeztethetné. Az ellenőrzésről jegyzőkönyvet kell készíteni. Az esetlegesen feltárt hiányosságok felszámolására a jegyzőkönyv elkészítését követő 30 napon belül az ellenőrzött bv. szerv vagy szervezeti egység vezetője – szükség szerint az INFO bevonásával – intézkedési tervet készít. Az intézkedési tervet a jegyzőkönyvhöz csatolni kell. A jegyzőkönyv és az intézkedési terv elkészítése és teljesítése során az ellenőrzést végrehajtó és az ellenőrzött bv. szerv vagy szervezeti egység köteles együttműködni.
48. Az Ellenőrzési Szolgálat által végrehajtandó, információbiztonsági tárgykört érintő ellenőrzésekre vonatkozó előírásokat a büntetés-végrehajtási szervezet szakmai ellenőrzéséről szóló 3/2018. (VI. 4.) BVOP utasítás (a továbbiakban: Szakmai Ellenőrzésről szóló BVOP utasítás) tartalmazza.
49. Az egyes rendszerekre vonatkozó védelmi intézkedések megfelelőségéről független értékelők által végrehajtott ellenőrzésekkel (külső auditok) kell meggyőződni.
50. Külső audit végrehajtására javaslatot tehet az INFO vezetője és az IBF. A külső audit végrehajtását az országos parancsnok engedélyezi vagy rendeli el. A külső auditról – amennyiben azt nem az IBF kezdeményezte – az IBF-et az audit megkezdése előtt tájékoztatni, az auditban az IBF részvételének lehetőségét biztosítani kell. A külső auditok lefolytatására és dokumentálására az előző pontokban foglaltak irányadók. A külső auditok eredeti dokumentumait az INFO őrzi.
51. A külső auditokról az IBF nyilvántartást vezet, amely tartalmazza a külső audit
    a) tárgyát, beleértve az érintett rendszer, szolgáltatás megnevezését is,
    b) időpontját,
    c) végrehajtóját (szervezet megnevezése, munkatársak neve),
    d) végrehajtásában közreműködő szervezeti egység megnevezését és a végrehajtásában közreműködő munkatársak nevét,
    e) végrehajtására vonatkozó szerződés, megállapodás azonosító adatait,
    f) megállapításai számát és tartalmát,

g) megállapításai alapján készített intézkedési terv adatait (azonosító szám, készítő, jóváhagyó, végrehajtási határidők),
h) az intézkedési tervben rögzített feladatok számát és tartalmát,
i) a dokumentumok másolati példányát.

52. A külső auditok során az auditor számára az audit sikeres végrehajtásához szükséges adatok, dokumentumok megismerését (betekintést) biztosítani kell.
53. Az auditor számára dokumentumok átadása (papír alapon vagy elektronikusan) csak átadás-átvételi jegyzőkönyvvel történhet. Közérdekű vagy közérdekből nyilvános, továbbá nyílt adatok, dokumentumsablonok továbbítása e-mailben is történhet.
54. Az auditor számára csak betekintés biztosítható az alábbi adatkörökbe és dokumentumtípusokba (a dokumentumok, adatok nem adhatók át):
    a) a rendszer teljes logikai vagy fizikai rendszerterve,
    b) a privilegizált jogosultságok kezelésére vonatkozó leírás,
    c) konkrét jelszó,
    d) paraméterezési adatok (amennyiben nem gyártó által közzétettek),
    e) telepítési leírás (amennyiben nem gyártó által közzétett),
    f) személyes adatokat tartalmazó adatállomány.
55. Az egyes rendszerek speciális vizsgálataira (pl. sérülékenységvizsgálat, belsőfenyegetettség-értékelés, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskódelemzése stb.) az előző bekezdésekben foglaltak irányadóak.
56. Az ellenőrzések, külső auditok, speciális vizsgálatok eredményeinek bv. szervezet általi hasznosítását elő kell segíteni oly módon is, hogy a vizsgálat kezdeményezője vagy lefolytatója köteles a tapasztalatokat mindazon szervezeti egységekkel/állományi tagokkal megosztani, amelyek/akik esetében a munkavégzés során a tapasztalatok elősegíthetik a védelem hatékonyságának növelését. A tájékoztatást az audit lezárását követő egy hónapon belül végre kell hajtani. A tájékoztatásról az INFO vezetője az IBF bevonásával gondoskodik.
57. Az ellenőrzések, külső auditok, speciális vizsgálatok eredményeinek bv. szervezet általi hasznosítását és hasznosulását Az informatikai biztonság szervezete fejezetben rögzített éves informatikai biztonsági beszámolóban értékelni kell.
58. A biztonsági teljesítmény mérésének rendszerét az INFO az IBF bevonásával alakítja ki és működteti.

III. AZ INFORMATIKAI BIZTONSÁG SZERVEZETE

12. Az országos parancsnok

59. Az országos parancsnok
    a) felelős a bv. szervezet informatikai tevékenységének jogszerűségért, beleértve az informatikai biztonsági tevékenységet,
    b) gondoskodik az informatikai biztonság személyi és tárgyi feltételeinek biztosításáról,
    c) gondoskodik – szabályozás és ellenőrzés útján – az Ibtv.-ben és a kapcsolódó jogszabályokban előírt, információbiztonsággal összefüggő tevékenységek végrehajtásáról,
    d) minden év július 31-éig beszámoltatja az IBF-et és az INFO vezetőjét a bv. szervezet informatikai biztonsági helyzetéről.

13. Az IBF

60. Az IBF az Ibtv. 13. §-a alapján
    a) gondoskodik a bv. szervezet rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
    b) elvégzi, irányítja, illetve felügyeli az előző alpont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
    c) az INFO vezetőjének bevonásával előkészíti az IBSZ-t, gondoskodik naprakészen tartásáról, az IBSZ-szel kapcsolatos, központi lebonyolítású képzések, tájékoztatók tananyagának elkészítéséről,
    d) az INFO vezetőjének bevonásával előkészíti a bv. szervezet rendszereinek biztonsági osztályba sorolását és a bv. szervezet biztonsági szintbe történő besorolását,

e) az INFO vezetőjével közösen elkészített éves jelentésben beszámol az országos parancsnoknak a bv. szervezet informatikai biztonsági helyzetéről,
f) véleményezi a rendszerek biztonsága szempontjából a bv. szervezet e tárgykört érintő szabályzatait és szerződéseit,
g) kapcsolatot tart a hatósággal és az INFO vezetőjének útján, illetve bevonásával az eseménykezelő központtal,
h) az INFO vezetőjének bevonásával gondoskodik a bv. szervezet állományi tagjainak információbiztonsági tudatosságát növelő képzések, tájékoztatók elkészítéséről, megtartásáról,
i) gondoskodik – az INFO vezetőjének bevonásával – az Ibtv.-ben meghatározott követelmények teljesüléséről a bv. szervezet valamennyi rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők rendszereket érintő, biztonsággal összefüggő tevékenysége esetén,
j) együttműködik az INFO vezetőjével az információbiztonsági feladatok ellátásában,
k) jogosult az érintettektől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni, adatot bekérni, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot megismerni.

14. Az INFO vezetője

61. Az INFO vezetője
a) felelős a bv. szervezet által üzemeltetett vagy fejlesztett rendszerek jogszerű és szakszerű működéséért, a rendszerekre vonatkozó informatikai szakmai és információbiztonsági előírások teljesítéséért, a hatályos szabályozó eszközök és a bevált gyakorlatok érvényesítéséért,
b) folyamatba épített ellenőrzéssel gondoskodik az informatikai szakmai és az információvédelmi előírásoknak megfelelő működés biztosításáról,
c) kezdeményezi a bv. szervezet rendszereivel összefüggő informatikai szakmai és információbiztonsági intézkedéseket, beszerzéseket, illetve közreműködik azok végrehajtásában,
d) gondoskodik – az IBF bevonásával – a bv. szervezet rendszereivel összefüggő szabályozási, nyilvántartási feladatok ellátásáról,
e) közreműködik a bv. szervezet rendszereivel összefüggő ellenőrzésekben, auditokban, sérülékenységvizsgálatokban,
f) együttműködik az IBF-fel az információbiztonsági feladatok ellátásában.

15. Az INFO munkatársai

62. Az INFO munkatársai ellátják az INFO vezetője által számukra meghatározott információbiztonsági feladatokat.

16. A bv. szerv informatikai szakterületének vezetője

63. A bv. szerv informatikai szakterületének vezetője felelős a bv. szerv által üzemeltetett rendszerek biztonságáért és rendelkezésre állásáért.
64. A bv. szerv informatikai szakterületének vezetője felelős az IBSZ-ben, valamint az IBK-ban meghatározott, a bv. szervre vonatkozó előírások betartásáért és betartatásáért.

17. A bv. szerv informatikai szakterületének munkatársai

65. A bv. szerv szakterületi vezetőjének utasítása alapján végrehajtják az IBSZ-ben és IBK-ban meghatározott feladatokat, ennek keretében figyelemmel kísérik a bv. szerv informatikai rendszereinek működését.

18. A Biztonsági Szolgálat vezetője

66. A Biztonsági Szolgálat vezetője felelős a bv. szervezet által fejlesztett és üzemeltetett rendszerekre vonatkozó személy- és fizikai biztonsági – objektumvédelmi – követelmények meghatározásáért, teljesítéséért és teljesítésük ellenőrzésért, együttműködve az INFO vezetőjével.

19. A bv. szerv és szervezeti egységeinek vezetői

67. A bv. szerv és szervezeti egységeinek vezetői
    a) felelősek az irányításuk, vezetésük alá tartozó bv. szerv, illetve szervezeti egységek informatikai biztonsággal összefüggő tevékenységének jogszerűségéért, az IBSZ-ben foglaltak végrehajtásáért,
    b) gondoskodnak az irányításuk alá tartozó szervezeti egységek feladatkörébe tartozó nyilvántartások vezetéséről és naprakészen tartásáról, különös tekintettel a jogszabályokban és az IBSZ-ben előírt nyilvántartásokra,
    c) kötelesek – hatáskörük keretein belül – az IBF és az INFO vezetőjének írásbeli megkeresésére az informatikai biztonsággal összefüggő, szükséges intézkedéseket megtenni, és a megtett intézkedésekről a megkeresőt 15 napon belül tájékoztatni.

20. Az adatgazda

68. Az adatgazda
    a) ellátja az Ibtv.-ben és a kapcsolódó jogszabályokban meghatározott adatgazdai feladatokat,
    b) felelős a rendszer használatára vonatkozó szakmai szabályok meghatározásáért és írásbeli rögzítéséért, beleértve az üzletmenet-folytonosság biztosításával kapcsolatos – hatáskörébe tartozó – tervezési és szabályozási feladatokat is,
    c) felelős a rendszer biztonsági osztályának meghatározásához szükséges adatok és információk biztosításáért és naprakészen tartásáért,
    d) ellátja a rendszer használatához szükséges jogosultságok kezelésével kapcsolatos, számára meghatározott – irányítói – feladatokat,
    e) meghatározza a rendszer által kezelt, feldogozott, tárolt adatok körét, típusát, őrzési idejét,
    f) javaslatot tesz a rendszer fejlesztésére, módosítására, kivonására.

IV. AZ INFORMATIKAI BIZTONSÁG VESZÉLYEZTETÉSE, MEGSÉRTÉSE

69. Az IBSZ, a vonatkozó jogszabályok, szabályozó eszközök rendelkezéseinek be nem tartása, valamint az informatikai biztonság veszélyeztetése, megsértése esetén a munkatárssal szemben fegyelmi, illetve büntetőjogi felelősségre vonásnak van helye a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény (a továbbiakban: Hszt.) és a belügyminiszter irányítása alatt álló fegyveres szervek hivatásos állományú tagjai Fegyelmi Szabályzatáról szóló 11/2006. (III. 14.) BM rendelet alapján.
70. Az informatikai biztonsági előírások be nem tartásával okozott kárért való felelősségre vonatkozó rendelkezéseket a Hszt. és a belügyminiszter irányítása alatt álló fegyveres szervek és hivatásos állományú tagjainak kártérítési felelősségéről szóló 23/1997. (III. 19.) BM rendelet tartalmazza.
71. Az informatikai biztonsági előírások megsértése esetén alkalmazandó eljárásra és jogkövetkezményekre vonatkozó rendelkezéseket a BVOP vagy a bv. szerv által kötendő szerződésben rögzíteni kell.

V. SZERVEZETI BIZTONSÁGI KÖVETELMÉNYEK

21. Összeférhetetlen szerepkörök és feladatok szétválasztása

72. Az informatikai és az informatikai biztonsági feladatokat ellátó szervezeti egységek (informatikai szakterületek), személyek (IBF) szervezeti szintű szétválasztása a jelenlegi struktúra szerint biztosított.
73. Az informatikai szerepkörök és feladatok szervezeti egységre és személyre (véglegesen vagy átmeneti időszakra történő) telepítését úgy kell végrehajtani, hogy a fejlesztési, üzemeltetési, ellenőrzési feladatok ellátásának egymástól való függetlensége biztosított legyen.

22. Helyettesítés

74. Az informatikai és az informatikai biztonsági szerepkörök és feladatok személyre telepítésekor a közvetlen vezető köteles gondoskodni a helyettesítésről.

VI. SZEMÉLYI BIZTONSÁGI KÖVETELMÉNYEK

23. Általános rendelkezések

75. A munkatársakkal, külső támogatókkal szemben támasztott általános követelményeket a munkaerővel és személyi juttatással történő gazdálkodásról, valamint a személyi juttatások kifizetésével kapcsolatos adatszolgáltatásról szóló 45/2017. (IV. 7.) OP szakutasítás, a büntetés-végrehajtási szervezet Biztonsági Szabályzatának kiadásáról szóló 26/2015. (III. 31.) OP szakutasítás (a továbbiakban: Biztonsági Szabályzat), továbbá a büntetés-végrehajtási szervek területére történő be- és kilépés, valamint a bv. szervek területén tartózkodás részletes szabályairól szóló 56/2017. (VII. 14.) OP szakutasítása tartalmazza.
76. A szabályozás kiterjed a munkavégzésre irányuló jogviszony létesítését megelőző időszakra, a jogviszony fennállásának időszakára és a jogviszony megszűnését követő időszakra is.
77. A nemzetbiztonsági ellenőrzés alá eső munkaköröket a belügyminiszter feladat- és hatáskörét érintően a nemzetbiztonsági ellenőrzés alá eső személyek meghatározásáról szóló 15/2015. (IV. 10.) BM rendelet határozza meg. A kapcsolódó feladatokat a személyügyi szakterületek látják el.
78. A vagyonnyilatkozat-tételi kötelezettség teljesítésével kapcsolatos feladatokat a vagyonnyilatkozat-tételi kötelezettségről szóló 2007. évi CLII. törvény alapján a személyügyi szakterületek látják el.
79. Az IBSZ személyi hatálya alá tartozókkal szemben érvényesíteni kell a jogviszony megszűnése vagy megváltozása utáni időszakra vonatkozó titoktartási megállapodások megszegésének jogkövetkezményeit.

24. Információbiztonsági képzés, továbbképzés

80. A bv. szervezet munkatársait a bv. szervezetnél végzendő tevékenység megkezdése előtt az IBSZ tartalmára épülő, az informatikai biztonsági események jelentési kötelezettségére is figyelmeztető, továbbá az információbiztonsági tudatosság növelését is célzó információbiztonsági képzésben kell részesíteni.
81. Az előzőeken túl az információbiztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá, ha a bv. szervezet informatikai biztonságát, illetve az IBSZ tartalmát érintő jelentős változás következik be, a jogszabályváltozás hatálybalépését, illetve a jelentős változást követő 60 napon belül a munkatársakat információbiztonsági továbbképzésben kell részesíteni.
82. A külső támogatókat információbiztonsági tájékoztatásban kell részesíteni.
83. A képzés, továbbképzés, tájékoztatás tematikájának, tananyagának összeállításáért az IBF felelős, aki e feladatait az INFO vezetőjének bevonásával végzi.
84. A képzés, továbbképzés lebonyolításáért a személyügyi szakterület vezetője, a tájékoztatás megtartásáért a külső támogatót fogadó szervezeti egység vezetője felelős.
85. Az érintettek a Nyilatkozat (2. vagy 3. melléklet) aláírásával igazolják, hogy a képzésen, továbbképzésen, illetve tájékoztatáson részt vettek, az információbiztonsági előírásokat megismerték, és azok betartását magukra nézve kötelezőnek ismerik el. A nyilatkozatot a bv. szervezet munkatársai esetében a haladási napló mellékleteként, külső támogatók esetében a szerződéssel együtt kell őrizni. A nyilatkozat – amennyiben erre a lehetőség biztosított – elektronikus úton is megtehető.
86. A munkatársak és a külső támogatók a rendszerekhez hozzáférést csak a képzésen, illetve tájékoztatáson való részvétel és a Nyilatkozat aláírása után kaphatnak.
87. Az informatikus munkakört, szerepkört, feladatkört ellátó munkatársak képzéséről, továbbképzéséről az INFO vezetője gondoskodik a rendelkezésre álló erőforrások függvényében.
88. A bv. szervezet rendszeres képzésben részesít minden felhasználót, amelyet minden évben két alkalommal, az első félévben március 31-éig, a második félévben szeptember 30-áig kell végrehajtani. Az oktatás részévé kell tenni a Belügyminisztérium és a belügyminiszter által irányított szervek elektronikus információbiztonsággal összefüggő biztonságtudatos viselkedési kódexe kiadásáról szóló 17/2019. (VIII. 15.) BM utasítás 1. mellékletében szereplő biztonságtudatos viselkedési kódexet.
89. A képzésre vonatkozó részletes szabályokat a büntetés-végrehajtási szakmai oktatás és vizsgáztatás rendszeréről szóló 25/2016. (VII. 4.) OP szakutasítás tartalmazza.

25. Informatikai biztonsági feladatok és felelősségek meghatározása

90. Az informatikai biztonsággal kapcsolatos
    a) szervezeti szintű feladatokat és felelősségeket az IBSZ,
    b) szakterületi, illetve az egyes rendszerekkel összefüggő feladatokat és felelősségeket az IBSZ figyelembevételével kiadott szabályozó eszköz, felhasználói kézikönyv, rendszerdokumentáció,
    c) egyéni feladatokat és felelősségeket a munkaköri leírások
    tartalmazzák.
91. Külső támogató esetében az informatikai biztonsággal kapcsolatos egyéni feladatokat és felelősségeket a vonatkozó szerződésben és mellékleteiben kell meghatározni.
92. Az előző pontban foglaltak rögzítéséért, aktualizálásáért és végrehajtásáért az INFO vezetője felelős.

26. A szervezeti egység vezetőjének jogai és kötelezettségei

93. A szervezeti egység vezetője jogosult és köteles az irányítása alá tartozó személyek munkavégzéséhez szükséges infokommunikációs eszközök, valamint a használandó rendszerek és azokhoz szükséges jogosultságok körét meghatározni, továbbá az előzőek biztosításához szükséges engedélyezési eljárásokat kezdeményezni, illetve lefolytatni.
94. A szervezeti egység vezetője köteles az előző bekezdésben foglalt, rendszer-, eszköz- és jogosultság-használatok indokoltságát évente egyszer – az INFO által biztosított adatok alapján – írásban dokumentált módon, a hatályos szabályozó eszközök alapján felülvizsgálni és indokolt esetben a kiadott engedélyek módosítása vagy visszavonása érdekében szükséges intézkedéseket megtenni.
95. A szervezeti egység vezetője köteles gondoskodni az irányítása alá tartozó személyek informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ szükséges mértékű ismeretét is.
96. A szervezeti egység vezetője az informatikai biztonsági előírások megsértésének észlelése esetén köteles
    a) azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,
    b) amennyiben meghatározható rendszerre korlátozódik a biztonsági előírások megsértése, az adatgazdával való egyeztetést követően indokolt esetben kezdeményezni a rendszer használatának felfüggesztését, illetve üzemszüneti eljárásrend bevezetését,
    c) kivizsgáltatni az informatikai biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,
    d) a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni,
    e) értesíteni az INFO vezetőjét, és tájékoztatni az IBF-et.

27. A felhasználó jogai és kötelezettségei

97. A felhasználó jogosult a munkavégzéshez szükséges infokommunikációs eszközöket használni, a használatukhoz szükséges ismereteket dokumentáció vagy képzés formájában megkapni.
98. A felhasználó a rendelkezésére bocsátott infokommunikációs eszközöket csak a bv. szervezet céljaival, feladataival kapcsolatos, a munkaköri feladatai ellátásához szükséges tevékenység céljára, rendeltetésszerűen, a számára megállapított jogosultságok keretein belül, a jogszabályokkal és a szabályozó eszközökkel összhangban, rendeltetésszerűen használhatja.
99. A felhasználó köteles a használatra átvett informatikai eszközöket az elvárható gondossággal kezelni, és a károsodásoktól védeni.
100. A felhasználó személyes anyagi felelősséggel tartozik az általa szándékosan vagy gondatlanságból az infokommunikációs eszközökben okozott, bizonyított károkért.
101. A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tevékenységért, tranzakcióért a bejelentkezéstől a kijelentkezésig a felhasználó (távoli segítségnyújtás esetében a segítségnyújtó, vezérlést átvevő személy) felelős.
102. Ez a felelősség akkor is fennáll, ha a tevékenységet, tranzakciót harmadik személy hajtotta végre, amennyiben erre az IBSZ előírásainak felhasználó általi be nem tartása miatt került sor.
103. A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, illetve ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni, vagy azt kikapcsolni, amennyiben azt

felügyelet nélkül hagyja. A munkaállomást a munkaidő végén vagy a munkavégzés befejezésekor – eltérő rendelkezés hiányában – ki kell kapcsolni.

104. Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, a felhasználói fiókból és az azonosított kapcsolatból is kijelentkezett.
105. Közös használatú hálózati nyomtató esetében a felhasználó a kinyomtatott dokumentumot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.
106. A felhasználó a rendelkezésére bocsátott mobil infokommunikációs eszközöket és adathordozókat köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.
107. A felhasználó köteles az általa észlelt informatikai biztonsági eseményről vagy annak bekövetkezési lehetőségéről értesíteni közvetlen vezetőjét, aki gondoskodik a szükséges intézkedések megtételére.
108. A felhasználó – amennyiben az INFO vezetője másként nem rendelkezik – köteles az informatikai rendszer általa észlelt rendeltetésellenes működését a közvetlen elöljárója részére haladéktalanul jelenteni.

28. A privilegizált jogosultsággal rendelkező munkatárs jogai és kötelezettségei

109. A privilegizált jogosultsággal rendelkező munkatárs a felhasználói jogosultságokon túlmutató többletjogosultságait csak a jogszabályokkal és a szabályozó eszközökkel összhangban, rendeltetésszerűen, a munkaköri leírásában foglalt feladatok ellátásához használhatja.

29. A külső támogatókra vonatkozó rendelkezések

110. A rendszerekhez és az infokommunikációs eszközökhöz külső támogató csak szerződés alapján, a szerződésben foglalt keretek között, dokumentáltan férhet hozzá.
111. A rendszerekhez és az infokommunikációs eszközökhöz hozzáférő külső támogató egyedileg, írásban köteles nyilatkozni arról, hogy az IBSZ-ben foglaltakat megismerte, és magára nézve kötelezőnek ismeri el.
112. A külső támogatókra az általuk betöltött szerepkörre, feladatkörre vonatkozó előírások értelemszerűen irányadóak.

VII. ADMINISZTRATÍV BIZTONSÁGI KÖVETELMÉNYEK

30. Rendszerek dokumentálása

113. A rendszerek teljes életciklusát dokumentálni kell, így a tervezés (követelménymeghatározás), a fejlesztés és a továbbfejlesztés vagy a beszerzés, a tesztelés és az ellenőrzés, az éles indítás/használatbavétel, az üzemeltetés, a fenntartás és a karbantartás, valamint a megszüntetés (kivonás, archiválás, megsemmisítés) fázisait is.
114. A dokumentáció teljességéért és naprakészségéért (folyamatos aktualizálásáért) az INFO vezetője felel.
115. A rendszer dokumentációja akkor teljes, ha tartalmazza a szakmai (funkcionális), az informatikai (műszaki) és az informatikai biztonsági szempontból releváns valamennyi adatot.
116. Az egyes rendszerek esetében elvárt dokumentumok körét és mélységét a jogszabályok előírásainak figyelembevételével a rendszer tervezésekor kell meghatározni, és a rendszer teljes életciklusa alatt folyamatosan frissíteni.
117. A dokumentáció tartalmazza a rendszer által megvalósítandó szakmai funkciókban részt vevő rendszerelemek meghatározását, a szakmai funkció megvalósításának módját mind fizikai, mind logikai szempontból.
118. A dokumentáció tartalmazza a rendszerben alkalmazott biztonsági megoldásokat, beleértve a rendszer egy esetleges részleges vagy teljes körű meghibásodása vagy megsemmisülése esetére kidolgozott eljárásrendet.
119. A rendszerek dokumentációjának őrzéséről, arra jogosultak számára hozzáférhetővé tételéről, továbbá folyamatos aktualizálásáról az INFO vezetője gondoskodik.

31. Tervezési dokumentáció

120. A rendszer tervezése során elkészítendő dokumentációra A fejlesztési folyamat dokumentálása részben foglaltak irányadóak.
121. A tervezési dokumentációra vonatkozó további előírásokat az IBK tartalmazza.

32. Üzemeltetési (adminisztrátori) és felhasználói dokumentáció

122. A rendszer üzemeltetéséhez és használatához szükséges rendszerdokumentációt, így különösen az üzemeltetési leírást és a felhasználói kézikönyvet vagy felhasználói leírást a rendszer üzemeltetésének megkezdése előtt el kell készíteni, és az érintettek számára – jellemzően elektronikus úton – hozzáférhetővé kell tenni. A dokumentáció elkészítésére és aktualizálására a Rendszerek dokumentálása részben foglaltak irányadók.

33. Rendszerek és rendszerelemek nyilvántartása

123. A rendszerek és rendszerelemek nyilvántartását az EIR-alapnyilvántartás tartalmazza. A nyilvántartás kialakításáért és vezetéséért (hitelességéért, pontosságáért és naprakészségéért) az INFO vezetője felelős, aki azt közzéteszi az arra jogosultak számára.
124. Az EIR-alapnyilvántartás az alábbi szakmai adatokat tartalmazza:
    a) rendszer megnevezése,
    b) modul megnevezése,
    c) rendszer (modul) rövid neve,
    d) rendeltetése,
    e) státusza (éles üzemben, kivezetve stb.),
    f) éles működés kezdete,
    g) éles működés vége,
    h) kezelt/feldolgozott adatok köre,
    i) speciális besorolás az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 187/2015. Korm. rend.) 14. § (2) bekezdése alapján (zárt célú),
    j) szakmai működtetésért felelős, adatgazda,
    k) szabályozó eszköz,
    l) felhasználói leírás,
    m) irányadó (konkrét) jogszabály,
    n) adatok őrzési ideje,
    o) hozzáférők köre (bv. szervezet, BVOP, bv. intézetek, bv. intézmények, gazdasági társaságok),
    p) hozzáférő külső szerv,
    q) hozzáférés jogalapja (együttműködési megállapodás/szerződés száma, kelte),
    r) biztonsági osztálya a besorolás alapján,
    s) tényleges biztonsági osztálya a védelmi intézkedések teljesülése alapján,
    t) megjegyzés.
125. Az EIR-alapnyilvántartás az alábbi informatikai adatokat tartalmazza:
    a) fejlesztő/szállító,
    b) üzemeltető,
    c) szerződött karbantartó (ha van), szerződés száma, kelte,
    d) alkalmazás rendszergazda,
    e) infrastruktúra rendszergazda,
    f) kapcsolódó adatkezelő rendszerek,
    g) katasztrófatűrő megoldás,
    h) rendszerdokumentáció megnevezése, elérési helye,
    i) katasztrófa-helyreállítási terv (DRP), elérési helye,
    j) licencszám,
    k) első beszerzés éve,
    l) szerverazonosító,
    m) adatbázis-azonosító, -verzió.
126. Az EIR-alapnyilvántartás szakmai adatai pontosságáért és naprakészségéért a rendszer működtetéséért felelős szervezeti egység, az informatikai adatai pontosságáért és naprakészségéért az INFO felel.
127. A részletes szoftver- és licencnyilvántartást az informatikai szakterület vezeti.

128. A rendszerek és rendszerelemek készlet szerinti nyilvántartását a Forrás.NET rendszer tartalmazza. A készlet szerinti nyilvántartásért a gazdasági szakterület felelős.
129. A készletek kezelésére vonatkozó előírásokat a Büntetés-végrehajtás Országos Parancsnoksága számviteli politikájának kiadásáról szóló 68/2015. (VIII. 27.) OP szakutasítás tartalmazza.

VIII. AZ INFORMATIKAI TÁRGYÚ SZERZŐDÉSES JOGVISZONYOKRA VONATKOZÓ RENDELKEZÉSEK

130. A bv. szervezet informatikai és informatikai biztonsági tárgyú szerződéseit a Regiszter szerződésnyilvántartó programban nyilván kell tartani. A szerződések nyilvántartásáért (hitelességéért, pontosságáért és naprakészségéért) a gazdasági szakterület felelős.
131. Szoftverfejlesztési tevékenységre irányuló szerződésben rendelkezni kell különösen az alábbiakról:
    a) a kellő mélységben kommentezett forráskód átadása a bv. szervezet részére, amennyiben ez nem lehetséges, a forráskód letétbe helyezése,
    b) a szerzői jogi védelem alá eső szoftver esetén a vagyoni jogok a lehető legszélesebb körben átruházásra kerülnek a bv. szervezet részére,
    c) az előző bekezdésben foglaltaktól csak különösen indokolt esetben lehet eltérni azzal, hogy a szerzői jogi védelem alá eső szoftver kizárólagos felhasználási joga a jogszabály által engedett legszélesebb körben a bv. szervezet részére átruházásra kerül.

IX. ÜZLETMENET-FOLYTONOSSÁG BIZTOSÍTÁSA

132. A bv. szervezet által használt rendszerek összeomlása, kompromittálódása vagy hibája esetére a belső folyamatok folytonosságát a BCP-ben rögzített folyamatokkal kell biztosítani. A tervezés és szabályozás a rendszer működtetéséért felelős szervezeti egység és az INFO közös feladata.
133. A BCP-vel kapcsolatos részletszabályokat az IBK tartalmazza.

34. Mentés és archiválás

134. A rendszerekben kezelt, feldolgozott, tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani, amelyet az informatikai szakterület vezetője a Szakmai Ellenőrzésről szóló BVOP utasítás alapján havonta ellenőriz.
135. A rendszerekben kezelt, feldolgozott, tárolt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során már nem szükséges, azonban őrzésük indokolt, archiválni kell.
136. A mentési és archiválási eljárásokat és kapcsolódó feladatok részletszabályait az IBK tartalmazza.
137. Az archivált adatállományokat tároló adathordozókat háromévente dokumentáltan – jegyzőkönyv felvételével – ellenőrizni kell. Az ellenőrzés során meg kell győződni az adathordozó sértetlenségéről és további alkalmazhatóságáról, valamint a tárolt adatállomány sértetlenségéről és rendelkezésre állásáról. Az ellenőrzés végrehajtása a mentésért felelős szervezeti egység feladata.

X. AZ INFORMATIKAI BIZTONSÁGI ESEMÉNYEK JELENTÉSE ÉS KEZELÉSE

138. Az Ibtv. szerinti biztonsági esemény kiterjedése szerint lehet helyi vagy országos szintű. Helyi szintű biztonsági esemény, melynek hatása csak az adott bv. szervre terjed ki, országos szintű esemény, mely egy adott bv. szervben történik ugyan, de kihatással van az országos rendszer működésének biztonságára is.
139. Az elektronikus információs rendszerben bekövetkezett biztonsági eseményeket dokumentálni kell, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében.
140. Az Ibtv. szerinti biztonsági események jelentésével és kezelésével kapcsolatos további szabályokat az IBK tartalmazza.
141. A biztonsági eseményekkel kapcsolatos képzésekre az Információbiztonsági képzés, továbbképzés rész rendelkezéseit megfelelően alkalmazni kell.

XI. FIZIKAI BIZTONSÁGI KÖVETELMÉNYEK

142. A rendszereket, rendszerelemeket, infokommunikációs eszközöket úgy kell telepíteni és tárolni, hogy
    a) a lehető legkisebb mértékre csökkentsék a fizikai és környezeti veszélyekből adódó lehetséges károkat,
    b) azokhoz a jogosult munkatársakon és külső támogatókon kívül más személy hozzáférése – jogosulatlan hozzáférés – kizárt (a lehető legkisebb mértékűre csökkentett) legyen.
143. A környezeti feltételeket a befogadó helyiségek rendeltetése, a telepítési környezetek alapján az alábbiak szerint kell meghatározni:
    a) irodai környezet (jellemzően a felhasználói és az általános informatikai tevékenységet támogató munkaállomások befogadására szolgáló helyiségek),
    b) helyi informatikai szakterület által működtetett szerverszoba,
    c) INFO által működtetett központi gépterem.
144. A bv. szervezet munkatársai és a külső támogatók a bv. szervezet tulajdonát képező infokommunikációs eszközt és mobil adathordozót a bv. szervezet telephelyeiről csak munkaköri feladat ellátására, a közvetlen vezető írásbeli – eseti vagy általános felhatalmazást tartalmazó – engedélyével vihetik ki. A rendelkezést nem kell alkalmazni a bv. szervezet által személyi használatra biztosított telefonra és infokommunikációs eszközökre.
145. A fizikai és környezeti biztonsági előírásokat, feladatokat és felelősségeket – beleértve a beléptetés technikai és adminisztratív eszközrendszerének működtetésével és ellenőrzésével kapcsolatos feladatokat – a Biztonsági Szabályzat tartalmazza.

XII. LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

146. A rendszerre vonatkozó védelmi megoldásokat új rendszer esetében a fejlesztő, már működő rendszer esetében az INFO szükség szerint a fejlesztő bevonásával tervezi meg, és gondoskodik azok megvalósításáról, beleértve a szükségessé váló korszerűsítéseket, módosításokat is.

XIII. HOZZÁFÉRÉS A RENDSZEREKHEZ

147. A felhasználó a rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.
148. A rendszer használata során a felhasználó egyedi azonosítását folyamatosan biztosítani kell. Minden felhasználót kizárólagos személyi használatú azonosítóval kell ellátni, amelyhez egyedi jelszót kell rendelni.
149. A bv. szervezet az azonosítási, autentikációs és jogosultságkezelési feladatok támogatására központi címtárat alkalmaz, amelynek használatát új rendszerek kialakításakor lehetőség szerint tervezni kell.
150. Az azonosítás, az autentikáció és a jogosultságkezelés folyamata, technológiája a fejezetben leírtaktól – különösen régi fejlesztésű vagy speciális rendeltetésű rendszerek esetében – eltérhet, az egyes rendszerek esetében a speciális előírásokat a rendszerdokumentáció tartalmazza.
151. A felhasználók nyilvántartását és a rendszer használatához képzett azonosítóját a központi címtár (Active Directory) tartalmazza.
152. A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelen személy általi megismerését kizárni. Tilos a jelszót más által megismerhető módon feljegyezni, azt más személlyel bármilyen formában közölni. Amennyiben a jelszó illetéktelen személy tudomására juthatott, vagy bármilyen módon nyilvánosságra kerülhetett, erről a tényről a felhasználó köteles tájékoztatni a közvetlen vezetőjét, aki gondoskodik az INFO értesítéséről és az IBF tájékoztatásáról. A szükséges intézkedések megtételéről a közvetlen vezető és az INFO vezetője együttesen, feladatkörüknek megfelelően gondoskodnak.
153. Egyes rendszerek, felhasználók, továbbá hozzáférési módok esetében a jelszavas azonosítást birtoklásalapú azonosítás egészíti ki.
154. A jelszóképzésre és a jelszóvédelemre vonatkozó előírások a privilegizált felhasználók és a felhasználói irodai munkakörnyezet körébe nem tartozó rendszerek esetében is értelemszerűen alkalmazandók.
155. A jelszó visszafejthető módon történő tárolása tiltott.
156. A mindennapi munkavégzéshez használt felhasználói jogosultsághoz, felhasználói fiókhoz privilegizált jogok, jogosultságok nem állíthatók be.
157. A jelszó képzésére és kezelésére, továbbá a távoli hozzáférésre vonatkozó szabályokat az IBK tartalmazza.

158. A munkatárs részére csak a munkaköre ellátásához szükséges és elégséges jogosultságok adhatók ki. A rendelkezés megtartásáért az érintett közvetlen vezetője a felelős.
159. A külső támogató jogosultságait a külső támogatót fogadó szervezeti egység vezetője engedélyezheti és igényelheti, továbbá köteles rendelkezni a jogosultság visszavonásáról is. A külső támogatók adatait is rögzíteni kell a jogosultságkezelő rendszerben.
160. A jogosultságokat úgy kell kialakítani, hogy megkülönböztethetők legyenek a felhasználói és a privilegizált felhasználói jogosultságok, jogosultságcsoportok.
161. A jogosultságkezelésre vonatkozó részletes szabályokat az IBK tartalmazza.

35. Külső rendszerek elérése

162. A külső fél által a bv. szervezet tagjai számára az interneten elérhetővé tett rendszerek, szolgáltatások a külső fél által rögzített és elérhetővé tett hozzáférési és használati szabályok szerint használhatók az IBK ide vonatkozó előírásai szerint.

XIV. FELHASZNÁLÓI IRODAI MUNKAKÖRNYEZET

163. A hálózatra csatlakoztatott informatikai eszközökön csak jogtiszta és a bv. szervezet által támogatott szoftverek körébe tartozó szoftverek telepíthetők és használhatók.
164. Az eszközökön aktivizált automatikus programtevékenységeket (pl. vírusvédelmi szoftver működése) a felhasználó nem akadályozhatja.

36. Intranethasználat

165. Minden felhasználó jogosult a munkahelyi intranet használatára.

37. Internethasználat

166. Minden felhasználó jogosult az internet informatikai védelmi szabályok szerint korlátozott használatára, azonban a szakterületi vezetője engedélyezheti a hozzáférés kiterjesztését.
167. A felhasználó az internetet kizárólag szolgálati feladatai ellátása, szakmai tájékozottsága növelése érdekében használhatja.
168. Az internet használata során különösen, de nem kizárólagosan az alábbi, jogszabályba ütköző cselekmények tilosak:
    a) mások személyiségi jogainak megsértése,
    b) másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység (pl. pornográf anyagok használata, közzététele, kéretlen levelek, levélláncok továbbítása),
    c) szerzői jog megsértése (pl. szoftver illegális terjesztése),
    d) tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték),
    e) profitszerzést célzó, direkt üzleti célú tevékenység, reklámok terjesztése,
    f) a rendszer erőforrásaihoz, a rendszeren elérhető adatokhoz arra nem jogosult személy, szervezet számára hozzáférés biztosítása,
    g) a rendszer biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok),
    h) a bv. szervezet rendszereinek megbénítását célzó támadás (denial of service attack),
    i) az azonosítási, hitelesítési és egyéb védelmi eljárások kijátszása,
    j) tilos a bv. szervezetre vonatkozó, a bv. szervezettel kapcsolatba hozható, jogszabályok által védett tartalom (pl. ügyfelek, munkatársak személyes adatai, üzleti titok stb.) nem engedélyezett közzététele, elérhetővé tétele, ideértve az összes publikus felhőszolgáltatás (pl. Dropbox, OneDrive stb.) használatát is.
169. A személyi állomány tagjának internethasználatát a közvetlen vezető, illetve az ellenőrzésre feljogosított személy ellenőrizheti.
170. A bv. szervezettel kapcsolatos közérdekű és közérdekből nyilvános adatok, információk (tájékoztatók, közlemények stb.) közzétételére vonatkozó előírásokat a büntetés-végrehajtási szervezet Adatvédelmi és Adatbiztonsági Szabályzatáról szóló 3/2019. (III. 20.) BVOP utasítás, a külső és belső kommunikációra vonatkozó előírásokat a büntetés-végrehajtási szervezet kommunikációjáról szóló 12/2019. (IX. 20.) BVOP utasítás tartalmazza.

171. A bv. szervezet személyi állománya tagja az internetes felületen magánszemélyként történő megnyilvánulásakor vagy magánvéleménye kinyilvánításakor
    a) a bv. szervezet állományába tartozásának tényét, továbbá az arra utaló képet és hangfelvételt,
    b) a beosztását,
    c) a rendfokozatát, valamint
    d) a szolgálati és szolgálatteljesítési helyére vonatkozó adatokat
    nem hozhatja nyilvánosságra.
172. Nyilvánosságra hozatalnak minősül a 171. pontban meghatározott adatok internetes felületen történő regisztráláskor mások számára is hozzáférhető módon való rögzítése.
173. Ha a hivatásos állomány tagja a 171. pontban meghatározott adatokat internetes felületen már nyilvánosságra hozta, úgy azt köteles az utasítás hatálybalépését követő 8 napon belül törölni, vagy mások számára hozzáférhetetlenné tenni.
174. Nem tartozik a 171. pontban meghatározott tilalom alá, ha a hivatásos állomány tagja magánszemélyként történő megnyilvánulására, illetve magánvéleménye kinyilvánítására
    a) a szolgálati időn kívül végzett tudományos, oktatói, művészeti, lektori, szerkesztői, a jogi oltalom alá eső szellemi tevékenységével összefüggésben vagy
    b) a bv. szervezet által szerkesztett és kiadott sajtótermékben vagy internetes felületen
    kerül sor.
175. A hivatásos állomány tagja a 174. pontban meghatározott esetekben is köteles magánszemélyként úgy megnyilvánulni, illetve a magánvéleményét kinyilvánítani, hogy az összhangban legyen a 171–174. pontban megfogalmazott elvárásokkal.

38. Levelezés

176. Az e-mail-címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz rendelve.
177. A személyhez rendelt e-mail-címek képzésének módja: vezetéknév.keresztnév@bv.gov.hu. Azonos neveknél az egyediséget a vezetéknevet követő sorszámmal történő kiegészítés biztosítja. Többelemű neveknél a felhasználóval történő egyeztetést követően lehetséges a név rövidítése.
178. Névmódosítást követően a régi e-mail-cím másodlagos címként (alias) fennmarad.
179. A felhasználó a postafiókját az interneten keresztül munkahelyén kívülről is el tudja érni.
180. A postafiókokhoz rendelt tárhelyek mérete korlátozott, az aktuális kvótáról az INFO tud felvilágosítást adni. Közvetlenül a határérték elérése előtt a felhasználó figyelmeztető üzenetet kap, a határérték túllépése esetén a kimenő és bemenő levélforgalom korlátozásra kerül, a felhasználó nem tud levelet fogadni és küldeni mindaddig, amíg nem csökkenti a tárolt adatmennyiséget a beállított kvóta szintjére vagy az alá. A felhasználó felelőssége a postafiók tartalmának kezelése, a szükségtelen küldemények törlése, vagy a megfelelő helyen történő archiválása.
181. A felhasználó szervezetén belüli levelezés során törekedni kell arra, hogy nagyméretű csatolmányokat lehetőleg ne e-mailben küldjenek a felhasználók, hanem megosztott tárhelyen helyezzék el azokat, és e-mailben csak a hivatkozást küldjék el. Ilyen megoldásokkal a nagy méretű fájlokból csak egy-egy példány kerül tárolásra az informatikai rendszerben és sem a feladó, sem a címzett tárhelyét nem terhelik.
182. A bv. szervezet tagjának levelezését a közvetlen vezető, illetve az ellenőrzésre feljogosított személy ellenőrizheti.
183. Az elektronikus levelezésre, továbbá az elektronikus tárhelyek igénybevételére vonatkozó részletszabályokat az IBK tartalmazza.

39. Szoftvertelepítés

184. A bv szervezet által üzemeltetett infokommunikációs eszközökre programok telepítése történhet:
    a) az INFO által központilag,
    b) az INFO erre felhatalmazott munkatársai által manuálisan,
    c) a bv. szerv informatikai szakterülete munkatársai által, az INFO útmutatása szerint, az általa biztosított telepítőkészletből.
185. A bv. szervezet tulajdonában álló munkaállomásra, infokommunikációs eszközre a felhasználó programot nem telepíthet, abban az esetben sem, ha a program jogtiszta. A felhasználó által történő szoftvertelepítés tiltásának beállítása az informatikai szakterület által a tartományi házirendben történik.

186. A felhasználó az eszközökre telepített szoftverek beállításait csak a jogosultsága által engedélyezett mértékben változtathatja meg. A beállított korlátozások bármilyen eszközzel történő megkerülése tilos.
187. Az engedély nélkül vagy a korlátozás megkerülésével a felhasználó által esetlegesen telepített szoftvereket az informatikai szakterület a felhasználó tájékoztatása mellett törölheti.

40. A mobil infokommunikációs eszközök használata

188. A mobil infokommunikációs eszköz központilag telepített és felügyelt védelmi megoldása nem módosítható, megkerülhető vagy törölhető.
189. A nem a bv. szervezet által biztosított (saját vagy idegen tulajdonú) mobil infokommunikációs eszközön munkahelyi tevékenységgel összefüggő, a munkahelyre vonatkozó, törvény által védett adatok, titkok (személyes adat, üzleti titok stb.), a bv. szervezet működésére, a bv. szervezet által üzemeltetett rendszerekre vonatkozó adatok, információk nem kezelhetők, nem dolgozhatók fel, nem tárolhatók.
190. A munkahelyi levelezés mobil infokommunikációs eszközön történő elérése során az alábbi előírások betartása szükséges:
    a) tilos az eszköz gépjárműben, szállítóeszközben felügyelet nélkül hagyása,
    b) a levelezés csak akkor nyitható meg, ha a felhasználó biztosítani tudja, hogy annak tartalma a kijelzőn idegenek számára nem olvasható.
191. A BVOP személyi állományának beosztáshoz kötődő, munkaköri feladatok ellátására irányuló használatáról a Büntetés-végrehajtás Országos Parancsnoksága mobil telekommunikációs eszközökkel történő ellátása rendjéről, valamint a szolgáltatások igénybevételének szabályairól szóló 24/2018. (V. 15.) OP szakutasítás rendelkezik.

41. A mobil adathordozók kezelése

192. A bv. szervezet tulajdonát képező mobil adathordozók kizárólag a munkavégzéssel összefüggő célokra használhatóak. Alkalmazásuk abban az esetben engedélyezett, ha a gazda eszköz (számítógép, tablet stb.) menedzselt eszköz, és képes a csatlakoztatott mobil adathordozón kártékonykód-ellenőrzést végezni.
193. A mobil adathordozókat a rajtuk tárolt vagy tárolandó adatok védelmi előírásainak megfelelően kell kezelni.
194. A mobil adathordozókra, továbbá az adattörlésre és fizikai adatmegsemmisítésre vonatkozó további szabályokat az IBK tartalmazza.

XV. AZ INFORMATIKAI BESZERZÉSEK

195. A rendszereket, infokommunikációs eszközöket, informatikai szolgáltatásokat és az ezekkel kapcsolatos informatikai biztonsági tevékenységet érintő beszerzések tervezése az informatikai szakterület feladata.
196. A rendszerek, infokommunikációs eszközök, informatikai szolgáltatások beszerzése során a kötendő szerződésben – a beszerzés tárgyának megfelelő tartalommal és mélységben – rögzíteni kell az alábbiakat:
    a) a rendszerdokumentáció szállító általi biztosításának, megfelelősége ellenőrzésének feltételeit, rendjét,
    b) a beszerzés tárgyával összefüggő érzékeny adatok védelmére vonatkozó előírásokat (adat- és titokvédelmi rendelkezések, nyilatkozatok),
    c) amennyiben értelmezhető, a beszerzés tárgyának rendeltetésszerű és biztonságos alkalmazásához, használatához szükséges oktatások, képzések követelményeit, tartalmát, rendjét.
197. A beszerzésekre vonatkozó részletes előírásokat a Büntetés-végrehajtás Országos Parancsnoksága Beszerzési Szabályzatáról szóló 6/2019. (VIII. 9.) BVOP utasítás tartalmazza.

XVI. AZ INFORMATIKAI FEJLESZTÉSEK

42. Általános rendelkezések

198. A fejlesztés során folyamatosan biztosítani kell, hogy az INFO a fejleszteni tervezett rendszer, infokommunikációs eszköz, informatikai szolgáltatás informatikai biztonsági aspektusait ellenőrizhesse.
199. A fejlesztés és a változáskezelés folyamataiba az információvédelmi ellenőrzést be kell építeni.
200. Fejlesztési tevékenység csak a bv. szervezet ilyen rendeltetésű informatikai környezeteiben végezhető.

201. A fejlesztésekhez és a tesztelésekhez éles rendszerből kinyert személyes adatok kizárólag anonimizált módon használhatók fel.
202. Új rendszer, rendszerelem, infokommunikációs eszköz, szoftver vagy szoftververzió rendszerbe állítását az INFO vezetője engedélyezi.
203. A fejlesztés funkcionális követelményeinek meghatározása a rendszer működéséért felelős szervezeti egység bevonásával történik.
204. A fejlesztésekre vonatkozó részletes előírásokat az IBK tartalmazza.
205. A fejlesztési tevékenységhez kapcsolódóan a fejlesztő részéről szükség szerint támogató (support) tevékenységet kell biztosítani.
206. A fejezetben foglalt előírások érvényesülését a fejlesztésre irányuló szerződésben biztosítani kell.

43. A fejlesztési folyamat dokumentálása

207. A fejlesztő köteles a fejlesztési folyamatot úgy dokumentálni, hogy a fejlesztési folyamat során elvégzett tevékenységek és a készített dokumentumok egymásnak megfeleltethetők legyenek. A fejlesztés során készülő dokumentumokat verziókezelten, rendszerenként elkülönítve, elektronikusan, visszakereshető formában kell tárolni.
208. A fejlesztések tervezése során az informatikai szakmai követelmények meghatározásáról és megfelelő dokumentálásáról a fejlesztő az INFO bevonásával gondoskodik.
209. Az informatikai szakmai követelmények meghatározásának, dokumentálásának része a jogszabályban előírt biztonsági követelmények meghatározása és teljesítésük módjának rögzítése, így különösen
    a) a rendszerbiztonsági terv,
    b) az információbiztonsági architektúra leírás,
    c) az INFO vezetője által meghatározott egyéb rendszerdokumentáció elkészítése, valamint
    d) az OVI űrlap kitöltése.

44. Fejlesztői változáskövetés

210. A fejlesztői változáskövetés szabályozása és megvalósítása során biztosítani kell az alábbiakat:
    a) a változtatásokat minden esetben a fejlesztésre irányadó szabályok szerint dokumentálni kell,
    b) a változtatások lehetséges biztonsági hatásait a végrehajtás előtt értékelni kell,
    c) csak a jóváhagyott változtatások hajthatók végre,
    d) a változtatások okáról és tartalmáról az üzemeltetésért felelős szervezeti egységet az általa meghatározott módon tájékoztatni kell.

45. Tesztelés

211. A rendszer, rendszerelem, infokommunikációs eszköz megfelelőségének értékeléséhez szükséges tesztelési folyamatok megtervezéséről és végrehajtásáról, a tesztelendő rendszer, rendszerelem, infokommunikációs eszköz létrehozásáról, beszerzéséről, illetve üzembe állításáról az INFO vezetője gondoskodik.
212. A tesztelési folyamatokra vonatkozó részletes előírásokat a rendszerdokumentáció és a rendszerbiztonsági terv tartalmazza.
213. A tesztelésre vonatkozó előírások teljesítéséért a fejlesztő – az INFO bevonása mellett – felelős.
214. Tesztrendszerekkel kapcsolatos felhasználói jogosultságkezelést az IBK tartalmazza.
215. Az informatikai és a funkcionális tesztelés végrehajtásáról is gondoskodni kell. A funkcionális tesztelésbe a rendszer működtetéséért felelős szakterületet be kell vonni.
216. Tesztelési tevékenység csak tesztkörnyezetben végezhető. Ettől eltérő rendelkezést az INFO vezetője írásban adhat.
217. Módosításokat csak a tesztkörnyezetben történt előzetes kipróbálást követően lehet átvezetni éles rendszerre. A módosítások során alkalmazni kell a verziókövetésre vonatkozó előírásokat.

46. Fejlesztők általi oktatás

218. A fejlesztett rendszer fejlesztője köteles a bv. szervezet kijelölt informatikus – és indokolt esetben felhasználói és elektronikus információbiztonsági – munkakört betöltő munkatársai számára oktatást biztosítani, amelyen a rendszer működésével és használatával összefüggő ismeretek elsajátíthatók.

XVII. AZ INFOMATIKAI ÜZEMELTETÉS

219. A rendszerek rendeltetésszerű működéséért, folyamatos rendelkezésre állásáért az INFO vezetője felel.
220. Az egyes rendszerekre vonatkozó előírásokat a rendszerdokumentáció tartalmazza.

47. Karbantartás

221. A rendszerek, infokommunikációs eszközök karbantartására vonatkozó előírásokat az IBK tartalmazza.

48. Adathordozók kezelése karbantartás során

222. A rendszerek, infokommunikációs eszközök karbantartására, javítására, cseréjére vonatkozó, a bv. szervezet mint megrendelő által kötött szerződésekben biztosítani kell, hogy a rendszerek, infokommunikációs eszközök adattárolást megvalósító elemeit a bv. szervezet visszatarthassa, azokat a szerződő félnek ne legyen köteles átadni.
223. A további előírásokat az IBK tartalmazza.

49. Hibakezelés

224. A hibakezelési előírásokat az IBK tartalmazza.
225. A folyamatokat úgy kell kialakítani, hogy azok összhangban legyenek az Informatikai biztonsági események jelentése és kezelése fejezetben foglaltakkal.

50. Konfigurációkezelés

226. A konfigurációkezeléssel összefüggő tevékenységekre, folyamatokra vonatkozó előírásokat az IBK tartalmazza.

XVIII. MUNKAÁLLOMÁS-FELÜGYELET

227. A hálózatra kapcsolódó munkaállomások felügyeletét az informatikai szakterület a Tartományi házirendben meghatározottak szerint látja el.
228. A távoli segítségnyújtás (távsegítség) során kliensoldali programot, amely bármilyen módon lehetővé teszi a felhasználó képernyőjén levő információk távoli elérését vagy input eszközeinek távvezérlését, csak a felhasználó indíthat el, azt automatikusan induló programként telepíteni tilos. A távsegítség bevezetése és alkalmazása előtt a szolgáltatás tartalmáról, továbbá a távsegítség során elvégzett beavatkozásról a felhasználót a távsegítséget nyújtó tájékoztatni köteles.
229. A rendszerek használatával kapcsolatos hiba- és változásbejelentések kezelése céljából az INFO az erre rendszeresített és az intraneten közzétett elektronikus levelezési címen keresztül ügyfélszolgálatot tart fenn.

XIX. NAPLÓZÁS

230. A rendszer használatával összefüggő eseményeket a rendszerben naplózni kell. Ez a rendelkezés vonatkozik az üzemeltetési, rendszerfelügyeleti, rendszerbiztonsági feladatok ellátására is.
231. A naplózás további szabályait az IBK tartalmazza.

XX. ADATTÁROLÁS ÉS -TOVÁBBÍTÁS

232. Az adattárolásra és -továbbításra vonatkozó előírásokat a rendszer működtetéséért felelős szervezeti egység, az adatvédelmi tisztviselő és az INFO vezetője együttesen, a konkrét eset ismeretében határozza meg és rögzíti.

XXI. KÁRTÉKONY KÓDOK ELLENI VÉDELEM

233. A kártékony kódok elleni védelem megtervezéséről és végrehajtásáról az INFO gondoskodik, részletszabályait az IBK tartalmazza.

51. A felhasználó felelőssége a kártékony kódok elleni védelmi eszközök és eljárások alkalmazása során

234. A bv. szervezet automatikus védelmi rendszert (programot) működtet rosszindulatú szoftverek, kártékony kódok észlelésére és megsemmisítésére.
235. Az a felhasználó, aki a vírusvédelmi rendszert kikapcsolja, illetve a vírusellenőrzést vagy vírusvédelmi intézkedést (vírusirtást) szándékosan akadályozza, az ebből eredő károkért teljes felelősséggel tartozik.
236. Ha a vírusvédelmi rendszer nem működik a munkaállomáson (a Windows tálcán nem látható annak ikonja vagy hibát jelez), a felhasználó köteles azt az informatikai szakterület részére azonnal jelenteni. A vírusvédelmi rendszer helyreállításáig a felhasználó mobil adathordozót nem kezelhet a munkaállomásán, illetve mobil munkaállomás esetén internetre, hálózatra nem csatlakozhat.
237. Ha a felhasználó rosszindulatú szoftver, kártékony kód jelenlétére gyanakszik, az informatikai szakterületet értesítenie kell, és a gyanús eszköz vagy rendszer használatát lehetőleg fel kell függesztenie.

XXII. TITKOSÍTÁS

238. Kizárólag közérdekű és közérdekből nyilvános adatok esetében a titkosítás alkalmazása nem kötelező.
239. Nem a fenti adatkörbe tartozó adatok, így különösen törvény által védett adatok, titkok esetében a titkosításról, illetve – amennyiben a titkosítás alkalmazása lehetetlen vagy alkalmazása aránytalan nehézséggel vagy költséggel járna – kockázatcsökkentő intézkedésekről kell gondoskodni.
240. A titkosítás biztosításról az informatikai szakterület gondoskodik, annak részletes szabályait az IBK tartalmazza.

52. Vezeték nélküli hozzáférés

241. A bv. szervezet objektumaiban vendég wifi-lefedettség biztosított, az alábbi jellemzőkkel:
    a) internetelérést tesz lehetővé,
    b) tűzfal védelemmel és ezen keresztüli védelmi képességekkel ellátott,
    c) az IP-cím allokáció az üzemeltetési szakterület által felügyelt eszközökkel, központosítva valósul meg,
    d) jelszavas hozzáféréssel működik.

XXIII. ZÁRÓ RENDELKEZÉSEK

242. Ez az utasítás a közzétételét követő napon lép hatályba.
243. Hatályát veszti
    a) a büntetés-végrehajtási szervezet Informatikai Biztonsági Szabályzatáról szóló 9/2016. (II. 16.) OP szakutasítás,
    b) a büntetés-végrehajtási szervezet informatikai eljárásrendjéről szóló 11/2018. (III. 5.) OP szakutasítás,
    c) a hivatásos állományba tartozásra vonatkozó adatok internetes felületen történő nyilvánosságra hozatalának korlátozásáról szóló 3/2015. (X. 30.) BVOP utasítás.

Dr. Tóth Tamás bv. vezérőrnagy s. k.,
országos parancsnok

1. melléklet a 15/2019. (XI. 8.) BVOP utasításhoz

KIVONAT
a büntetés-végrehajtási szervezet EIR-alapnyilvántartásából

Rendszer		
nyilvántartási sorszáma	biztonsági osztálya	speciális besorolása
2.	4	–
4.	4	–
5–10.	4	zárt célú rendszer a 187/2015. Korm. rend. 14. § (2) bekezdés c) alpontja szerint
11–31.	4	zárt célú rendszer a 187/2015. Korm. rend. 14. § (2) bekezdés c) alpontja szerint
32.	2	–
34.	3	–
38.	3	–
40.	3	–
41.	3	–
42–48.	4	zárt célú rendszer a 187/2015. Korm. rend. 14. § (2) bekezdés b) alpontja szerint
49.	3	–
59.	4	–

2. melléklet a 15/2019. (XI. 8.) BVOP utasításhoz

Nyilatkozat

Alulírottak a jelen Nyilatkozat aláírásával elismerjük, hogy a bv. szervezet információbiztonsági előírásait, különösen az Informatikai Biztonsági Szabályzatot és az Informatikai Biztonsági Kézikönyvet megismertük, az abban foglaltakat magunkra nézve kötelezőnek ismerjük el.

Sorszám	Dátum	Név, rendfokozat	Aláírás

3. melléklet a 15/2019. (XI. 8.) BVOP utasításhoz

Nyilatkozat

Alulírottak a jelen Nyilatkozat aláírásával elismerjük, hogy a bv. szervezet információbiztonsági előírásainak ránk vonatkozó részét, különösen az Informatikai Biztonsági Szabályzatot megismertük, az abban foglaltakat magunkra nézve kötelezőnek ismerjük el.

Sorszám	Dátum	Név, rendfokozat	Aláírás

II. Nemzetközi szerződésekkel kapcsolatos közlemények

A külgazdasági és külügyminiszter 52/2019. (XI. 8.) KKM közleménye a Magyarország és a Kínai Népköztársaság (Heilongjiang Tartomány Oktatási Minisztériuma) között a Heilongjiang Kínai Orvostudományi Egyetem oktatási tevékenységének Magyarországon való támogatásáról szóló Megállapodás kihirdetéséről szóló 2017. évi CLXXIV. törvény 2. §-ának és 3. §-ának hatálybalépéséről

A 2017. évi CLXXIV. törvénnyel a Magyar Közlöny 2017. december 11-i 207. számában kihirdetett, a Magyarország és a Kínai Népköztársaság (Heilongjiang Tartomány Oktatási Minisztériuma) között a Heilongjiang Kínai Orvostudományi Egyetem oktatási tevékenységének Magyarországon való támogatásáról szóló Megállapodás (a továbbiakban: Megállapodás) (4) bekezdése az alábbiak szerint rendelkezik a hatálybalépésről:
„Jelen megállapodás a legutolsó írásbeli értesítés kézhezvételétől számított harmincadik (30.) napon lép hatályba."

A Megállapodás hatálybalépéséhez szükséges feltétel teljesülésének napja: 2019. október 22.
A Megállapodás hatálybalépésének naptári napja: 2019. november 21.

A fentiekre tekintettel, összhangban a Magyarország és a Kínai Népköztársaság (Heilongjiang Tartomány Oktatási Minisztériuma) között a Heilongjiang Kínai Orvostudományi Egyetem oktatási tevékenységének Magyarországon való támogatásáról szóló Megállapodás kihirdetéséről szóló 2017. évi CLXXIV. törvény 4. § (3) bekezdésével megállapítom, hogy a Magyarország és a Kínai Népköztársaság (Heilongjiang Tartomány Oktatási Minisztériuma) között a Heilongjiang Kínai Orvostudományi Egyetem oktatási tevékenységének Magyarországon való támogatásáról szóló Megállapodás kihirdetéséről szóló 2017. évi CLXXIV. törvény 2. §-a és 3. §-a 2019. november 21-én, azaz kettőezertizenkilenc november huszonegyedikén lép hatályba.

Szijjártó Péter s. k.,
külgazdasági és külügyminiszter

III. Közlemények

A Belügyminisztérium nyilvántartások vezetéséért felelős helyettes államtitkára közleménye elveszett, eltulajdonított, megsemmisült gépjárműtörzskönyvekről

A Belügyminisztérium nyilvántartások vezetéséért felelős helyettes államtitkára a közúti közlekedési igazgatási feladatokról, a közúti közlekedési okmányok kiadásáról és visszavonásáról szóló 326/2011. (XII. 28.) Korm. rendelet 83. § (1) bekezdése alapján az alábbi elveszett, eltulajdonított, megsemmisült gépjárműtörzskönyvek sorszámát teszi közzé:

777534J	699752B	155704M	370846K	554734F
986739D	705393I	156314N	372975P	555006N
000758G	712648P	159770T	374371I	560778R
006417N	716427L	164404J	374480P	563002F
067147P	823329L	166828L	378263R	567312B
083112M	849775L	181800P	379489E	569911R
088924S	850282M	182931J	405659R	572803K
112204N	854339R	200957S	413574H	574667C
113295N	004114N	204263L	421513G	580588F
127044P	016746N	206288P	422555G	581360R
159539K	024608B	213036D	427800L	589996S
161626R	029639T	222195G	428180G	597748K
172980S	030324G	230105I	435203L	600264N
196366G	030558M	235911L	435469N	605824P
204147R	031539H	244463S	449774S	614657P
227617M	032539R	244852J	450055M	616668R
242098P	038993R	254130L	458973R	618314N
245748M	041079D	264345K	462516H	619182R
260483M	049448M	268672M	467734L	619637J
301438P	059224I	270831G	469797P	632583L
311326H	062960S	278220R	475442S	635367P
338925R	066639T	278481F	484368N	638510M
350250R	070992S	279257S	484879K	642513P
355862I	072197R	283441R	484901R	643162R
370745R	073532S	288339I	487316R	648138M
371545N	076444R	291650S	492288G	650488R
386909P	076846L	303612S	495236N	663106S
426689S	078356T	308052R	497005S	674161L
429042S	083358M	319422K	498160E	674388S
442318S	085297P	319849R	499165G	684495F
445084I	088145S	321890R	502434I	697387P
450901R	088939N	326002P	508260L	707263P
478744M	095041S	326143R	523678P	709404H
521847L	100642L	329966D	532969N	709780K
565114M	100659J	334478N	533904S	712383J
587222E	106696R	338255S	536500N	712891R
604426H	125324L	350097M	537846S	713065L
610444S	131850H	357407G	545030A	715636R
643975I	132947N	358116M	545586M	718275H
657325G	138635S	358964M	547059M	718339H
698995M	145626F	360114P	548894M	718594P

720487P
722976R
726268L
728560B
729336N
733454H
736498S
752068P
753939N
758361I
766016S
771125P
773336J
781044K
788314R
801035S
802864H
802876M
805182P
810509A
810830R
810891P
816118S
819555R
819990M
820957H
827123J
830164N
837377M
839153G
841831R
856626P
858338L
858826D
867204K
873894H
879829S
883466H
890809M
905146P
905652P
909119I
921100K
921541N
921951K
925229I
926454C
926700R
928454E
934106B
935032H
941403N
967450R
972360K
974056E
980726L
983628E
988051P
989677P
991579P
011989K
017426D
017807L
027759H
032643M
033276R
035845H
038179M
047270G
052397S
052604T
056296R
062000T
066281M
068190P
078447P
078727J
082076S
084951P
097074S
102686N
102734P
102963K
104172M
104295H
115670H
116915T
130216S
130622D
139449G
149591P
152294R
153260L
157787L
164737S
167918T
176077I
182151E
184549P
190781T
191334L
192376M
193020I
198959P
207202M
217048N
224751A
237799S
261649M
266268R
268711B
272377K
280331H
285357H
289584L
298701M
311077S
312484M
313749N
316616N
317914M
328389I
329630F
341112M
344531P
344694P
349580P
355328P
356659J
361445N
366587P
368263D
374308K
380847F
386100M
391912I
401144N
404602S
406226L
419217I
429094L
434188R
434396L
442956B
445844E
461033C
467970S
472960P
473040B
478944S
487588N
494152K
497964A
502624L
512841F
517078L
520741F
535344M
541214H
549748R
553309F
555915L
556058L
568712R
579355N
582468R
587819I
589549C
598168M
598730H
608766N
609361L
610291R
620319H
625306R
627006I
630052R
632204D
636180S
650409D
654896N
660002J
666849M
672109H
687259H
692007E
696611N
697879P
699005I
699386S
702851B
706712K
709074L
710736J
720615H
721004G
726773D
727107R
727480H
734242R
743242K
746581K
749696M
756473L
760206S
765287L
775517B
778464L
802840M
809572I
810415R
825687S
832113P
838549P
839550K
846586J
847123R
862238N
889860E
895511N
895712R
898800S
908240P
909799K
927203N
929722R
933426D
935074K
943659R
944340K
944606P
956488J
963226A
965708L
973846R
976126H
982560R
984586E
993064J
004462F
005064R
005615F
010122I
012373N
019070P
023178N
029520K
036636N
047122G
051310L
056195M
057391T
057793K
059127B
059563R
061161P
061709N
063089G
071889M
080813C
085949D
095597T
101359C
102829M
106612T
115940R
122877P
128511N
135525N
139220P

146282S
160935I
174284M
184843T
189179J
195482R
203480P
206500A
219644R
220097J
223378I
226442D
228792N
229347L
231095C
233209J
249256P
255536P
259527P
267664I
284862N
291977J
294218K
295213F
298065P
299832R
311975S
312255M
320809N
330086F
331895I
339795B
340940S
348065N
352554N
355606S
358444C
359264M
359733S
363889H
364671L
365335D
366914J
374450I
377167H
391925L
393414I
405114I
408345E
414753C
423329F
439679N
446313P
448878P
449826S
452168I
456475M
457731R
478865M
479214F
481211P
484549G
492602K
496307N
511310H
514257R
517085L
530503P
538743S
545548H
545560I
547742L
548370G
548998R
550594N
551599G
562065H
565992I
566599N
579811J
580112L
580951M
581138M
588282J
597890H
599269I
603187R
603983L
610888M
612520P
620550I
622064P
625907H
634643R
636163I
639614S
639985H
640180D
649528E
661800J
664306H
671196P
672501K
672966N
674069S
679839I
681599L
684608M
688524N
692588D
695868F
699479L
703844J
707450H
713731N
714767H
719563M
724731D
727493P
736960K
740183S
763729J
766245J
774900L
775552C
775978J
776228G
778583F
785354C
788740L
790051R
793603G
794959R
796997N
799596L
814129M
821130N
821520E
827436I
831058N
832451M
839029R
840884P
844889R
856372F
861960N
867620P
874937M
877108P
884321P
885054R
888855F
888909J
895695M
903406P
911209L
911962K
914231L
915480E
928058J
942976B
946823N
950085C
951787G
951913P
951948R
969383I
973883R
975167L
982944L
986070P
992938M
994473H
995745I
997178R
052247M
053714P
053746J
060499R
067653M
102239I
132751H
134585I
135300I
147923N
158135K
181219H
181477P
190210K
204147I
229178I
243330N
257334N
262261N
288501D
295555F
299520I
313592I
346178M
349840K
371729L
397870K
402363M
410307P
411632P
468146J
471590I
546830R
555934R
598061K
603626R
620590S
621895I
626986S
684472N
691369L
693571G
704132N
704808K
716217M
719783M
743277P
773907R
780840G
784058G
785082R
796438L
799176L
811401P
825669J
847990I
863610N
876122N
888136I
888207L
904051P
944709N
946919E

Budapest, 2019. október 31.

Az Országgyűlés Hivatala közleménye elismerések adományozásáról

A 4/2018. számú házelnöki rendelkezés alapján az Országgyűlés Elnöke a tevékenységükkel az Országgyűlési Könyvtár működését segítő, az Országgyűlés Hivatalával jogviszonyban nem álló személyek elismerésére 2019. november 6-án

Varga Éva részére

Nagy Miklós-díjat adományozott.

Az Igazságügyi Minisztérium közleménye Miniszteri Elismerő Oklevél adományozásáról

Dr. Varga Judit igazságügyi miniszter asszony az 1956. évi forradalom és szabadságharc kezdetének napja nemzeti ünnepünk alkalmából – az igazságügyi miniszter által adományozható elismerésekről szóló 4/2015. (III. 3.) IM rendelet alapján – huzamos időn át végzett szakmai munkája, valamint az Igazságügyi Minisztérium eredményes működése szempontjából fontos szakmai feladat végrehajtásában szerzett érdemei elismeréseként

Miniszteri Elismerő Oklevelet

adományozott:

dr. B. Tóth Enikőnek, a Közigazgatási Államtitkári Titkárság titkárságvezetőjének, főosztályvezetőjének;
Bajnócziné dr. Horváth Evelin Editnek, a Jogi Szolgáltatási Főosztály vezető-kormányfőtanácsosának;
Barta Gábornak, az Igazságügyi Szakmai Irányítási és Módszertani Főosztály főosztályvezetőjének;
dr. Borzsák Levente Benőnek, a Miniszteri Kabinet politikai tanácsadójának;
Buczkó Mátyásnénak, a Büntető Anyagi Jogi és Büntetés-végrehajtási Jogi Kodifikációs Főosztály vezető-kormánytanácsosának;
dr. Czombos Tamásnak, az Európai uniós jogi ügyekért felelős helyettes államtitkárnak;
dr. Csuhány Péternek, a Jogszabály-előkészítés Összehangolásáért és Közjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság kormány-főtanácsosának;
dr. Daragóné dr. Szombathelyi Zsófiának, a Közszolgálati Kodifikációs és Koordinációs Főosztály főosztályvezetőjének;
dr. Farkas Fatimének, a Civilisztikai és Igazságügyi Kodifikációs Főosztály kormánytanácsosának;
Gether Dánielnek, a Versenyképességi és Belső Piaci Érdekérvényesítésért felelős Főosztály főosztályvezetőjének;
dr. Guttman Hanga Lillának, a Közigazgatási Államtitkári Titkárság vezető-kormányfőtanácsosának;
Győry János Imrének, az Európai Uniós Gazdaságpolitikai és Migrációs Főosztály, EU Költségvetési Osztály osztályvezetőjének;
dr. Kelemen Lászlónak, a Kegyelmi Főosztály kormánytanácsosának;
Kiss Andreának, az Európai Uniós Intézményi Kapcsolatokért és Személyzetpolitikáért Felelős Főosztály kormánytanácsosának;
dr. Koppány Juliannának, az Igazságügyi Kapcsolatokért Felelős Államtitkári Kabinet politikai főtanácsadójának;
dr. Kovács Ferencnek, az Adatvédelmi Kodifikációs és Koordinációs Főosztály vezető-kormányfőtanácsosának;
Környi László Évának, a Parlamenti Államtitkári Kabinet kabinetfőnökének;
dr. Kupecki Nórának, a Jogszabály-előkészítés Összehangolásáért és Közjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság kormány-főtanácsosának;
dr. Mázi András Bélának, az Alkotmányjogi Főosztály főosztályvezetőjének;
dr. Molnár Katalinnak, az Európai Uniós Jogi Ügyekért Felelős Helyettes Államtitkári Titkárság kormány-főtanácsosának;
Móni Istvánné dr. Nagy Mónikának, az Adatvédelmi Kodifikációs és Koordinációs Főosztály főosztályvezetőjének;

dr. Nagy Eszternek, az Igazságügyi Szolgáltatásokért Felelős Helyettes Államtitkári Titkárság titkárságvezetőjének, főosztályvezetőjének;

dr. Nagy Mártának, a Költségvetési Főosztály, Felügyeleti Osztály osztályvezetőjének;

dr. Orbán Szabolcsnak, a Jogszabály-előkészítés Összehangolásáért és Közjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság, Közigazgatási Eljárásjogi Kodifikációs Osztály osztályvezetőjének;

dr. Pátkai Nándornak, a Jogszabály-előkészítés Összehangolásáért és Közjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság titkárságvezetőjének, főosztályvezetőjének;

dr. Petrity Krisztinának, a Közszolgálati Kodifikációs és Koordinációs Főosztály, Közszolgálati Jogi Osztály osztályvezetőjének;

Polonyiné Perecz Liliánának, az Állandó Képviselet Gazdálkodásfelügyeleti Főosztály kormány-főtanácsosának;

Rácz István Tamásnak, az Európai Uniós Intézményi Kapcsolatokért és Személyzetpolitikáért Felelős Főosztály vezető-kormányfőtanácsosának;

dr. Rácz Ritának, a Miniszteri Kabinet politikai tanácsadójának;

Rada Beátának, a Költségvetési Főosztály kormánytanácsosának;

dr. Ráth Olivér Zoltánnak, az Alkotmányjogi Főosztály vezető-kormányfőtanácsosának;

dr. Ribaritsné dr. Győri Enikőnek, a Gazdasági Kodifikációs Főosztály, Gazdasági Jogi Kodifikációs Osztály osztályvezetőjének;

Rima Anikónak, a Pénzügyi és Számviteli Főosztály, Pénzügyi Osztály kormány-főtanácsosának;

dr. Salgó László Péternek, a Jogszabály-előkészítés összehangolásáért és közjogi jogalkotásért felelős helyettes államtitkárnak;

dr. Sembery-Sugár Hajnalkának, az Igazságügyi Felügyeleti Főosztály főosztályvezetőjének;

dr. Simon Ákosnak, a Jogszabály-előkészítés Összehangolásáért és Közjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság, Törvény-előkészítési Koordinációs Osztály osztályvezetőjének;

dr. Somogyi Dávid Lászlónak, a Civilisztikai és Igazságügyi Kodifikációs Főosztály, Peres Eljárásjogi Kodifikációs Osztály beosztott bírójának;

Szilágyi Tamásnak, az Európai Uniós Gazdaságpolitikai és Migrációs Főosztály főosztályvezetőjének;

dr. Tornyai Gergelynek, az Európai Bírósági Főosztály kormánytanácsosának;

dr. Tóth Ágnesnek, a Gazdasági Kodifikációs Főosztály, Gazdasági Jogi Kodifikációs Osztály vezető-kormányfőtanácsosának;

Tüsér Zoltán Bélánénak, a Pénzügyi és Számviteli Főosztály kormánytanácsosának;

dr. Váradi Ágnesnek, a Kiemelt Nemzetközi Koordinációs Főosztály főosztályvezetőjének;

dr. Vincze Veronikának, a Parlamenti Főosztály főosztályvezetőjének;

dr. Virányi-Gyermán Erikának, a Nemzetközi és Európai Uniós Igazságügyi Együttműködésért Felelős Államtitkári Kabinet kabinetfőnökének;

Zámbó Dávidnak, az Informatikai és Fejlesztési Főosztály főosztályvezetőjének;

dr. Zsombolyay Péternek, az Igazságügyi és Magánjogi Jogalkotásért Felelős Helyettes Államtitkári Titkárság titkárságvezetőjének, főosztályvezetőjének.

A Hivatalos Értesítőt az Igazságügyi Minisztérium szerkeszti.
A szerkesztésért felelős: dr. Salgó László Péter.
A szerkesztőség címe: Budapest V., Kossuth tér 4.
A Hivatalos Értesítő hiteles tartalma elektronikus dokumentumként a http://www.magyarkozlony.hu honlapon érhető el.
A Hivatalos Értesítő oldalhű másolatát papíron kiadja a Magyar Közlöny Lap- és Könyvkiadó Kft.
Felelős kiadó: Papp Tibor ügyvezető.