DKÜ

**A Digitális Kormányzati Ügynökség Zrt.**

# INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Hatályos: 2025. február 18. napjától.

DKÜ

# Informatikai biztonsági szabályzat

# (IBSZ)

**Verziószám: v8.0.**

# Tartalomjegyzék

I. Általános rendelkezések ... 6
II. Programmenedzsment ... 6
II.1. Az Informatikai biztonsági szabályzat célja ... 6
II.2. Az IBSZ rendeltetése ... 6
II.3. Az IBSZ kezelése ... 7
II.3.1. Az IBSZ felülvizsgálata ... 7
II.3.2. Az IBSZ oktatása ... 7
II.3.3. Az IBSZ szabályozási környezete ... 8
II.3.4. Az IBSZ hatálya ... 9
II.3.5. Értelmező rendelkezések, alapfogalmak, rövidítések ... 9
II.4. A védelem tárgya, eszközei és működése ... 11
II.4.1. A védelem tárgya ... 11
II.4.2. Az informatikai biztonság szervezete ... 12
II.4.2.1. Vezérigazgató ... 12
II.4.2.2. Szakterületi vezető ... 12
II.4.2.3. Az adatgazda ... 13
II.4.2.4. Biztonsági vezető ... 13
II.4.2.5. Információbiztonsági felelős (IBF) ... 14
II.5. Szervezeti szintű alapfeladatok ... 15
II.5.1. Intézkedési terv ... 15
II.5.2. Az elektronikus információs rendszerek nyilvántartása ... 15
II.5.3. Biztonsági elemzés, teljesítmény mérése ... 15
II.5.4. Az elektronikus információbiztonsággal és annak jogosultságaival kapcsolatos engedélyezési eljárás ... 15
II.5.5. Kapcsolattartás ... 15
II.5.6. A DKÜ Zrt. szempontjából kritikus rendszerek, erőforrások kezelése ... 16
II.5.7. Felügyeleti stratégia ... 16
III. Hozzáférés-felügyelet ... 16
III.1. Hozzáférés ellenőrzési eljárásrend ... 16
III.2. Felhasználói fiókok kezelése, fiókkezelés ... 16
III.3. Hozzáférés ellenőrzés érvényesítése ... 16
III.4. A felhasználók hozzáféréssel kapcsolatos kötelességei, felelősségek szétválasztása ... 16
III.5. Legkisebb jogosultság elve ... 16
III.6. Sikertelen bejelentkezési kísérletek ... 16
III.7. A rendszerhasználat jelzése ... 18
III.8. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek ... 18
III.9. Távoli hozzáférés ... 18
III.10. Vezeték nélküli hozzáférés ... 18
III.11. Mobil eszközök hozzáférés ellenőrzése ... 18
III.12. Külső elektronikus információs rendszerek használata ... 18
III.13. Nyilvánosan elérhető tartalom, információmegosztás ... 18
IV. Tudatosság és képzés ... 18
IV.1. Képzési eljárásrend ... 18
IV.2. Biztonságtudatossági képzés ... 19
IV.3. Szerepkör, vagy feladat alapú biztonsági képzés ... 19
IV.4. A biztonsági képzésre vonatkozó dokumentációk ... 19
V. Naplózás és elszámoltathatóság ... 19
V.1. Naplózási eljárásrend ... 19
VI. Értékelés, engedélyezés és monitorozás ... 19
VI.1. Biztonsági értékelések ... 19
VI.2. Informatikai biztonsági rendszer felülvizsgálata, folyamatos felügyelet ... 19
VI.3. Az elektronikus információs rendszer kapcsolódásai ... 19
VI.4. Személyi biztonság ... 19

VII. Konfigurációkezelés ..... 19
VII.1. Biztonsági hatásvizsgálat ..... 20
VII.2. Konfigurációs beállítások ..... 20
VII.3. A konfigurációváltozások felügyelete (változáskezelés) ..... 20
VII.4. Legszűkebb funkcionalitás ..... 20
VII.5. Információs rendszerelem leltár ..... 20
VII.6. A szoftverhasználat korlátozásai ..... 20
VII.7. A felhasználó által telepített szoftverek ..... 20
VIII. Üzletmenet folytonosság tervezése ..... 21
VIII.1. Üzletmenet folytonossági terv informatikai erőforrás kiesésekre ..... 21
VIII.2. BCP akciótervek oktatása, folyamatos működésre felkészítő képzés ..... 21
VIII.3. Az elektronikus információs rendszer mentései ..... 21
VIII.4. Üzletmenet-folytonossági terv tesztelése ..... 21
VIII.5. Az elektronikus információs rendszer helyreállítása és újraindítása ..... 21
IX. Azonosítás és hitelesítés ..... 21
IX.1. Azonosítás és hitelesítés ..... 21
IX.2. A felhasználói hozzáférés kezelése ..... 22
IX.3. Azonosító kezelés ..... 22
IX.4. Hálózati hozzáférés privilegizált fiókokhoz ..... 22
IX.5. A hitelesítésre szolgáló eszközök kezelése ..... 22
IX.6. A hitelesítésre szolgáló eszköz visszacsatolása ..... 22
IX.7. Hitelesítés kriptográfiai modul esetén ..... 22
IX.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) ..... 22
IX.9. Hitelesítés szolgáltatók tanúsítványának elfogadása ..... 22
IX.10. Ellenőrzés ..... 22
X. Biztonsági incidensek, események kezelése ..... 23
X.1. Képzés a biztonsági események kezelésére ..... 23
X.2. A biztonsági incidensek, események figyelése és jelentése ..... 23
X.3. A biztonsági incidensek, események kezelése, kivizsgálása ..... 23
X.4. Biztonsági események kezelésének tesztelése ..... 23
X.5. Biztonsági eseménykezelési terv, incidenstípusok ..... 23
X.6. Az incidenskezeléshez kapcsolódó szerepkörök feladatai, felelősségei ..... 23
XI. Karbantartás ..... 23
XII. Adathordozók védelme ..... 23
XII.1. Hozzáférés az adathordozókhoz ..... 23
XII.2. Adathordozók címkézése ..... 23
XII.3. Adathordozók tárolása ..... 24
XII.4. Adathordozók szállítása ..... 24
XII.5. Adathordozók törlése, információtörlés ..... 24
XII.6. Adathordozó kriptográfiai védelme ..... 24
XII.7. Adathordozók használata ..... 24
XIII. Fizikai és környezeti védelem ..... 24
XIII.1. Biztonsági területek ..... 24
XIII.1.1. Biztonsági zónák meghatározása ..... 24
XIII.1.2. Zónák védelme ..... 24
XIII.2. Fizikai belépési engedélyek ..... 25
XIII.3. A fizikai belépés ellenőrzése ..... 25
XIII.4. A fizikai hozzáférések felügyelete ..... 25
XIII.5. A látogatók ellenőrzése ..... 25
XIII.6. Vészvilágítás ..... 26
XIII.7. Tűzvédelem ..... 26
XIII.8. Hőmérséklet és páratartalom ellenőrzés ..... 26
XIII.9. Vezetéken szállított anyag okozta kár elleni védelem ..... 26
XIII.10. Be- és kiszállítás ..... 26
XIII.11. Karbantartó személyek ..... 26

XIII.12. Harmadik fél adatközpontjában elhelyezett rendszerek ... 26
XIV. Tervezés ... 27
XIV.1. Biztonságtervezési eljárásrend ... 27
XIV.2. Rendszerbiztonsági terv ... 27
XV. Személyi biztonság ... 27
XV.1. Munkakörök, feladatok biztonsági szempontú besorolása ... 27
XV.2. Személyek háttérellenőrzése ... 27
XV.3. Eljárás a jogviszony megszűnésekor, megváltozásakor ... 27
XV.4. Az áthelyezések, átirányítások és kirendelések kezelése ... 27
XV.5. Hozzáférési megállapodások ... 28
XV.6. Külső személyekhez kapcsolódó biztonsági követelmények ... 28
XV.7. Fegyelmi intézkedések ... 28
XV.8. Munkaköri leírás ... 28
XV.9. Viselkedési szabályok az internet használata során ... 28
XVI. Kockázatelemzés ... 28
XVI.1. Biztonsági besorolások ... 28
XVI.2. Fenyegetésfelismerő képesség ... 28
XVI.3. Információosztályozás ... 29
XVI.4. Tesztelés, képzés és felügyelet ... 29
XVI.4.1. Sérülékenységi teszt ... 29
XVI.4.2. Frissítési képesség ... 29
XVI.4.3. Privilegizált hozzáférés ... 29
XVI.4.4. Felfedhető információk ... 29
XVII. Rendszer és szolgáltatás beszerzés ... 29
XVII.1. Erőforrás igény felmérés ... 29
XVII.2. Beszerzések ... 30
XVII.3. Az elektronikus információs rendszerre vonatkozó dokumentáció ... 30
XVII.4. Biztonságos kódolás ... 30
XVII.5. Külső elektronikus információs rendszerek szolgáltatásai ... 30
XVII.5.1. Felhőszolgáltatások használatára vonatkozó információbiztonság ... 30
XVII.6. Folyamatos ellenőrzés ... 30
XVIII. Rendszer- és kommunikációvédelem ... 30
XIX. Rendszer- és információsértetlenség ... 30
XIX.1. Kártékony kódok elleni védelem ... 31
XIX.1.1. Webszűrés ... 31
XIX.2. Az elektronikus információs rendszer felügyelete ... 31
XIX.3. Biztonsági riasztások és tájékoztatások ... 31
XIX.4. A kimeneti információ kezelése és megőrzése ... 31
XX. Ellátási lánc kockázatkezelése ... 31
XX.1. Beszerzési stratégiák, eszközök és módszerek ... 31
XX.2. Beszállítók értékelése és felülvizsgálata ... 31
XX.3. Rendszerek, rendszerelemek vizsgálata ... 31
XXI. Központi rendszerekre vonatkozó speciális előírások ... 31
XXI.1. Együttműködés a nemzeti kiberbiztonsági hatósággal ... 31
XXI.2. Központi rendszer igénybevételére vonatkozó információbiztonsági követelmények ... 32
XXI.3. Együttműködés a felhasználó szervezettel ... 32
XXI.4. Központi rendszert érintő kiberbiztonsági incidensek kezelése ... 32
XXI.5. Együttműködés kiberbiztonsági válsághelyzetekben ... 33

# I. Általános rendelkezések

1) Az Informatikai biztonsági szabályzat (a továbbiakban: IBSZ vagy Szabályzat) a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény alapján készült, megfelelve az MSZ ISO/IEC 27001:2023 szabvány követelményeinek.

# II. Programmenedzsment

## II.1. Az Informatikai biztonsági szabályzat célja

2) Az IBSZ alapvető célja, hogy a Digitális Kormányzati Ügynökség Zrt. (a továbbiakban: DKÜ Zrt.) elektronikus információs rendszereiben (a továbbiakban: elektronikus információs rendszer vagy EIR), valamint azok alkalmazása során olyan adat- és információvédelmi eljárásrendet alakítson ki és olyan intézkedéseket vezessen be, amelyek alkalmazása biztosítja az adat- és információvédelem alkotmányos elveinek, továbbá az információbiztonság követelményeinek (bizalmasság, sértetlenség, rendelkezésre állás) érvényesülését mind a szándékolt, mind a nem szándékolt, biztonságot veszélyeztető cselekményekkel, eseményekkel, katasztrófákkal szemben (legyenek azok emberi, technológiai vagy természeti eredetűek).

3) Az IBSZ-ben foglaltaknak megfelelően biztosítani kell az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

4) Az IBSZ kialakításának célja, hogy meghatározza, és egységes keretbe foglalja azokat a szabályokat, amelyeket a személyi hatálya alá tartozóknak a rá vonatkozó mértékben ismernie, valamint a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.

5) Célja továbbá, hogy szabályozza és ellenőrizhetővé tegye a biztonsági és védelmi rendszert, valamint, hogy olyan tervezési támpontokat nyújtson, amelyek segítik a rendszer elemeinek kivitelezését, illetve mérhetővé, és visszacsatolhatóvá teszik az elvárt biztonsági szintet.

6) Az IBSZ meghatározza a védelmi eljárások során a jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket, amelyek támogatják:

   a) a megelőzést és a korai figyelmeztetést;
   b) az észlelést;
   c) a reagálást;
   d) a biztonsági események kezelését.

## II.2. Az IBSZ rendeltetése

7) Az IBSZ rendeltetése, hogy a DKÜ Zrt. működéséhez igénybe vett elektronikus információs rendszerek alkalmazása során biztosítva legyen:

   a) az EIR-ekkel, valamint azok működésével kapcsolatos kockázatok kezelése, ennek keretén belül;
   b) az EIR-ek sebezhetőségének ésszerű minimumra való csökkentése;
   c) az infokommunikációs folyamatokat fenyegető veszélyek megelőzése, elhárítása;
   d) az információk és adatok EIR-ek segítségével való kezelése (gyűjtés, feldolgozás, tárolás, átvitel, elosztás, megjelenítés, megsemmisítés), valamint további hasznosítása során az informatikai biztonsági eseményekből származó

hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése;
e) az EIR-ek zavartalan üzemeltetése;
f) az üzemeltetett EIR-ek rendeltetésszerű használata;
g) az üzembiztonságot szolgáló karbantartás és fenntartás;
h) az adatok és információk tartalmi és formai épségének megőrzése;
i) az alkalmazott EIR-hez tartozó dokumentációk nyilvántartása;
j) a felhasználói jogosultsági körök meghatározása;
k) az adatok és információk biztonságos mentése;
l) az adat- és információ védelem és biztonság feltételeinek megteremtése;
m) a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása.

8) Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kibertv.), illetve végrehajtási rendeletei, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: 7/2024 MK rendelet), valamint a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról 418/2024. (XII. 23.) Korm. rendelet (a továbbiakban: 418/2024 Korm. rendelet) alapján a DKÜ Zrt. az elektronikus információs rendszereit biztonsági osztályba sorolja mely eredmény meghatározza a DKÜ Zrt.-re, mint szervezetre vonatkozó teljesítendő követelményeket.

## II.3. Az IBSZ kezelése

### II.3.1. Az IBSZ felülvizsgálata

9) Az IBSZ felülvizsgálatára az alábbiak szerint kerül sor:

a) évente egy alkalommal, a belső felülvizsgálatok során;
b) minden olyan esetben, amikor az IBSZ-ben leírtakhoz képest jelentős változás történik, a szabályozási környezetben, valamint az infokommunikációs területet a *Szervezeti és működési szabályzat* szintjén érintő változása esetén;
c) az eredeti szabályozás alapjait érintő minden változás (új kockázatok, új káresemények, új veszélyhelyzetek, és a műszaki infrastruktúra átalakítása) esetén soron kívül;
d) a DKÜ Zrt. *Normaalkotási szabályzatában* meghatározott normafelülvizsgálati rendszerességgel.

10) A mindenkori felülvizsgálat végrehajtása az információbiztonsági felelős (a továbbiakban: IBF) feladata az érintett munkatársak közreműködésével.

### II.3.2. Az IBSZ oktatása

11) Az IBSZ előírásait a hatálya alá tartozók tevékenységük során kötelesek betartani, melyre tekintettel a Szabályzat tartalmának megismerését valamennyi érintett számára biztosítani kell. Minden új belépő köteles a belépést követő 30 napon belül megismerni az IBSZ tartalmát. Valamennyi érintett foglalkoztatott esetében kötelező az ismeretek évenként történő felfrissítése, megerősítése.

12) A DKÜ Zrt. a Szabályzat előírásainak megismerését, frissítését és megerősítését elektronikus úton továbbított oktatási anyagok segítségével biztosítja. Ennek megvalósításáért az IBF a humánerőforrás-gazdálkodási területtel (a továbbiakban: HR terület) együttműködve felelős.

### II.3.3. Az IBSZ szabályozási környezete

13) A Szabályzatot elsődlegesen az alábbi belső normákkal összhangban kell alkalmazni:

a) Adatvédelmi szabályzat;
b) Alapszabály;
c) Belső Kontrollrendszer Kézikönyv;
d) Beszerzési szabályzat;
e) Hasznosítási és selejtezési szabályzat;
f) Humán erőforrás szabályzat;
g) Integrált Irányítási Kézikönyv;
h) Integrált kockázatkezelési szabályzat;
i) Jogosultságkezelési szabályzat;
j) Kötelezettségvállalási szabályzat;
k) Közbeszerzési szabályzat;
l) Központosított közbeszerzési szabályzat;
m) Normaalkotási szabályzat;
n) Szervezeti és működési szabályzat;
o) Tűzvédelmi szabályzat.

14) A Szabályzathoz az alábbi eljárásrendek, folyamatleírások kapcsolódnak:

a) Adminisztratív eljárásrend;
b) Biztonságelemzési eljárásrend;
c) Fizikai biztonsági eljárásrend saját gépterem üzemeltetésre;
d) Információbiztonsági incidensek kezelése folyamatleírás;
e) Informatikai katasztrófaelhárítási eljárásrend (DRP eljárásrend);
f) Jogosultságkezelés folyamatleírása;
g) Képzések tervezése, megvalósítása folyamatleírás;
h) Konfigurációkezelési eljárásrend;
i) Logikai védelmi eljárásrend;
j) Mentési és archiválási eljárásrend;
k) Naplózási eljárásrend;
l) Rendszer- és kommunikációvédelmi eljárásrend;
m) Üzletmenet-folytonossági eljárásrend (BCP eljárásrend).

15) A Szabályzatot – elsősorban, de nem kizárólag – az alábbi jogszabályokkal, szabványokkal összhangban kell alkalmazni:

a) 2024. évi LXIX. törvény Magyarország kiberbiztonságáról;
b) 7/2024 MK rendelet (VI.24.) a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről;
c) 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról;
d) MSZ ISO/IEC 27001:2023 Információbiztonság, kiberbiztonság és a magánélet védelme. Információbiztonság-irányítási rendszerek. Követelmények szabvány (IBIR szabvány).

### II.3.4. Az IBSZ hatálya

16) Az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörökhöz rendelt tevékenységet, a tevékenységhez kapcsolódó felelősséget a Kibertv. szabályozza.

17) Az IBSZ személyi hatálya kiterjed:

a) a DKÜ Zrt. valamennyi munkavállalójára, a DKÜ Zrt.-nél üzemeltetett, felügyelete alá tartozó elektronikus információs rendszerek fejlesztőire, üzemeltetőire, beszállítóira, közreműködőire;
b) a DKÜ Zrt.-vel eseti (szerződéses) munkakapcsolatban lévő személyekre, amelyeknek érvényesülését a velük kötött szerződések tartalmának megfelelő kialakításával kell biztosítani.

18) Az IBSZ tárgyi hatálya kiterjed:

a) A DKÜ Zrt.-nél üzemeltetett, felügyelete alá tartozó elektronikus információs rendszerekre, valamint az azokban gyűjtött, tárolt, feldolgozott, továbbított és megjelenített adatokra.
b) A DKÜ Zrt. infokommunikációs infrastruktúrájára.
c) A DKÜ Zrt. belső infokommunikációs folyamataiban, illetve az általa nyújtott és igénybe vett infokommunikációs szolgáltatásokban kezelt valamennyi okmányra, dokumentációra, utasításra, szabályzatra.
d) Az infokommunikációs infrastruktúra által kezelt, a DKÜ Zrt.-hez köthető adatok és információk teljes körére (függetlenül keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól).
e) A DKÜ Zrt. által kezelt adathordozókra, azok tárolására és felhasználására, beleértve a beérkezés, szétosztás és selejtezés/megsemmisítés folyamatait is.

### II.3.5. Értelmező rendelkezések, alapfogalmak, rövidítések

19) A Szabályzatban előforduló fogalmakat, rövidítéseket az alábbiak szerint kell értelmezni:

| Fogalom, rövidítés (betűrendben) | Értelmezés |
|---|---|
| BCP: | Üzletmenet-folytonossági terv. |
| Biztonsági osztályba sorolás: | A Kibertv 4. § 17. pontja szerinti fogalom:<br>A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. |
| CSIRT: | Számítógép-biztonsági és incidenskezelő csoport. |
| DRP: | Katasztrófa-helyreállítási terv. |
| EIR: | DKÜ Zrt.-nél üzemeltetett, vagy a DKÜ Zrt. felügyelete alá tartozó elektronikus információs rendszerek. |
| Életciklus: | A Kibertv 4. § 26. pontja szerinti fogalom:<br>Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam. |
| Infokommunikációs elem: | berendezés, eszköz, rendszer, hálózat, beleértve mindezek hardver és szoftver elemeit, valamint az infokommunikációs infrastruktúrához kapcsolódó |

| Fogalom, rövidítés (betűrendben) | Értelmezés |
|---|---|
| | fejlesztési (tervezési, projekt, használatba vételi stb.) és üzemeltetési (felhasználói, biztonsági, selejtezési stb.) és dokumentációt (leírást, utasítást, szabályzatot, feljegyzést stb.) is. |
| Infokommunikációs folyamat: | az infokommunikációs infrastruktúra által megvalósított informatikai vagy kommunikációs tevékenységek összessége. |
| Infokommunikációs infrastruktúra: | a DKÜ Zrt. tulajdonában lévő és/vagy általa kezelt, tárolt vagy EIR-jében, rendszerében használt infokommunikációs infrastrukturális elemek összessége. |
| Információbiztonsági esemény: | Bármely nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az információbiztonság-irányítás hatálya alá tartozó elemekben vagy elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idézhet elő, vagy amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elveszhet, vagy megsérülhet. |
| Információbiztonsági incidens: | Bármely 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. |
| Információbiztonsági szabályozások: | IBSZ, az IBSZ-hez kapcsolódó eljárásrendek, folyamatleírások, *Jogosultságkezelési szabályzat.* |
| Kiberbiztonsági incidens: | A Kibertv 4. § 46. pontja szerinti fogalom:<br>Olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát |
| Kockázatelemzés: | A Kibertv 4. § 55. pontja szerinti fogalom:<br>Az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése. |
| Kriptográfia: | Mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek információnak |

| Fogalom, rövidítés (betűrendben) | Értelmezés |
|---|---|
| | illetéktelenek előli elrejtését hivatottak megvalósítani. |
| Sérülékenységvizsgálat: | A Kibertv 4. § 89. pontja szerinti fogalom: Sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre. |
| Szakterületi vezető: | a DKÜ Zrt. Szervezeti és működési szabályzatában szakterületként meghatározott szervezeti egység vezetője: vezérigazgató, vezérigazgató-helyettes, igazgató. |
| Szervezeti egység vezető: | a DKÜ Zrt. Szervezeti és működési szabályzatában megjelenített szervezeti egység vezetője: csoportvezető, igazgató, vezérigazgató-helyettes. |
| Titkosítás: | A titkosítás a kriptográfiának az az eljárása, amellyel az információt (nyílt szöveg) egy algoritmus (titkosító eljárás) segítségével olyan szöveggé alakítjuk, ami olvashatatlan olyan ember számára, aki nem rendelkezik az olvasáshoz szükséges speciális tudással. Ez a speciális tudás az, amit általában kulcsnak nevezünk. |

## II.4. A védelem tárgya, eszközei és működése

### II.4.1. A védelem tárgya

20) A védelem tárgya a DKÜ Zrt. EIR infrastruktúrája és infokommunikációs folyamatai biztonságának megteremtése és fenntartása. E tekintetben a DKÜ Zrt. EIR infrastruktúrájának környezete és rendszerelemei a következőek:

a) hardver rendszerek;
b) szoftver rendszerek;
c) kommunikációs, hálózati rendszerek;
d) adathordozók;
e) dokumentumok és dokumentáció;
f) személyi környezet (külső és belső).

21) A védelem tárgya a fentiekre vonatkozóan:

a) az EIR infrastruktúra elemeinek működési biztonsága;
b) az EIR infrastruktúra fejlesztéséhez és üzemeltetéshez szükséges okmányok, dokumentációk;
c) az adatok és információk, valamint az adathordozók dokumentált megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig;
d) az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

22) A védelem működése, eszközei:

a) A Szabályzatban meghatározott védelemnek működnie kell az EIR-ek teljes életciklusának időtartama alatt, a megtervezésüktől kezdve a beszerzésükön, fejlesztésükön és üzemeltetésükön keresztül egészen a használatból való kivonásukig (a továbbiakban együttesen: az EIR alkalmazása). A Szabályzatban meghatározott védelmet kell alkalmazni a DKÜ Zrt. EIR-jeit érintő belső folyamatokra vonatkozóan.
b) Az IBSZ működtetése során kockázatalapú megközelítéssel, a kívánt biztonsági szint beállításával kezeli a kockázatokat azok megelőzésétől, felmérésétől, besorolásától kezdve az alkalmazott eljárásrendig és konkrét intézkedésekig. Az IBSZ kockázatkezelése ciklikus tevékenység, amely a sérülékenység, a veszélyforrások és a lehetséges következmények alapján a valószínűségek súlyozásával alakítja ki és működteti a kockázattal arányos mértékű védelmet. A védelem eszközei fizikai, személyi, szervezeti, adminisztratív (technikai, jogi, ügyrendi) összetevőkből állnak.

### II.4.2. Az informatikai biztonság szervezete

#### II.4.2.1. Vezérigazgató

23) A vezérigazgató, mint a DKÜ Zrt. szervezetének vezetője:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését;
b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését;
c) meghatározza a DKÜ Zrt. elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve jóváhagyja, kiadja az IBSZ-t;
d) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról;
e) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak;
f) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről;
g) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről;
h) ha az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy a Kibertv. -ben foglaltak szerződéses kötelemként teljesüljenek;
i) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy a Kibertv. -benfoglaltak szerződéses kötelemként teljesüljenek;
j) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért;
k) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

#### II.4.2.2. Szakterületi vezető

24) Felelős azért, hogy a vezetése alatt álló szakterületek, szervezeti egységek betartsák az informatikai biztonsági követelményeket.

25) Feladata a vezetése alatt álló szakterület, szervezeti egység tekintetében:

a) a hozzáférési jogosultság igények (beállítás, visszavonás) kezdeményezése;
b) a szervezeti egység által gyűjtött adatok biztonsági osztályba sorolása;
c) szakterületen belül az adatgazda kijelölése;
d) a rendellenes használattal kapcsolatos ügyek kivizsgálása.

### II.4.2.3. Az adatgazda

26) Az adatgazda feladata és hatásköre:

a) a használt adatok meghatározása és csoportosítása biztonsági és védelmi szint alapján;
b) besorolja az adatokat;
c) kockázatelemzést végez;
d) elvégzi az üzleti hatáselemzést a módszertanok alapján;
e) meghatározza az összeférhetetlen szerepköröket;
f) jóváhagyja a jogosultság igényeket;
g) évente felülvizsgálja a jogosultságokat.

### II.4.2.4. Biztonsági vezető

27) A Biztonsági vezető feladata és hatásköre:

a) Felel a DKÜ Zrt. működéséhez kapcsolódó üzleti adatok sértetlenségéért, bizalmasságáért, rendelkezésre állásáért.
b) Az érintett szakterületekkel együttműködve betartja és betartatja az információbiztonsági előírásokat, azokra vonatkozóan javaslatokat készít.
c) Az érintett szakterületekkel együttműködik az elektronikus információs rendszerek és elektronikus felületek megfelelő biztonsági szintű környezetének kialakításában és fejlesztésében.
d) Felügyeli a DKÜ Zrt. elektronikus információs rendszereinek védelmét.
e) Közreműködik az elektronikus információs rendszereket érő információbiztonsági incidensek elhárításában, továbbá felel ezen incidensek kivizsgálásáért és kezeléséért, működteti és vezeti az információbiztonságra vonatkozó Incidenskezelő csoportot.
f) Felelős az elektronikus információs rendszerek sérülékenységvizsgálatáért, ezzel összefüggő cselekvési tervek készítéséért és azok végrehajttatásáért, bevonva az érintett szakterületeket.
g) Információbiztonsági szempontú ajánlásokat és elvárásokat fogalmaz meg az elektronikus információs rendszerek tervezésével, fejlesztésével, üzemeltetésével kapcsolatban.
h) Jelenti a vezérigazgatónak az informatikai biztonságot érintő eseményeket, illetve tájékoztatja az eseményről és annak részleteiről.
i) Vizsgálatot kezdeményez az informatikai biztonságot érintő esemény kapcsán.
j) Bármely érintett szervezeti egységnél jogosult az IBSZ rendelkezései betartásának ellenőrzésére.
k) Az informatikai biztonsági előírások megsértőivel szemben felelősségre vonási eljárást kezdeményezhet.
l) Gondoskodik az üzleti hatáselemzés módszertanáról.

### II.4.2.5. Információbiztonsági felelős (IBF)

28) Az IBF feladata és hatásköre:

a) koordinálja az IBSZ-ben foglaltak szakszerű végrehajtását;
b) folyamatosan figyeli a Computer Security Incident Response Team (a továbbiakban: CSIRT) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket;
c) folyamatosan figyelemmel kíséri a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet értesítéseit; szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki; a belső biztonsági riasztást és figyelmeztetést eljuttatja az illetékes személyekhez;
d) felügyeli a védelem eljárásrendjének kialakítását;
e) karbantartja az információbiztonsági szabályozásokat;
f) a szakterületek bevonásával felügyeli a biztonságot növelő intézkedéseket;
g) információbiztonsági, üzletmenetfolytonossági teszteket kezdeményez az *Üzletmenet-folytonosság eljárásrend* szerinti módszertan alapján;
h) koordinálja a biztonsági események kezelését, elhárítását;
i) súlyos biztonsági esemény elhárítása után kezdeményezi az IBSZ, illetve egyéb információbiztonsági szabályozások felülvizsgálatát, valamint rendkívüli biztonsági auditot kezdeményezhet bármely EIR-re vonatkozóan;
j) biztosítja az IBSZ hatálya alá tartozók számára az IBSZ, illetve az IBSZ változásainak megismerését és az ismeretek folyamatos szinten tartását a HR terület közreműködésével;
k) ellenőrzi az informatikai biztonságot érintő szabályok előírásainak, eljárásrendjének a működés során való betartását;
l) kapcsolatot tart a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézettel és a CSIRT-tel, továbbá szükség esetén egyéb hatóságokkal;
m) az Ibtv. hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatja a jogszabályban meghatározott szervet;
n) közreműködik a szervezet valamennyi elektronikus információs rendszerének a tervezésében, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében;
o) biztonsági incidens jelentést készít és vezeti a biztonsági incidens jelentések nyilvántartását;
p) javaslatot tesz az új védelmi eszközök beszerzésére, illetve védelmi technológiák, eljárások bevezetésére;
q) javaslatot tesz az informatikai biztonságot érintő, a biztonság szinten tartását és növelését célzó költségvetési tételekre, azok módosítására;
r) informatikai biztonsági szempontból megelőző intézkedéseket kezdeményez;
s) megfigyelőként részt vesz az informatikai biztonsági auditon, valamint előzetesen véleményezi a biztonsági audit megállapításait, javaslatokat tesz az audit megállapításaira.

### II.4.2.6. Stratégiai és biztonsági igazgatóság (SBI)

29) A Stratégiai és biztonsági igazgatóság (a továbbiakban: SBI) feladata és hatásköre:

a) A Rendszerbiztonsági terv elkészítése és felülvizsgálata;
b) Harmadik fél adatközpontjára vonatkozó biztonsági követelmények megállapítása, a követelményeknek való megfelelőség megállapítása az elektronikus információs rendszerek kihelyezése esetén;

c) Sérülékenység vizsgálatok lefolytatása az elektronikus információs rendszerekre;
d) Elektronikus információs rendszerek biztonsági helyzetének figyelemmel kísérése azok teljes életútján.

## II.5. Szervezeti szintű alapfeladatok

30) A fejezetben meghatározott védelmi intézkedések, eszközök és módszerek a 7/2024 MK rendelet, valamint a DKÜ Zrt. biztonsági érettsége alapján az alábbiak szerint kerülnek meghatározásra.

31) A DKÜ Zrt. az információbiztonsági-irányítási rendszer bevezetése és fenntartása érdekében előre meghatározott feladatokat rögzít, ami az *Adminisztratív védelmi eljárásrend*ben található.

### II.5.1. Intézkedési terv

32) A DKÜ Zrt. intézkedési terve az IBF és az üzemeltető által azonosított koncepcionális hiányosságok javítására, valamint az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányul.

33) Az intézkedési terv tartalmi követelményeit, IBF feladatait, illetve a felülvizsgálatra vonatkozó előírásokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

### II.5.2. Az elektronikus információs rendszerek nyilvántartása

34) A DKÜ Zrt. az EIR-ekről folyamatosan aktualizált nyilvántartást vezet, amelynek tartalmi követelményeit az *Adminisztratív védelmi eljárásrend* tartalmazza. A nyilvántartás naprakészen tartásáért az IBF a felelős.

### II.5.3. Biztonsági elemzés, teljesítmény mérése

35) A DKÜ Zrt. évente, kockázattal arányosan értékeli az elektronikus információs rendszer és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését. A biztonsági elemzés és teljesítmény mérése a *Logikai védelmi eljárásrendben* található részletesen. A biztonsági elemzés módszereként a DKÜ Zrt. által alkalmazott elektronikus információs rendszerek osztályba sorolásának felülvizsgálata figyelembe vehető.

### II.5.4. Az elektronikus információbiztonsággal és annak jogosultságaival kapcsolatos engedélyezési eljárás

36) Az EIR-ekkel kapcsolatos felhasználói, külső és belső hozzáférések engedélyezése a *Logikai védelmi eljárásrend* és a *Jogosultságkezelési szabályzat* szerint történik. A hozzáféréssel kapcsolatos beállítási igényeket minden esetben az érintett EIR adatgazdája engedélyezi.

37) Az információbiztonsággal összefüggő felelősségi köröket az IBSZ II.4.2 fejezete határozza meg.

### II.5.5. Kapcsolattartás

38) A DKÜ Zrt. az érintett szervezetekkel, az ágazati szervezetekkel és a hatóságokkal a rendelkezésre álló feltételrendszer alapján kapcsolatrendszert alakít ki és tart fenn, az *Adminisztratív védelmi eljárásrend* alapján.

### II.5.6. A DKÜ Zrt. szempontjából kritikus rendszerek, erőforrások kezelése

39) A DKÜ Zrt. a Kockázatelemzés során azonosított kritikus rendszerek, erőforrások vonatkozásában Rendszerbiztonsági tervet dolgoz ki, mely tervben kidolgozza, dokumentálja, valamint évente egy alkalommal frissíti a dokumentum tartalmát. A Rendszerbiztonsági terv azokat a követelményeket tartalmazza, melyeket a kritikusnak minősülő rendszerek, erőforrások vonatkozásában alkalmazni szükséges. A Rendszerbiztonsági terv elkészítéséért és felülvizsgálatáért az SBI felelős.

### II.5.7. Felügyeleti stratégia

40) A felügyeleti stratégiára vonatkozó szabályokat, valamint a kapcsolódó vizsgált teljesítménymutatókat részletesen a *Logikai védelmi eljárásrend* tartalmazza.

## III. Hozzáférés-felügyelet

### III.1. Hozzáférés ellenőrzési eljárásrend

41) A DKÜ Zrt. a *Jogosultságkezelési szabályzatban* határozza meg a jogosultságkezelési, engedélyezési és nyilvántartási feladatait.

### III.2. Felhasználói fiókok kezelése, fiókkezelés

42) A felhasználó fiókok kezelése utasítást a *Logikai védelmi eljárásrend* tartalmazza.

### III.3. Hozzáférés ellenőrzés érvényesítése

43) A jelszavakhoz rendelt hozzáférési jogok kizárólag az adott felhasználó hatáskörébe tartoznak, azokért az adott felhasználó tartozik felelősséggel.

44) A normál napi üzletmenetben a számon kérhetőség érdekében csak személyhez kötött azonosítók használhatóak. A személyekhez nem kötött azonosítók esetében a rendszerjelszó-menedzsment szabályai a *Logikai védelmi eljárásrendben* foglaltak szerint kell eljárni.

45) Az informatikai eszközöket minden felhasználó csak a saját személyi azonosítójával és jelszavával használhatja. A jelszót titokban kell tartani, a személyes felhasználói azonosítóhoz tartozó jelszót más személy tudomására hozni tilos.

46) A felhasználói jelszavakra vonatkozók szabályok és egyéb hozzáférési szabályok a *Logikai védelmi eljárásrendben* találhatóak.

### III.4. A felhasználók hozzáféréssel kapcsolatos kötelességei, felelősségek szétválasztása

47) Az operációs rendszerekhez való adminisztrátori szintű hozzáférés csak rendszerüzemeltetők számára engedélyezett.

### III.5. Legkisebb jogosultság elve

48) A legkisebb jogosultság elvére vonatkozó szabályokat részletesen a *Logikai védelmi eljárásrend* tartalmazza.

### III.6. Sikertelen bejelentkezési kísérletek

49) A sikertelen bejelentkezési kísérleteket naplózni kell a Naplózási eljárásrend előírásainak megfelelően.

### III.7. A rendszerhasználat jelzése

50) A jelentős biztonsági osztályú vagy annál nagyobb besorolású EIR-ek esetén a rendszer a használatra vonatkozó figyelmeztető üzenetet vagy jelzést küld a felhasználó számára, amelynek tartalma a *Logikai védelmi eljárásrendben* található.

51) Az elektronikus információs rendszer a nyilvánosan elérhető rendszerek esetén kijelzi a rendszerhasználat feltételeit, mielőtt további hozzáférést biztosít amennyiben felügyelet, adatrögzítés vagy naplózás történik, kijelzi, hogy ezek megfelelnek az adatvédelmi szabályoknak, leírást biztosít a rendszer engedélyezett felhasználásáról.

### III.8. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

52) A DKÜ Zrt.-nél az EIR-ekben azonosítás vagy hitelesítés nélkül engedélyezett tevékenységeket a EIR-ek *Rendszerbiztonsági tervei* tartalmazzák.

### III.9. Távoli hozzáférés

53) Távoli munkavégzés során kizárólag a DKÜ Zrt. által biztosított és központilag menedzselt eszközzel szabad csatlakozni a belső hálózathoz.

54) A távoli hozzáférésre vonatkozó szabályokat részletesen a *Logikai védelmi eljárásrend* tartalmazza.

### III.10. Vezeték nélküli hozzáférés

55) A vezeték nélküli hozzáférésre vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### III.11. Mobil eszközök hozzáférés ellenőrzése

56) A mobil eszközök hozzáférés ellenőrzésére vonatkozó szabályait a *Logikai védelmi eljárásrend* tartalmazza.

### III.12. Külső elektronikus információs rendszerek használata

57) A külső elektronikus információs rendszerek használatára vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### III.13. Nyilvánosan elérhető tartalom, információmegosztás

58) A nyilvánosan elérhető tartalomra, valamint az információmegosztásra vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

## IV. Tudatosság és képzés

### IV.1. Képzési eljárásrend

59) Az informatikai biztonság tudatosítása érdekében a DKÜ Zrt. munkavállalói részére évente legalább egy alkalommal oktatásokat, képzéseket kell tartani az *Adminisztratív védelmi eljárásrendben* leírtak szerint.

### IV.2. Biztonságtudatossági képzés

60) Az új belépők képzése a *Humán erőforrás szabályzat* mellékletében foglalt információbiztonsági tájékoztató megismerésével, illetve az *Adminisztratív védelmi eljárásrend* alapján valósul meg.

### IV.3. Szerepkör, vagy feladat alapú biztonsági képzés

61) Az oktatásokat a képzésben részt vevő munkatársak szerepköre alapján kell megszervezni, minden esetben figyelembe véve az adott szerepkörhöz kapcsolódó kockázatokat. Az oktatásoknak ki kell terjedni az *Adminisztratív védelmi eljárásrendben* leírtakra.

### IV.4. A biztonsági képzésre vonatkozó dokumentációk

62) A biztonsági képzésre vonatkozó dokumentációkra vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

## V. Naplózás és elszámoltathatóság

### V.1. Naplózási eljárásrend

63) Az egyes EIR-ekre vonatkozó naplózás szabályozása egyedileg történik. Ezeket az általános elvárások szintjén a követelmény specifikációkban kell rögzíteni. A naplózás szabályait és folyamatát a *Naplózási eljárásrend* tartalmazza.

## VI. Értékelés, engedélyezés és monitorozás

### VI.1. Biztonsági értékelések

64) A DKÜ Zrt. értékeli az általa működtetett elektronikus információs rendszerek és azok működési környezetének védelmi intézkedéseit. A biztonsági értékelés szabályait és folyamatát a *Biztonságelemzési eljárásrend* tartalmazza.

### VI.2. Informatikai biztonsági rendszer felülvizsgálata, folyamatos felügyelet

65) Az informatikai biztonsági rendszer felülvizsgálatára, folyamatos felügyeletére vonatkozó szabályokat a *Biztonságelemzési eljárásrend* tartalmazza.

### VI.3. Az elektronikus információs rendszer kapcsolódásai

66) Az engedélyezésre, valamint a folyamatos felügyeletre vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza, az elektronikus információs rendszer kapcsolódásait a *Rendszerbiztonsági tervek* tartalmazzák.

### VI.4. Személyi biztonság

67) A DKÜ Zrt.-n belüli személyi biztonsággal összefüggő felhasználói jogokat a *Logikai védelmi eljárásrend* tartalmazza.

## VII. Konfigurációkezelés

68) DKÜ Zrt.-nél a konfigurációkezelésre vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.1. Biztonsági hatásvizsgálat

69) A DKÜ Zrt. az elektronikus információs rendszerekben végrehajtott módosítások után ellenőrzi, hogy a védelmi intézkedések helyesen lettek-e bevezetve, megfelelően működnek-e, és biztosítják-e a kívánt eredményeket, figyelembe véve az elektronikus információs rendszer biztonsági követelményeit.

70) A biztonsági hatásvizsgálatra vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.2. Konfigurációs beállítások

71) A konfigurációs beállításokra vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

72) A konfigurációs beállítások változtatásait, a változáskezelés szabályainak megfelelően kell elvégezni.

### VII.3. A konfigurációváltozások felügyelete (változáskezelés)

73) A konfigurációváltozások felügyeletére vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.4. Legszűkebb funkcionalitás

74) Az EIR-ek tervezésekor és módosításaikor a konfigurációt úgy kell meghatározni, hogy az csak a szükséges és elégséges szolgáltatásokat nyújtsa. Ennek során tervezési elvként meghatározandók a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek.

75) Amennyiben a szoftver beszerzése kötelezettségvállalással jár, a DKÜ Zrt. *Kötelezettségvállalási szabályzata* és – a beszerzés eljárásrendjétől függően – a *Beszerzési szabályzata* vagy a *Közbeszerzési szabályzata* szerint kell eljárni.

76) Az informatikai biztonsági célkitűzéseknek nem megfelelő, illetve hibás, nem javítható eszközöknek véglegesen ki kell kerülniük az informatikai biztonsági rendszerből.

77) A legszűkebb funkcionalitásra vonatkozó szabályokat részletesen a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.5. Információs rendszerelem leltár

78) A rendszerelem leltárra vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.6. A szoftverhasználat korlátozásai

79) A szoftverhasználat korlátozásaira vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

### VII.7. A felhasználó által telepített szoftverek

80) A felhasználó által telepített szoftverekre vonatkozó szabályokat a *Konfigurációkezelési eljárásrend* tartalmazza.

## VIII. Üzletmenet folytonosság tervezése

81) Az üzletmenet folytonossági tervek elkészítésével kapcsolatos elvárásokat az *Üzletmenet-folytonossági eljárásrend* tartalmazza.

82) A helyreállítási terveket az *Informatikai katasztrófaelhárítási eljárásrend* figyelembevételével kell elkészíteni.

### VIII.1. Üzletmenet folytonossági terv informatikai erőforrás kiesésekre

83) Az egyes EIR-ekre vonatkozó üzletmenet folytonossági tervekben meg kell határozni az érintett szolgáltatás szempontjából kulcsfontosságú szereplőket. Az egyes üzletmenet-folytonossági terveket kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kell ismertetni.

84) Az üzletmentfolytonossági tervek felülvizsgálatát, publikálhatóságát, tartalmi elemeit, a folyamatos működésre felkészítő képzés kritériumait az *Adminisztratív védelmi eljárásrend* tartalmazza.

### VIII.2. BCP akciótervek oktatása, folyamatos működésre felkészítő képzés

85) A BCP akciótervek tartalmi követelményeire vonatkozó szabályokat az *Üzletmenet-folytonossági eljárásrend* tartalmazza.

86) A folyamatos működésre felkészítő képzésre vonatkozó szabályokat az *Üzletmenet-folytonossági eljárásrend* tartalmazza.

### VIII.3. Az elektronikus információs rendszer mentései

87) Az elektronikus információs rendszer mentéseire vonatkozó szabályokat a *Mentési és archiválási eljárásrend* tartalmazza.

88) Gondoskodni kell az elektronikus információs rendszereken hozzáférhető érzékeny adatok és az EIR-ek dokumentációjának biztonsági mentéséről és archiválásáról.

89) Az adat visszaállítási eljárásoknak az a céljuk, hogy az informatikai biztonság elveinek érvényesítése érdekében az EIR-ben tárolt adatok egy korábbi állapotát állítsák vissza. A mentések gyakoriságát a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal összhangban szükséges megállapítani.

### VIII.4. Üzletmenet-folytonossági terv tesztelése

90) A BCP akciótervek tesztelésére vonatkozó szabályokat az *Üzletmenet-folytonossági eljárásrend* tartalmazza.

### VIII.5. Az elektronikus információs rendszer helyreállítása és újraindítása

91) Az elektronikus információs rendszerek helyreállításait és újraindítását az egyes EIR-ekre vonatkozó *Informatikai katasztrófaelhárítási eljárásrend* előírásainak megfelelően kell elvégezni.

## IX. Azonosítás és hitelesítés

### IX.1. Azonosítás és hitelesítés

92) Az azonosítási és hitelesítési elvárások teljesülését a *Logikai védelmi eljárásrend* szerint szükséges ellenőrizni.

### IX.2. A felhasználói hozzáférés kezelése

93) A DKÜ Zrt. az elektronikus információs rendszerekben bejelentkezési és kilépési gyakorlatot alkalmaz az EIR-ekhez és a szolgáltatásokhoz történő hozzáférés biztonsága érdekében. A felhasználói hozzáférések kezelésének pontos szabályait a *Logikai védelmi eljárásrend* tartalmazza.

### IX.3. Azonosító kezelés

94) Az azonosítók kezelésére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### IX.4. Hálózati hozzáférés privilegizált fiókokhoz

95) A privilegizált fiókok hálózati hozzáférésére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### IX.5. A hitelesítésre szolgáló eszközök kezelése

96) A felhasználók hozzáférési jogai minden év végén, munkakörének vagy munkafeladatainak változásakor, illetve biztonsági incidensek bekövetkezésekor felülvizsgálatra kerülnek, a felhasználói jogosultságok aktuális állapotát tükröző listát az üzemeltető készíti és jóváhagyásra továbbítja a DKÜ Zrt. részére. A hitelesítésre szolgáló eszközök kezelését a *Logikai védelmi eljárásrend* tartalmazza.

### IX.6. A hitelesítésre szolgáló eszköz visszacsatolása

97) Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információkat a jogosulatlan személyek általi esetleges felfedésétől, felhasználásától.

### IX.7. Hitelesítés kriptográfiai modul esetén

98) Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

### IX.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

99) A DKÜ Zrt.-n kívüli felhasználók elektronikus információs rendszerhez történő hozzáférése során számukra a vonatkozó szabályoknak megfelelően egyedi azonosítókat kell létrehozni, biztosítani kell az egyedi azonosítást.

100) A DKÜ Zrt.-n kívüli felhasználók tevékenységének a naplózására kiemelt figyelmet kell fordítani.

### IX.9. Hitelesítés szolgáltatók tanúsítványának elfogadása

101) Az elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság (NMHH) elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítés szolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez.

### IX.10. Ellenőrzés

102) Az azonosítással és hitelesítéssel kapcsolatos előírások ellenőrzésére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

# X. Biztonsági incidensek, események kezelése

## X.1. Képzés a biztonsági események kezelésére

103) A biztonsági események kezelésére vonatkozó képzés szabályait az *Adminisztratív védelmi eljárásrend* tartalmazza.

## X.2. A biztonsági incidensek, események figyelése és jelentése

104) A biztonsági incidensek, események figyelése és jelentésére vonatkozó elvárásokat az *Adminisztratív védelmi eljárásrend*, valamint az *Információbiztonsági incidensek kezelése folyamatleírás* tartalmazza.

## X.3. A biztonsági incidensek, események kezelése, kivizsgálása

105) A biztonsági incidensekkel kapcsolatos vizsgálatok folyamatát, valamint a dokumentálás tartalmi követelményeit az *Adminisztratív védelmi eljárásrend* tartalmazza.

## X.4. Biztonsági események kezelésének tesztelése

106) A biztonsági események kezelésének tesztelésére vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

## X.5. Biztonsági eseménykezelési terv, incidenstípusok

107) A biztonsági eseménykezelési terv tartalmi követelményeire, valamint a biztonsági incidensek besorolására vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

## X.6. Az incidenskezeléshez kapcsolódó szerepkörök feladatai, felelősségei

108) Az incidenskezeléshez kapcsolódó szerepkörök feladatai és felelősségei az *Adminisztratív védelmi eljárásrend* rendelkezik.

# XI. Karbantartás

109) A DKÜ Zrt. elektronikus rendszereinek karbantartását a *Logikai védelmi eljárásrend* tartalmazza.

# XII. Adathordozók védelme

## XII.1. Hozzáférés az adathordozókhoz

110) A digitális adathordozókat azonosítóval kell ellátni, és erről nyilvántartást kell vezetni. Az adathordozók illetéktelen kézbe kerülése elleni védelem minden munkatárs felelőssége. Az adathordozók hozzáférési szabályait a *Logikai védelmi eljárásrend* tartalmazza.

## XII.2. Adathordozók címkézése

111) Az adathordozók megjelölésére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XII.3. Adathordozók tárolása

112) Az adathordozók tárolására vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XII.4. Adathordozók szállítása

113) Az adathordozók szállítására vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XII.5. Adathordozók törlése, információtörlés

114) A digitális adathordozó megsemmisítéséről vagy a digitális adathordozó törléséről jegyzőkönyvet kell készíteni, a megsemmisítés során a *Hasznosítási és selejtezési szabályzat*, a *Biztonságos adattörlési eljárásrend* és a *Logikai védelmi eljárásrend* iránymutatásait is figyelembe kell venni.

### XII.6. Adathordozó kriptográfiai védelme

115) Az adathordozók kriptográfiai védelmére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XII.7. Adathordozók használata

116) Az adathordozók használatára vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

## XIII. Fizikai és környezeti védelem

117) A DKÜ Zrt. fizikai védelmi intézkedéseit a *Fizikai biztonsági eljárásrend* tartalmazza.

### XIII.1. Biztonsági területek

#### XIII.1.1. Biztonsági zónák meghatározása

118) Felhasználói helyiség: a DKÜ Zrt. tulajdonában lévő, felhasználói célra kiadott informatikai eszközök elhelyezésére szolgáló helyiség.

119) Biztonsági zóna: kiemelten védendő terület, ahol szervergépek, központi adattárak, biztonsági mentéseket végrehajtó és egyéb érzékeny adatokat tároló informatikai eszközök helyezkednek el.

a) Raktár: tartalékeszközök, mentési adathordozók, javításra váró eszközök stb. tárolására szolgáló hely.
b) Szerverterem: szerverek elhelyezésére szolgáló helyiség.

#### XIII.1.2. Zónák védelme

120) Felhasználói helyiségek védelme:

a) Azokat a helyiségeket, ahol informatikai eszköz van, zárható ajtóval kell ellátni.
b) Onnan való távozáskor minden esetben be kell zárni (a távozás időtartalmától függetlenül).

121) Raktárak védelme a felhasználói helyiségekre vonatkozó védelmi szabályokon túl:

a) Az informatikai eszközök raktárába kizárólag a *Jogosultságkezelési szabályzat* szerint biztosított jogosultsággal lehet belépni.

122) Szervertermek és mentések üzemelésére szolgáló termek védelmére vonatkozó szabályokat a *Fizikai védelmi eljárásrend* tartalmazza.

### XIII.2. Fizikai belépési engedélyek

123) Rendszeresen, de legalább évente felül kell vizsgálni a belépésre jogosult személyek listáját. A jogosultság megszűnésekor ki kell vezetni a belépésre jogosult személyek listájáról azokat, akiknek a belépése nem indokolt – ezzel együtt a kiadott belépőkártyát vissza kell vonni.

### XIII.3. A fizikai belépés ellenőrzése

124) A DKÜ Zrt. területére kizárólag a beléptető kártyával és rendszerrel védett meghatározott be-, és kilépési pontokon biztosított a belépésre jogosultak számára a fizikai belépést. A fizikai belépéseket naplózni kell. Jogosulatlan belépési kísérletnek minősül, a többszöri belépési kísérlet a védett munkaterületre kilépés nélkül, valamint a munkaidőtől jelentősen eltérő időpontban történő belépés kísérlete.

125) Az épületben az ad-hoc belépésre jogosultakat a DKÜ Zrt. munkatársának kísérni és tevékenységüket figyelemmel követni szükséges.

126) Minden munkatárs köteles megóvni a rá bízott kulcsokat, a részükre kiadott belépőkártyát, és az egyéb fizikai hozzáférést biztosító vagy ellenőrző eszközöket.

127) Az egyéni belépési engedélyek ellenőrzése a belépési pontokon, beléptető rendszer, vagy biztonsági szolgálat segítségével történik, a belépésekről tételes nyilvántartás készül.

128) A belépőkártyák és kulcsok haladéktalanul megváltoztatandóak a kulcs elvesztése vagy a belépőkártya kompromittálódása esetén, vagy ha az adott személy elveszti a belépési jogosultságát.

129) A DKÜ Zrt. minden tagjának kötelessége az észlelt rendellenességek jelentése az IBF, a biztonsági vezető vagy az INI igazgató részére.

### XIII.4. A fizikai hozzáférések felügyelete

130) Az informatikai rendszerek szempontjából kiemelt helyiségekbe (pl. szervertermekbe) külön beléptető rendszert kell alkalmazni. A szervezeti egység vezető legalább fél évente átvizsgálja a fizikai hozzáférésekről készült naplókat, hogy észlelje a fizikai biztonsági eseményt. Ezen felül azonnal átvizsgálja a fizikai hozzáférésekről készült naplókat, ha a rendelkezésre álló információk jogosulatlan fizikai hozzáférésre utalnak a biztonsági események kezelésére vonatkozó szabályokkal összhangban.

### XIII.5. A látogatók ellenőrzése

131) Egy évig meg kell őrizni a Társaság székhelyén üzemelő elektronikus információs rendszereknek helyt adó létesítményekbe történt látogatói belépésekről szóló információkat. A biztonsági vezető, vagy megbízottja azonnal átvizsgálja a látogatói belépésekről készített információkat és felvételeket, ha a rendelkezésre álló információk jogosulatlan belépésre utalnak.

132) A látogatók ellenőrzésére vonatkozó szabályokat részletesen a *Fizikai védelmi eljárásrend* tartalmazza.

### XIII.6. Vészvilágítás

133) A vészvilágításra vonatkozó szabályokat a *Fizikai védelmi eljárásrend* tartalmazza.

### XIII.7. Tűzvédelem

134) Azok a helyiségek, ahol informatikai eszközök helyezkednek el, „D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent. A tűzvédelemmel kapcsolatos részletes szabályozás a DKÜ Zrt. *Tűzvédelmi szabályzatában* történik.

### XIII.8. Hőmérséklet és páratartalom ellenőrzés

135) A hőmérséklet és páratartalom ellenőrzésére vonatkozó szabályokat részletesen a *Fizikai védelmi eljárásrend* tartalmazza.

### XIII.9. Vezetéken szállított anyag okozta kár elleni védelem

136) A vezetéken szállított anyag okozta kár elleni védelem a *Fizikai biztonsági eljárásrendben* található.

### XIII.10. Be- és kiszállítás

137) A be- és kiszállítás részletes szabályait a *Fizikai védelmi eljárásrend* tartalmazza.

### XIII.11. Karbantartó személyek

138) A karbantartó szervezetekről és személyekről nyilvántartást kell vezetni (amely személyekre lebontva tartalmazza a jogosultság egyértelmű megállapításához szükséges adatokat – pl. név, személyi azonosító okmány száma stb.).

139) Az elektronikus információs rendszeren karbantartást végzőktől meg kell követelni a hozzáférési jogosultság igazolását.

140) Megfelelő jogosultságokkal nem rendelkező személyek karbantartási tevékenységet kizárólag DKÜ Zrt.-hez tartozó, a kívánt hozzáférési jogosultságokkal és műszaki szakértelemmel rendelkező személy(ek) felügyelete mellett végezhetnek.

141) A karbantartó személyekre vonatkozó részletes szabályokat a *Fizikai biztonsági eljárásrend* tartalmazza.

### XIII.12. Harmadik fél adatközpontjában elhelyezett rendszerek

142) A DKÜ Zrt. valamely elektronikus információs rendszerét akkor helyezheti ki harmadik fél adatközpontjába, ha a befogadó adatközpont adott rendszer biztonsági szintje által megkövetelt követelményének való megfelelőségről a DKÜ Zrt. az SBI útján hitelt érdemlően meggyőződik.

143) A DKÜ Zrt. rendszerének harmadik fél adatközpontjába való elhelyezése során olyan megállapodást kell kötnie, amely a DKÜ Zrt. számára biztosítja az érinett EIR biztonsági osztályához kapcsolódó elvárásoknak való megfelelés helyszíni ellenőrzésének lehetőségét.

# XIV. Tervezés

## XIV.1. Biztonságtervezési eljárásrend

144) A biztonságtervezéssel kapcsolatos követelmények részletes leírását az *Adminisztratív védelmi eljárásrend* tartalmazza.

## XIV.2. Rendszerbiztonsági terv

145) A rendszerbiztonsági tervre vonatkozó követelményeket a *Logikai védelmi eljárásrend* tartalmazza.

# XV. Személyi biztonság

146) A felhasználó felelősséggel tartozik a munkavégzés céljából átvett informatikai eszközökért, köteles megőrizni a munkaállomás hardver, szoftver és alkalmazás sértetlenségét (integritását). A felelősség vállalását és az eszközök átvételét átvételi elismervényben kell rögzíteni.

147) A felhasználó felelősségeit és kötelességeit az *Adminisztratív védelmi eljárásrend* tartalmazza.

## XV.1. Munkakörök, feladatok biztonsági szempontú besorolása

148) Minden munkakörhöz meg kell állapítani a munkakör betöltéséhez szükséges biztonsági feltételeket. A felelősségek meghatározott időre kell, hogy szóljanak. A munkakörök és feladatok biztonság szempontú besorolását évente felül kell vizsgálni. Az informatikai biztonsági szempontból kritikus munkakörök besorolását az *Adminisztratív védelmi eljárásrend* tartalmazza.

## XV.2. Személyek háttérellenőrzése

149) A munkaviszony létesítésének általános folyamatát a *Humán erőforrás szabályzat* tartalmazza. A szükséges munkakörök betöltésére általános és szakmai feltételeknek való megfelelés esetén nyílik lehetősége a pályázónak.

150) A felvételkor szükséges igazoló ellenőrzés elvégzéséért a HR terület felelős, amely magában foglalja az *Adminisztratív védelmi eljárásrendben* leírtakat.

## XV.3. Eljárás a jogviszony megszűnésekor, megváltozásakor

151) Jogviszony megszűnése, módosulása esetén az *Adminisztratív védelmi eljárásrend* szerint kell eljárni.

## XV.4. Az áthelyezések, átirányítások és kirendelések kezelése

152) Munkakör változás esetén az érintettek új szervezeti egység vezetője (ha ez nem változik, akkor az eredeti) – a HR területtel egyeztetve – kezdeményezi az érintett személyek ellenőrzésére vonatkozó eljárást. Szükség esetén kezdeményezi a logikai és fizikai hozzáférés engedélyezést az újonnan használni kívánt elektronikus információs rendszerhez. Az EIR-ekhez való hozzáférési jogosultságok munkakör-változással összefüggő kezelését a *Jogosultságkezelési szabályzat* szerint kell végrehajtani.

### XV.5. Hozzáférési megállapodások

153) A DKÜ Zrt. az elektronikus információs rendszerekhez történő hozzáférés során a jelen szabályzat *III. Hozzáférés-felügyelet* fejezet szabályai szerint jár el.

### XV.6. Külső személyekhez kapcsolódó biztonsági követelmények

154) A külső személyekhez kapcsolódó biztonsági követelményeket az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XV.7. Fegyelmi intézkedések

155) Fegyelmi eljárás kezdeményezhető az elektronikus információbiztonsági szabályokat és az ehhez kapcsolódó eljárásrendeket megsértő személyekkel szemben a *Humán erőforrás szabályzatban* előírtak szerint.

156) Szándékos emberi hiba, mulasztás vagy a DKÜ Zrt.-t érő erkölcsi és pénzügyi veszteség, hatás esetén a vezérigazgató - mint munkáltató - jár el az Mt. által szabályozott fegyelmi eljárás keretében.

157) Amennyiben az elektronikus információbiztonsági szabályokat nem a DKÜ Zrt. személyi állományába tartozó személy sérti meg, érvényesíteni kell a vonatkozó szerződésben meghatározott következményeket, megvizsgálandó az egyéb jogi lépések megtételének lehetőségét, és szükség szerint alkalmazni kell ezeket az eljárásokat.

### XV.8. Munkaköri leírás

158) A DKÜ Zrt. minden esetben meghatározza az adott személyhez kapcsolódó szerep- és felelősségi köröket a munkaköri leírásokban a feladatok szétválasztásának biztosítása érdekében

### XV.9. Viselkedési szabályok az internet használata során

159) Az internet használata során alkalmazandó viselkedési szabályokat az *Adminisztratív védelmi eljárásrend* határozza meg.

## XVI. Kockázatelemzés

160) A kockázatelemzési és kockázatkezelési eljárásrendet az *Integrált Irányítási Kézikönyv* szerinti Kockázatkezelési módszertani útmutató, valamint az *Integrált Kockázatkezelési Szabályzat* határozza meg, mely tartalmát és végrehajtását az *Adminisztratív védelmi eljárásrend* szabályozza.

### XVI.1. Biztonsági besorolások

161) A DKÜ Zrt. minden elektronikus információs rendszerét az adatok bizalmassága, hitelessége, sértetlensége, illetve elvesztésével arányos kárérték szintektől függően a Kibertv., az MK rendelet rendelkezéseinek megfelelően besorolja.

162) A DKÜ Zrt. elektronikus információs rendszereinek biztonsági osztályokba sorolását az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XVI.2. Fenyegetésfelismerő képesség

163) A DKÜ Zrt. folyamatosan nyomon követi a meglévő és az újonnan megjelenő belső és külső fenyegetéseket, valamint külső forrásokból is tájékozódik az újonnan

megjelenő fenyegetésekkel kapcsolatban (pl.: hatósági riasztások, figyelmeztetések).

164) A DKÜ Zrt. biztosítja az összegyűjtött információbiztonsági fenyegetésekkel kapcsolatos információk elemzését és értékelését a fenyegetésfelismerő képességének erősítése érdekében.

### XVI.3. Információosztályozás

165) Az információosztályokat és azok meghatározásait az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XVI.4. Tesztelés, képzés és felügyelet

#### XVI.4.1. Sérülékenységi teszt

166) A DKÜ Zrt. az elektronikus információs rendszere tekintetében sérülékenységi tesztet végeztet a *Logikai védelmi eljárásrend* szerint. A sérülékenység vizsgálatot végző személynek kötelező szerepelnie az Alkotmányvédelmi Hivatal regisztrációs listáján.

#### XVI.4.2. Frissítési képesség

167) A sérülékenységi teszteszközök frissítési képességére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

#### XVI.4.3. Privilegizált hozzáférés

168) A sérülékenységi teszt végrehajtásához kapcsolódó privilegizált hozzáférésre vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

#### XVI.4.4. Felfedhető információk

169) A sérülékenységi vizsgálat után az SBI-nek fel kell mérnie, hogy egy támadó milyen érzékeny adatokhoz lehet képes hozzáférni a DKÜ Zrt. információvagyonából. A vizsgálatot követően kockázatelemzés hatására a DKÜ Zrt. intézkedéseket foganatosít az érzékeny adatok megismerésének elhárítására.

## XVII. Rendszer és szolgáltatás beszerzés

170) A DKÜ Zrt. elektronikus információs rendszereinek informatikai biztonsági helyzetét azok teljes életútján az SBI figyelemmel kíséri. A DKÜ Zrt. a fejlesztések életciklusainak egészére meghatározza és dokumentálja az információbiztonsági szerepköröket és felelősségeket, valamint a DKÜ Zrt.-re vonatkozóan meghatározza az információbiztonsági szerepköröket betöltő személyeket.

171) Az elektronikus információs rendszer életciklusa során a *Logikai védelmi eljárásrendben* meghatározottak szerint kell eljárni.

### XVII.1. Erőforrás igény felmérés

172) Az elektronikus információs rendszer és annak szolgáltatásai védelméhez szükséges erőforrásokat, az üzleti tervezés és a beszerzések éves tervezése részeként a *Beszerzési szabályzat,* a *Közbeszerzési szabályzat* szerint meg kell határozni, és külön meg kell jelentetni a fejlesztési projektek során és már a projekt tervezése során be kell építeni az információbiztonsági követelményeket.

173) Az elektronikus információs rendszer beszerzésének engedélyezési folyamata az *Adminisztratív védelmi eljárásrendben* található.

### XVII.2. Beszerzések

174) A DKÜ Zrt. az elektronikus információs rendszerének teljes életútján figyelemmel kíséri az információbiztonsági helyzetet.

175) Az elektronikus információs rendszerre, rendszerelemre vagy szolgáltatásra irányuló beszerzési szerződésekben szerződéses követelményként meghatározandó feltételeket az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XVII.3. Az elektronikus információs rendszerre vonatkozó dokumentáció

176) A DKÜ Zrt. megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó, mindenkor aktuális üzemeltetési és felhasználói dokumentációt. A dokumentációkkal kapcsolatos előírásokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XVII.4. Biztonságos kódolás

177) A DKÜ Zrt. a fejlesztésekhez kapcsolódóan meghatározza és a vonatkozó szerződésekben rögzíti a biztonságos kódolásra vonatkozó biztonsági követelményeket, melynek megvalósulását a fejlesztési életciklus során, a kapcsolódó döntési pontokon ellenőriz.

### XVII.5. Külső elektronikus információs rendszerek szolgáltatásai

178) A szerződéskötés előtt a beszerzéssel érintett szervezeti egység kijelölt munkatársa az IBF szükség szerinti támogatásával tisztázza, és amennyiben szükséges rögzíti az *Adminisztratív védelmi eljárásrend* szerinti követelményeket.

#### XVII.5.1. Felhőszolgáltatások használatára vonatkozó információbiztonság

179) A felhőszolgáltatások használatára vonatkozó információbiztonsági szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XVII.6. Folyamatos ellenőrzés

180) A DKÜ Zrt.-nek folyamatba épített ellenőrzést vagy ellenőrzési tervet kell végrehajtania. Az ellenőrzési terv végrehajtásával összefüggő feladatokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

## XVIII. Rendszer- és kommunikációvédelem

181) A rendszer- és kommunikációvédelem szabályait a *Rendszer- és kommunikációvédelmi eljárásrend* tartalmazza.

## XIX. Rendszer- és információsértetlenség

182) A rendszer- és információsértetlenségre vonatkozó rendelkezéseket abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert a DKÜ Zrt. üzemelteti. Üzemeltetési szolgáltatási szerződés esetén a rendszer- és információsértetlenségre vonatkozó követelményeket szerződéses kötelemként kell érvényesíteni, és azokat a szolgáltatónak kell biztosítania.

183) A hibajavítással kapcsolatos szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XIX.1. Kártékony kódok elleni védelem

184) A kártékony kódok elleni védelemre vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

#### XIX.1.1. Webszűrés

185) A webszűrésre vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

### XIX.2. Az elektronikus információs rendszer felügyelete

186) A DKÜ Zrt.-nél az elektronikus információs rendszerek felügyeletét az INI látja el, feladatait a *Logikai védelmi eljárásrendben* leírtak határozza meg.

### XIX.3. Biztonsági riasztások és tájékoztatások

187) A biztonsági riasztások és tájékoztatások az IBF feladatainak körébe tartozik, amely a *Logikai védelmi eljárásrendben* van meghatározva.

### XIX.4. A kimeneti információ kezelése és megőrzése

188) A kimeneti információ kezelésére és megőrzésére vonatkozó szabályokat a *Logikai védelmi eljárásrend* tartalmazza.

## XX. Ellátási lánc kockázatkezelése

189) Az ellátási lánc kockázatkezelésére vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XX.1. Beszerzési stratégiák, eszközök és módszerek

190) A beszerzésre vonatkozó szabályokat a *Beszerzési szabályzat*, valamint az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XX.2. Beszállítók értékelése és felülvizsgálata

191) A beszállítók értékelésére vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

### XX.3. Rendszerek, rendszerelemek vizsgálata

192) A rendszerek, rendszerelemek vizsgálatára vonatkozó szabályokat az *Adminisztratív védelmi eljárásrend* tartalmazza.

## XXI. Központi rendszerekre vonatkozó speciális előírások

### XXI.1. Együttműködés a nemzeti kiberbiztonsági hatósággal

193) A DKÜ Zrt. a központi rendszerként való minősülés megállapítása érdekében előzetesen egyeztet a nemzeti kiberbiztonsági hatósággal.

194) A központi rendszer vonatkozásában a DKÜ Zrt. a nemzeti kiberbiztonsági hatóság részére jelenti, hogy mely szervezetek részére szolgáltat.

### XXI.2. Központi rendszer igénybevételére vonatkozó információbiztonsági követelmények

195) Szerződéses követelményként meghatározza vagy a honlapján közzéteszi a központi rendszer igénybevételének feltételeként a felhasználó szervezet által betartandó információbiztonsági követelményeket.

196) A meghatározott feladatok végrehajtását a felhasználó szervezeteknél ellenőrizheti.

197) Az ellenőrzés során feltárt hiányosságok pótlására, hibák javítására határidő megjelölésével felszólítja a felhasználó szervezetet. Eredménytelenség esetén tájékoztatja a nemzeti kiberbiztonsági hatóságot.

### XXI.3. Együttműködés a felhasználó szervezettel

198) A DKÜ Zrt. a központi rendszer vonatkozásában a felhasználó szervezeteket a rendszert érintő előre tervezett eseményekről legalább öt nappal az esemény előtt értesíti.

199) A DKÜ Zrt. soron kívül tájékoztatja a központi rendszert érintő kiberbiztonsági incidensekről a felhasználó szervezeteket.

200) A DKÜ Zrt. a központi rendszert érintő kiberfenyegetés, kiberbiztonsági incidensközeli helyzet vagy kiberbiztonsági incidens esetén tájékoztatja a felhasználó szervezeteket a lehetséges megelőző, a helyreállításhoz szükséges vagy egyéb intézkedésekről.

201) Amennyiben a felhasználó szervezet elektronikus információs rendszere vonatkozásában végzett sérülékenységvizsgálat a központi rendszert érintő hibát, hiányosságot tár fel, a DKÜ Zrt. intézkedik azok kijavítása érdekében.

202) Jogszabály alapján kötelezően igénybe vett központi rendszer esetén a DKÜ Zrt. és a felhasználó szervezet közötti feladat- és felelősségmegosztást az adott központi rendszerre vonatkozó jogszabály rögzíti. Ennek hiányában, valamint önkéntesen igénybe vett központi rendszer esetében a DKÜ Zrt. és a felhasználó szervezet szolgáltatási szerződést köt, melyben rögzítik a feladat- és felelősségmegosztást.

### XXI.4. Központi rendszert érintő kiberbiztonsági incidensek kezelése

203) A DKÜ Zrt. az ismert fenyegetések elleni védelmi intézkedéseket, műszaki, technikai megoldásokat alkalmaz.

204) A DKÜ Zrt. bejelenti a CSIRT-nek a központi rendszert érintő kiberfenyegetéseket, kiberbiztonsági incidensközeli helyzeteket.

205) A központi rendszert érintő kiberfenyegetések, kiberbiztonsági incidensközeli helyzetek, kiberbiztonsági incidensek megelőzése, elhárítása, kezelése, illetve a következmények csökkentése érdekében megteszi a CSIRT által előírt intézkedéseket.

206) Az incidenskezelés során műszaki, technikai adatokat szolgáltat az incidensben érintettek és az incidensért felelős beazonosítása érdekében.

207) A vizsgálat lefolytatásához szükséges adatok, dokumentumok, eszközök és egyéb információk, valamint az ezeket tartalmazó hiteles bitazonos másolatokat a CSIRT rendelkezésére bocsátja.

208) A DKÜ Zrt. megosztja a CSIRT-tel az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságokat.

209) Tájékoztatja a CSIRT-et az elhárítás érdekében tett intézkedésekről, illetve az incidens vizsgálata során, az infrastruktúrával kapcsolatos beállításokról.

210) A DKÜ Zrt. hozzáférést biztosít a CSIRT szakemberei számára a kiberbiztonsági incidensben érintett infrastruktúrához.

211) A CSIRT kérésére a DKÜ Zrt. – szükség szerint – tiltásokat vezet be, felhasználói, előfizetői hozzáféréseket korlátoz, felfüggeszt vagy megszüntet.

212) A CSIRT kérésére, előzetes egyeztetést követően korai figyelmeztető- vagy csapdarendszereket, szenzorokat telepít, amennyiben az kockázatelemzéssel alátámasztott és a telepítés nem veszélyezteti a DKÜ Zrt. működését.

## XXI.5. Együttműködés kiberbiztonsági válsághelyzetekben

213) A kiberbiztonsági válsághelyzetekre történő felkészülés, valamint a kiberbiztonsági válsághelyzetek kezelése érdekében együttműködik a nemzeti eseménykezelő központtal, a CSIRT-tel és az Operatív Törzzsel