DKÜ

A Digitális Kormányzati Ügynökség Zrt.

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Hatályos: 2024. február 7. napjától

DKÜ

Informatikai biztonsági szabályzat

(IBSZ)

Verziószám: v6.0

Tartalomjegyzék

I. Általános rendelkezések

1) Az Informatikai biztonsági szabályzat (a továbbiakban: IBSZ vagy Szabályzat) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 11. § (1) bekezdés f) pontja alapján készült, megfelelve az MSZ ISO/IEC 27001:2014 szabvány követelményeinek.

I.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.

I.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) Az Ibtv. illetve végrehajtási rendelete, 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 rendelet (a továbbiakban: 41/2015 BM rendelet) alapján a DKÜ Zrt. az elektronikus információs rendszereit biztonsági osztályba sorolja, valamint meghatározza a DKÜ Zrt., mint szervezet biztonsági szint szerinti besorolását.

I.3. Az IBSZ kezelése

I.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.

I.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.

I.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) **2013. évi L. törvény** az állami és önkormányzati szervek elektronikus információbiztonságáról;

b) **41/2015. (VII. 15.) BM rendelet** 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;

c) **MSZ ISO/IEC 27001:2014 Informatika**. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények szabvány (a továbbiakban: **IBIR szabvány**).

I.3.4. Az IBSZ hatálya

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

I.3.5. Értelmező rendelkezések, alapfogalmak, rövidítések

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

Fogalom, rövidítés (betűrendben)	Értelmezés
EIR:	DKÜ Zrt.-nél üzemeltetett, vagy a DKÜ Zrt. felügyelete alá tartozó elektronikus információs rendszerek.
Infokommunikációs elem:	berendezés, eszköz, rendszer, hálózat, beleértve mindezek hardver és szoftver elemeit, valamint az infokommunikációs infrastruktúrához kapcsolódó fejlesztési (tervezési, projekt, használatba vételi stb.) és üzemeltetési (felhasználói, biztonsági, selejtezési stb.) és dokumentációt (leírást, utasítást, szabályzatot, feljegyzést stb.) is.
Infokommunikációs infrastruktúra:	a DKÜ Zrt. tulajdonában lévő és/vagy általa kezelt, tárolt vagy EIR-jében, rendszerében használt infokommunikációs infrastrukturális elemek összessége.
Infokommunikációs folyamat:	az infokommunikációs infrastruktúra által megvalósított informatikai vagy kommunikációs tevékenységek összessége.
Információbiztonsági szabályozások:	IBSZ, az IBSZ-hez kapcsolódó eljárásrendek, folyamatleírások, *Jogosultságkezelési szabályzat*.
Szakterületi vezető:	a DKÜ Zrt. Szervezeti és működési szabályzatában szakterületként meghatározott szervezeti egység

Fogalom, rövidítés (betűrendben)	Értelmezés
	vezetője: vezérigazgató, vezérigazgató-helyettes, igazgató vagy irodavezető.
Szervezeti egység vezető:	a DKÜ Zrt. Szervezeti és működési szabályzatában megjelenített szervezeti egység vezetője: csoportvezető, irodavezető, kabinetvezető, igazgató.

I.4. A védelem tárgya, eszközei és működése

I.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 következők:

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-eit 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.

I.4.2. Az informatikai biztonság szervezete

I.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 az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek;

i) ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az Ibtv.-ben foglaltak 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.

I.4.2.2. Szakterületi vezető

24) Felelős azért, hogy a vezetése alatt álló szakterület, szervezeti egységek betartsa 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.

I.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.

I.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.

I.4.2.5. Információbiztonsági felelős (IBF)

28) Az IBF feladata és hatásköre:

a) koordinálja az IBSZ-ben foglaltak szakszerű végrehajtását;
b) folyamatosan figyeli a kormányzati eseménykezelő központ 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 kormányzati eseménykezelő központtal és 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. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

29) A fejezetben meghatározott védelmi intézkedések, eszközök és módszerek a 41/2015.(VII. 15.) BM rendelet, valamint a DKÜ Zrt. biztonsági szintje által az alábbiak szerint kerülnek meghatározásra.

II.1. Szervezeti szintű alapfeladatok

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

II.1.1. A DKÜ Zrt. informatikai biztonsági szintje

31) A DKÜ Zrt. és szervezeti egységeinek informatikai biztonsági szintjét a 41/2015. BM rendelet alapján az *Adminisztratív védelmi eljárásrend* tartalmazza.

II.1.2. Cselekvési és intézkedési terv

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

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

II.1.3. 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.1.4. Az elektronikus információbiztonsággal és annak jogosultságaival kapcsolatos engedélyezési eljárás

35) 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.

36) Az információbiztonsággal összefüggő felelősségi köröket az IBSZ I.4.2 fejezete határozza meg.

II.1.5. Kapcsolattartás

37) 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.2. Kockázatelemzés

II.2.1. Biztonsági besorolások

38) A DKÜ Zrt. minden elektronikus információs rendszerét az adatok bizalmassága, hitelessége, sértetlensége, illetve elvesztésével arányos kárérték szintektől függően az Ibtv., valamint a 41/2015. BM rendelet rendelkezéseinek megfelelően besorolja.

39) A DKÜ Zrt. biztonsági szintbe sorolását, valamint az elektronikus információs rendszereinek biztonsági osztályokba sorolását az *Adminisztratív védelmi eljárásrend* tartalmazza.

II.2.2. Kockázatelemzés

40) 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.

II.2.3. Információosztályozás

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

II.3. Rendszer és szolgáltatás beszerzés

II.3.1. Erőforrás igény felmérés

42) 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.

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

II.3.2. Beszerzések

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

II.3.3. Az elektronikus információs rendszerre vonatkozó dokumentáció

45) 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.

II.3.4. Külső elektronikus információs rendszerek szolgáltatásai

46) A DKÜ Zrt. figyelemmel kíséri és értékeli a szolgáltatások szerződés szerinti teljesítését és szükség esetén beavatkozik, észrevételeit jelzi a vállalkozók felé.

47) 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.

II.3.5. Folyamatos ellenőrzés

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

II.4. Üzletmenet folytonosság tervezése

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

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

II.4.1. Üzletmenet folytonossági terv informatikai erőforrás kiesésekre

51) 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.

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

II.4.2. Az elektronikus információs rendszer mentései

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

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

55) 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.

56) Az IBF feladata ellenőrizni, hogy a kialakításra kerülő mentési rend alapján a mentett információk bizalmassága, sértetlensége és rendelkezésre állása mind az elsődleges, mind a másodlagos tárolási helyszínen biztosított.

57) Meghatározott gyakorisággal tesztelni kell a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének a garantálása érdekében.

58) A DKÜ Zrt. által meghatározott, az elektronikus információs rendszer kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak biztonsági másolatait egy elkülönített berendezésen vagy egy minősítéssel rendelkező tűzbiztos tárolóban kell tárolni.

59) Az elektronikus információs rendszer biztonsági másolat információit az előzőekben meghatározottak szerinti biztonsági tárolási helyszínen kell tárolni.

II.4.3. Az elektronikus információs rendszer helyreállítása és újraindítása

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

61) Az egyes informatikai helyreállítási tervek határozzák meg az eljárásokat, folyamatokat összeomlást, kompromitálódást vagy hibát követően az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításához és újraindításához.

62) A DR tervekben meghatározandó az elektronikus információs rendszerelemek előre definiált helyreállítási ideje, ami alatt helyre lehessen állítani egy olyan konfigurációellenőrzött és sértetlenség védett információból, ami az elem ismert működési állapotát reprezentálja.

63) Az informatikai helyreállítási tervben meg kell határozni a tranzakció alapú elektronikus információs rendszerek esetén a tranzakció helyreállításának módját.

II.5. Biztonsági incidensek, események kezelése

II.5.1. A biztonsági incidensek, események figyelése és jelentése

64) A biztonsági incidensek, események figyelése és jelentésére vonatkozó elvárásokat az *Információbiztonsági incidensek kezelése folyamatleírás* tartalmazza.

II.5.2. A biztonsági incidensek, események kezelése, kivizsgálása

65) Az Incidenskezelő csoport az értesítést követően átveszi az események irányítását, koordinálását, dokumentációját, a bizonyítékok tárolását, rendszerezését, illetve felelős a további események jegyzőkönyvbe foglalásáért.

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

II.5.3. Az incidenskezeléshez kapcsolódó szerepkörök feladatai, felelősségei

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

II.5.4. Képzés a biztonsági események kezelésére

68) Biztonsági eseménykezelési képzést kell biztosítani az elektronikus információs rendszer felhasználóinak a számukra kijelölt szerepkörökkel és felelősségekkel összhangban.

II.6. Emberi tényezőket figyelembe vevő – személy – biztonság

69) 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.

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

II.6.1. Munkakörök, feladatok biztonsági szempontú besorolása

71) 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.

II.6.2. A személyek ellenőrzése

72) 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.

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

II.6.3. Eljárás a jogviszony megszűnésekor, megváltozásakor

74) A személyi állománnyal kapcsolatos változásokat (munkaviszony létesítése, vagy megszüntetése, munkakörök megállapítása és módosítása) a HR területnek kell írásban jeleznie a szervezeti egység vezetője, valamint az IBF felé.

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

II.6.4. Az áthelyezések, átirányítások és kirendelések kezelése

76) 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.

II.6.5. Fegyelmi intézkedések

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

78) 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.

II.6.6. Viselkedési szabályok az internet használata során

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

II.7. Tudatosság és képzés

II.7.1 Képzési eljárásrend

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

II.7.2. Biztonságtudatosság képzés

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

II.7.3. Szerepkör, vagy feladat alapú biztonsági képzés

82) 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.

II.7.4. A biztonsági képzésre vonatkozó dokumentációk

83) Az érintett személyek számára a képzéseket a vezérigazgató rendeli el.

84) A képzés megtörténtét elektronikus vagy papír alapú formában dokumentálni szükséges, amelyért a HR terület a felelős.

85) A képzéseken való részvétel ellenőrzése a szervezeti egység vezető feladata.

III. FIZIKAI VÉDELMI INTÉZKEDÉSEK

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

III.1. Biztonsági területek

III.1.1. Biztonsági zónák meghatározása

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

88) 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.

III.1.2. Zónák védelme

89) 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).

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

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

91) Szervertermek és mentések üzemelésére szolgáló termek védelme a felhasználói helyiségekre vonatkozó védelmi szabályokon túl:

a) A belépés-kilépés szabályozására elektronikus kártyás beléptetési rendszert kell alkalmazni.
b) Áramszünet esetén az ajtónak kulccsal nyithatónak kell lenni.
c) A belépés-kilépés szabályainak betartását incidens gyanúja esetén a biztonsági kamera felvételeinek megtekintésével kell ellenőrizni és minden, a helyiségben történt tevékenységet egyértelmű és visszakereshető módon naplózni kell.
d) A helyiséget füst- és tűzérzékelővel kell ellátni, amely egy állandóan felügyelt helyiségben riaszt.
e) A helyiségekbe csak az annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat, tehát a helyiségen nem mehet át víz, gáz, csatorna, és egyéb közművezeték. Felette és a határoló falfelületeken vizesblokkot tartalmazó helyiségrész nem lehet, nyomó és ejtőcsövek és gázvezetékek nem haladhatnak át.

f) Csak az üzemeltetésre kijelölt személy, az ellenőrzést végzők, valamint az Informatikai és fejlesztési igazgatóság (INI) rendszerüzemeltetési csoportvezetője által engedélyezett személy léphet be.
g) A helyiségben kizárólag munkavégzés céljából szabad tartózkodni.
h) A helyiség takarítása és a helyben végzett karbantartás csak közvetlen ellenőrzés mellett történhet.
i) A helyiségeket raktárként használni tilos.
j) A helyiségek takarítása és karbantartása előtt gondoskodni kell az ott dolgozóknak arról, hogy a képernyőkön és a nyomtatókban illetéktelenekre nem tartozó adatok ne legyenek.
k) A helyiségeket klímaberendezéssel kell ellátni. A klíma berendezést abban az esetben kell működtetni, ha a helyiségben 22 °C-os hőmérséklet csak a berendezés használatával biztosítható.
l) Szünetmentes energiaellátás biztosítása szükséges.

III.1.3. Fizikai belépési engedélyek

92) 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.

III.1.4. A fizikai belépés ellenőrzése

93) 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.

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

95) Minden munkatárs köteles megóvni a rá bízott kulcsokat, hozzáférési kódokat, és az egyéb fizikai hozzáférést biztosító vagy ellenőrző eszközöket.

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

97) A hozzáférési kódok és kulcsok haladéktalanul megváltoztatandók a kulcs elvesztése vagy a hozzáférési kód kompromittálódása esetén, vagy ha az adott személy elveszti a belépési jogosultságát.

98) A szervezet minden tagjának kötelessége az észlelt rendellenességek jelentése az IBF, a biztonsági vezető vagy az INI igazgató részére.

III.1.5. A fizikai hozzáférések felügyelete

99) 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.

III.1.6. A látogatók ellenőrzése

100) Egy évig meg kell őrizni a Társaság székhelyén vagy telephelyén 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.

III.1.7. Vészvilágítás

101) A DKÜ Zrt. automatikus vészvilágítási rendszert alkalmaz és tart karban, amely áramszünet esetén aktiválódik, és amely biztosítja a vészkijáratokat és a menekülési útvonalakat.

III.1.8. Tűzvédelem

102) 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.

III.1.9. Hőmérséklet és páratartalom ellenőrzés

103) Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben az erőforrások biztonságos működéséhez szükséges szinten kell tartani a hőmérsékletet és páratartalmat, valamint figyelni szükséges a hőmérséklet és páratartalom szintjét.

III.1.10. Vezetéken szállított anyag okozta kár elleni védelem

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

III.1.11. Be- és kiszállítás

105) A létesítménybe bevitt, onnan kivitt informatikai rendszerelemeket csak engedély birtokában lehet mozgatni. Ezen eszközök mozgatásról nyilvántartást kell vezetni. Az engedélyezési és nyilvántartási kötelezettség nem vonatkozik a személyes használatra átadott hordozható számítógépekre és mobil eszközökre.

106) A be- és kiszállítás részletes szabályait a *Fikai védelmi eljárásrend* tartalmazza.

III.1.12. Karbantartók

107) 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.).

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

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

110) A karbantartókra vonatkozó részletes szabályokat a *Fizikai biztonsági eljárásrend* tartalmazza.

III.1.13. Harmadik fél adatközpontjában elhelyezett rendszerek

111) 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 IBF útján hitelt érdemlően meggyőződik.

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

IV. LOGIKAI VÉDELMI INTÉZKEDÉSEK

IV.1. Általános használati elvek

113) A logikai védelmi intézkedések úgy lettek összeállítva, hogy a biztonsági elvek a 41/2015. (VIII. 15.) BM rendelet alapján a biztonsági osztályba sorolt információs rendszerek, valamint az MSZ ISO/IEC 27001:2014 szabvány követelményeit kielégítse, továbbá az MSZ ISO/IEC 27001:2023 szabvány változásai folyamatosan beépítésre kerüljenek.

114) Jelen védelmi intézkedések részletes szabályait a *Logikai védelmi eljárásrend* tartalmazza.

IV.1.1. Az elektronikus információs rendszer kapcsolódásai

115) A DKÜ Zrt. csak a felügyelete alatt álló elektronikus információs rendszer felett gyakorol kontrollt, az EIR-ek felügyelet nélküli összekapcsolása más szervezetek informatikai rendszerével nem engedélyezett. A DKÜ Zrt. munkavállalóinak felügyelete alatt álló, ideiglenes kapcsolatok, így az adatok manuális letöltése más szervezetek informatikai rendszeréből, nem tartoznak e tiltás hatálya alá.

116) Minden olyan esetben, amikor a DKÜ Zrt. valamely EIR-je hozzákapcsolásra kerül valamilyen külső rendszerhez, akkor a felelős szervezeti egység vezető és az INI igazgató előzetes engedélye szükséges, és az IBF értesítendő. Az egyes kapcsolatokat, az interfészek paramétereit, a biztonsági követelményeket és a kapcsolaton keresztül átvitt elektronikus információk típusát dokumentálni kell.

IV.1.2. Személyi biztonság

117) A személyi biztonsággal kapcsolatos elvárások kiterjednek a DKÜ Zrt. teljes személyi állományára, valamint minden olyan természetes személyre, aki a DKÜ Zrt. elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az EIR-rel tényleges, vagy feltételezhetően kapcsolatba kerülő személy nem a DKÜ Zrt. munkavállalója, a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás megkötése során a személyi biztonsággal kapcsolatos elvárásokat, mint kötelezettséget érvényesíteni kell. A szervezeten belüli személyi biztonsággal összefüggő felhasználói jogokat a *Logikai védelmi eljárásrend* tartalmazza.

IV.2. Tervezés

IV.2.1. Biztonságtervezési eljárásrend

118) A DKÜ Zrt. informatikai rendszerek fejlesztése jelen IBSZ-ben meghatározottak szerint történik. A DKÜ Zrt. új informatikai rendszerek fejlesztésekor vagy meglévő rendszerek bővítésekor a biztonsági követelményeket a fejlesztés minden szakaszában vizsgálja és értékeli az érintett EIR biztonsági osztályba sorolásának tükrében. Csak a kockázatelemzés alapján meghatározott követelménynek megfelelő informatikai rendszerfejlesztés vagy rendszerbővítés hajtható végre.

119) A biztonságtervezéssel kapcsolatos követelmények részletes leírását a *Biztonságelemzési eljárásrend* tartalmazza.

IV.2.2. Rendszerbiztonsági terv

120) A DKÜ Zrt. az elektronikus információs rendszerek fejlesztésekor vagy meglévő rendszerek bővítésekor gondoskodik arról, hogy a vállalkozó, illetve üzemeltető által készített rendszerbiztonsági terv rendelkezésre álljon.

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

IV.3. Rendszer és szolgáltatás beszerzés

122) A DKÜ Zrt. elektronikus információs rendszereinek informatikai biztonsági helyzetét azok teljes életútján az IBF 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.

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

IV.4. Biztonsági elemzés, teljesítmény mérése

124) 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.

IV.5. Tesztelés, képzés és felügyelet

IV.5.1 Sérülékenységi teszt

125) 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.

IV.5.2 Frissítési képesség

126) A DKÜ Zrt. olyan sérülékenységi teszteszközt alkalmaztat, melynek sérülékenység feltáró képessége könnyen bővíthető az ismertté váló sérülékenységekkel.

127) A DKÜ Zrt. az elektronikus információs rendszerre vizsgált sérülékenység körét aktualizáltatja az új tesztet megelőzően, vagy a sérülékenység feltárását követően azonnal.

IV.5.3 Privilegizált hozzáférés

128) A DKÜ Zrt. a sérülékenységi teszt végrehajtásához a sérülékenységi vizsgálatot végző személynek a vizsgálat idejére hozzáférést biztosít a DKÜ Zrt. elektronikus információs rendszeréhez.

IV.5.4 Felfedhető információk

129) A sérülékenységi vizsgálat után az IBF-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.

IV.6. Konfigurációkezelés

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

IV.6.1. Biztonsági hatásvizsgálat

131) Rendszerbevezetés során megvizsgálandó az elektronikus információs rendszerben tervezett változtatásoknak az információbiztonságra való hatása. Ezt a következő szinteken kell megvalósítani:

a) logikai tervezés során, hogy a megtervezett rendszerműködés nem rejt-e biztonsági kockázatot;
b) fizikai tervezés során, hogy a megtervezett rendszer komponensek nem rejtenek-e biztonsági kockázatot;
c) élesbe állítás előtt, hogy az elkészült elektronikus információs rendszer nem rejt-e biztonsági kockázatot.

132) A változtatásokat éles rendszerben történő megvalósításuk előtt egy elkülönített tesztkörnyezetben kell megvizsgálni, hibákat, sebezhetőségeket, kompatibilitási problémákat és szándékos károkozásra utaló jeleket keresve.

IV.6.2. Konfigurációs beállítások

133) Az elkészült elektronikus információs rendszer tervezésekor, módosításaikor meghatározandó a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott – a „szükséges minimum” elv alapján – az elektronikus információs rendszerben használt információtechnológiai termékekre a kötelező konfigurációs beállítás. Ezen konfigurációs elem beállítási feltételeket dokumentálni szükséges az elkészült elektronikus információs rendszer dokumentumaiban.

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

IV.6.3. Legszűkebb funkcionalitás

135) 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.

136) A határvédelmi eszközökre vonatkozóan szúrópróbaszerűen ellenőrizendő az eszközök paramétereinek beállítása, hogy megfelelnek-e a meghatározott elvárásoknak.

137) A felhasználók a munkavégzésük során felmerült igények alapján szoftverigényt nyújthatnak be az INI felé. Az igényelt és indokoltan szükséges szoftverek beszerzéséről az INI és a szoftverigényt benyújtó felhasználó szervezeti egység vezetője dönt. 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.

138) A DKÜ Zrt. tulajdonába kerülő szoftvereket és alkalmazásokat fel kell venni a DKÜ Zrt. eszköznyilvántartó rendszerébe, és egyedi azonosítóval kell ellátni. Amíg ez nem történt meg, az alkalmazást nem lehet átadni felhasználás céljára. Az alkalmazások átadását, átvételét és bármilyen változtatását dokumentálni kell.

139) A DKÜ Zrt. tulajdonában lévő informatikai eszközökre szoftvereket és alkalmazásokat csak az INI igazgatója által megbízott, vagy munkakörükben erre felhatalmazott dolgozók telepíthetnek.

140) Személyi számítógépeken, laptopokon csak a DKÜ Zrt. által engedélyezett, a DKÜ Zrt. számára licenc joggal rendelkező alkalmazások, szoftverek telepíthetők, futtathatók.

141) Biztosítani kell, hogy a DKÜ Zrt. állománya csak megfelelően kibocsátott és engedélyezett szoftververziókat használjon. Kizárólag csak annyi szoftver telepíthető a felhasználókhoz, amennyi használata szükséges az adott felhasználó zavartalan munkavégzésének megvalósításához.

142) A DKÜ Zrt. az informatikai eszközök raktározására helyiséget biztosít. A raktárhelyiségben jól elkülönített módon kell tárolni a selejtezésre váró és a még használható anyagokat.

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

144) A végleges eltávolítás, vagy a javításra kiadás során gondoskodni kell az eszközök adattartalmának megsemmisítéséről, az adott elem pótlásáról. A végleges kikerülést dokumentálni kell.

145) A pillanatnyilag nem megfelelő, de még javítható eszközök javítását kizárólag csak megfelelő szakértelemmel és gyakorlati tapasztalatokkal rendelkező, szerződésben rögzített szolgáltató cégek végezhetik.

146) A leltárnyilvántartást évente ellenőrizni kell annak érdekében, hogy az pontosan tükrözze az elektronikus információs rendszer aktuális állapotát, valamint tartalmazza az elektronikus információs rendszer hatókörébe eső valamennyi hardver- és szoftverelemet, továbbá legyen kellően részletes a nyomkövetéshez és a jelentéskészítéshez.

147) A leltárt frissíteni kell az egyes rendszerelemek telepítésének, eltávolításának, frissítésének időpontjában.

IV.6.4. A szoftverhasználat korlátozásai

148) A DKÜ Zrt. számítástechnikai eszközein kizárólag olyan szoftvereket és kapcsolódó dokumentációt szabad használni, amelyek megfelelnek a rájuk vonatkozó szerződésbeli elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

149) A mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk használatát minimum évente ellenőrizni kell.

150) A számítástechnikai eszközökre telepített szoftvereket az INI rendszeresen ellenőrzi. Az ellenőrzést úgy kell ütemezni, hogy minden eszköz ellenőrzése minimum évente egyszer megtörténjen.

IV.7. Karbantartás

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

IV.8. Adathordozók védelme

IV.8.1. Hozzáférés az adathordozókhoz

152) 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.

IV.8.2. Adathordozók törlése

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

IV.8.3. Adathordozó kriptográfiai védelme

154) A DKÜ Zrt. kriptográfiai mechanizmusokat alkalmaz a digitális adathordozókon tárolt információk bizalmasságának és sértetlenségének a védelmére az ellenőrzött területeken kívüli szállítás, elhelyezés folyamán.

IV.8.4. Adathordozók használata

155) Az elektronikus információs rendszerekhez kizárólag a DKÜ Zrt. tulajdonában lévő és/vagy általa biztosított digitális adathordozók használata engedélyezett. A digitális adathordozók vírusellenőrzést követően vehetőek használatba. Idegen vagy engedély nélküli adathordozó használata tilos.

IV.9. Azonosítás és hitelesítés

IV.9.1. Azonosítás és hitelesítés

156) Az azonosítás és hitelesítés az elektronikus információs rendszerekre vonatkozóan az adott rendszer elvárásaiként kell megfogalmazni.

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

IV.9.2. A felhasználói hozzáférés kezelése

158) 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.

IV.9.3. Azonosító kezelés

159) Az elektronikus információs rendszerekben a felhasználói azonosító egységes képzési szabálya:

a) a felhasználói azonosítók egyediségét minden esetben biztosítani kell;
b) az érintett EIR-ben az alkalmazásgazda a jogosultság kérés alapján meghatározott szerepek szerint hozzáférési jogosultsággal ruházza fel a felhasználót;
c) a felhasználói azonosítók ismételt felhasználása tiltott.

IV.9.4. Hálózati hozzáférés privilegizált fiókokhoz

160) Hálózati hozzáférés esetén a privilegizált (különleges jogosultságokhoz kötött) felhasználóknál többtényezős azonosítást kell alkalmazni.

IV.9.5. A hitelesítésre szolgáló eszközök kezelése

161) 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.

IV.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

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

IV.9.7. Hitelesítés kriptográfiai modul esetén

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

IV.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

164) 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.

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

IV.9.9. Hitelesítés szolgáltatók tanúsítványának elfogadása

166) 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.

IV.10. Hozzáférés ellenőrzése

IV.10.1. Hozzáférés ellenőrzési eljárásrend

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

IV.10.2. Felhasználói fiókok kezelése

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

IV.10.3. Hozzáférés ellenőrzés érvényesítése

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

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

171) 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.

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

IV.10.4. A felhasználók hozzáféréssel kapcsolatos kötelességei

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

IV.10.5. Sikertelen bejelentkezési kísérletek

174) A sikertelen bejelentkezési kísérleteket naplózni kell.

175) Az esetszám korlátot meghaladó egy napon belüli egymást követő sikertelen bejelentkezési kísérletet követően automatikusan zárolni kell a felhasználói fiókot, vagy csomópontot a rendszerbiztonsági tervben előírtaknak megfelelően.

IV.10.6. A rendszerhasználat jelzése

176) A 3. 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.

177) 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.

IV.10.7. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

178) A DKÜ Zrt.-nél az EIR-ekben nem engedélyezett olyan felhasználói tevékenység, amit azonosítás és hitelesítés nélkül is végre lehet hajtani.

IV.10.8. Vezeték nélküli hozzáférés

179) A vezeték nélküli hálózatot több szegmensre kell bontani. Külön hálózati szegmenset kell biztosítani a vendégek számára, amelyről a belső hálózat nem érhető el.

180) A vezeték nélküli hálózat hozzáférés jelszavát minden dolgozó köteles titokban tartani.

IV.10.9. Mobil eszközök hozzáférés ellenőrzése

181) A felhasználóknak átadott notebookokra vírusvédelmi programot kell telepíteni, amelynek frissítését az INI központilag biztosítja.

182) A DKÜ Zrt. hálózatához – a vendéghálózat kivételével – a személyi használatra kiadott hordozható számítógépek és mobiltelefon kivételével egyéb mobil eszközzel tilos a hozzáférés.

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

184) A DKÜ Zrt. a hordozható laptop/notebook eszközök esetében megfelelő kriptográfiai védelemről Bitlocker segítségével gondoskodik. Az INI központilag AD-ban beállítva gondoskodik a Bitlocker bekapcsolásáról és menedzseléséről.

185) A mobil eszközökkel a DKÜ Zrt. hálózatában csak egy kifejezetten erre a célra létrehozott, szeparált alhálózatára lehet csatlakozni.

IV.10.10. Nyilvánosan elérhető tartalom

186) A DKÜ Zrt. honlapjának technikai jellegű módosításával és üzemeltetésével összefüggő feladatokat az INI látja el. A honlapon tartalom elhelyezését a honlap tartalommal való feltöltéséért felelős, *Szervezeti és működési szabályzatban* kijelölt szakterület részére továbbítva, bármely szakterületi vezető kezdeményezheti.

187) A tartalomra vonatkozó végső jóváhagyó a vezérigazgató.

188) A jóváhagyott tartalmat a Jogi és koordinációs iroda kijelölt munkatársa helyezi ki a honlapra.

IV.11. Rendszer- és információsértetlenség

189) 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.

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

IV.11.1. Kártékony kódok elleni védelem

191) Vírusgyanú vagy vírusfertőzés esetén azonnal értesíteni kell az IBF-et és az INI igazgatót és végre kell hajtani az utasításait.

192) A rendszergazdai jogosultsággal felruházott felhasználók a már feltelepített vírusvédelmi alkalmazás mellé nem telepíthetnek fel másik víruskereső programot.

193) A DKÜ Zrt. információtechnológiai eszközeivel a világhálón csak megbízható helyek látogatása engedélyezett és a szükséges letöltések csak innen történhetnek.

194) A vírusvédelmi rendszert úgy kell konfigurálni, hogy az kiterjedjen minden elemre, amely a *Logikai védelmi eljárásrendben* lefektetésre került.

195) Biztosítani kell a vírusvédelmi rendszer bevezetésének és üzemeltetésének teljes körű dokumentációját.

196) Gondoskodni kell arról, hogy a felhasználók ne tudják kikapcsolni a vírusvédelmi alkalmazást. A vírusvédelmi alkalmazás automatikus frissítéséről az INI gondoskodik.

IV.11.2. Az elektronikus információs rendszer felügyelete

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

IV.11.3. Biztonsági riasztások és tájékoztatások

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

IV.11.5. A kimeneti információ kezelése és megőrzése

199) A DKÜ Zrt. az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

IV.12. Naplózás és elszámoltathatóság

IV.12.1. Naplózási eljárásrend

200) 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.

IV.13. Rendszer- és kommunikációvédelem

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