KK/08/00057-3/2024

SZOLNOKI
TANKERÜLETI
KÖZPONT

Iktatószám:
TK/103/00029-6/2024

A Szolnoki Tankerületi Központ 6/2024. (IV.24.) számú Informatikai Biztonsági Szabályzata

Készítette:

Szolnok, 2024. április 24.

.....
Antal Attila
információbiztonsági felelős

Kiadja:

Szolnok, 2024. április 24.

.....
Rusvai Károly
tankerületi igazgató

Szolnoki Tankerületi Központ 01

A Szolnoki Tankerületi Központ jelen Szabályzatát az állami köznevelési közfeladat ellátásában fenntartóként részt vevő szervekről, valamint a Klebelsberg Központról szóló 134/2016. (VI. 10.) Korm. rendelet 5. § (1) bekezdés a) pontjában biztosított középirányítói hatáskörömben eljárva, a Klebelsberg Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás 1. mellékletének 40. §-a alapján jóváhagyom:

Budapest, 2024. május 9.

Klebelsberg Központ 01 Elnök

.....
Hajnal Gabriella
elnök
Klebelsberg Központ

Tartalomjegyzék

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben foglaltakra figyelemmel, valamint a Szolnoki Tankerületi Központ esetében az informatikai rendszerek biztonságos felhasználásának rendjét – a Tankerületi Központ Szervezeti és Működési Szabályzatának 5. § (2) bekezdésének f) pontja alapján biztosított jogkörömben eljárva a Tankerületi Központ szervezeti szintű informatikai biztonsági követelményeit az alábbiak szerint szabályozom:

ELSŐ RÉSZ

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat célja

1. § (1) Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja a Szolnoki Tankerületi Központ (a továbbiakban: Tankerületi Központ) informatikai biztonsági követelményjegyzékének kialakítása. A követelményjegyzék magában foglalja a Tankerületi Központra vonatkozó informatikai biztonsági feladatok és felelősségi körök meghatározását, és a rendszer által kezelt, feldolgozott, továbbított, valamint tárolt adatok bizalmasságát, sértetlenségét és rendelkezésre állását fenyegető veszélyek felderítésére, megelőzésére, elhárítására vonatkozó előírásokat.

(2) További célja a Tankerületi Központ által használt informatikai rendszerek, alkalmazások és szolgáltatások, valamint az általuk kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának szabványos, szabályozott és egységes biztosítása. Az egységesítés érdekében jelen szabályzat keretjelleggel meghatározza mindazokat a normákat és magatartásformákat, amelyek megvalósítják a kockázatokkal arányos, folyamatos és komplex információvédelmet az informatikai rendszer fizikai, adminisztratív és logikai védelmi területén.

(3) Az IBSZ általános célja, hogy a Tankerületi Központ által használt és működtetett informatikai rendszer biztonságát garantáló eljárásokat és előírásokat átlátható és nyomon követhető formában egységes keretbe foglalva rögzítse az informatikai biztonság magasabb fokú kialakításának további szabályozása érdekében.

2. A szabályzat hatálya

2. § (1) A Tankerületi Központ IBSZ-ében meghatározott előírások, feladatok, magatartási szabályok – munkakörre, álláshelyen ellátandó feladatokra való tekintet nélkül – kötelező érvényűek.

(2) Az IBSZ személyi hatálya kiterjed:

a) a Tankerület által foglalkoztatott kormányzati szolgálati viszonyban, munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban állókra (a továbbiakban: foglalkoztatottak),

b) az a) pont alá nem tartozó, a Tankerületi Központtal egyéb jogviszonyban álló személyekre, akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással az IBSZ tárgyi hatálya alá tartozó eszközöket, alkalmazásokat és szolgáltatásokat (a továbbiakban együtt: informatikai rendszert) használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak.

Az a) és b) pontban megnevezett személyek a továbbiakban együtt: felhasználók.

(3) A (2) bekezdés hatálya alá tartozó felhasználókkal kötendő, jogviszony létrehozására irányuló dokumentumban rögzíteni szükséges a jelen szabályzat betartására vonatkozó kötelezettségeket,

emellett biztosítani kell az IBSZ rendelkezéseinek érvényesülését is.

(4) Az IBSZ rendelkezéseit alkalmazni kell a külső helyszínen történő munkavégzéshez használt eszközökre is, amennyiben azok az IBSZ tárgyi hatálya alá tartoznak.

(5) Az IBSZ-t alkalmazni kell a Tankerületi Központ informatikai rendszereire, alkalmazásaira és azok moduljaira, az informatikai rendszerhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközökre és adathordozókra, az informatikai rendszerben kezelt, feldolgozott, tárolt adatokra, valamint az előzőekben felsoroltakkal kapcsolatos informatikai és biztonsági tevékenységekre is.

3. § Az IBSZ tárgyi hatálya kiterjed:

a) a Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: NISZ) által üzemeltetett, a Tankerületi Központ adatait feldolgozó, tároló vagy továbbító információhordozó eszközre, informatikai eszközökre és berendezésekre (ezek különösen: számítógépek, mobil eszközök, laptopok, IP telefonok, táblagépek, „okos” telefonok, nyomtatók, külső adattároló eszközök, aktív hálózati elemek, elektronikus adathordozók) az alkalmazás és felhasználás mértékéig és vonatkozásában,

b) az a) pontban meghatározott eszközökre vonatkozó minden dokumentációra (ezek különösen: fejlesztési, szervezési, programozási, üzemeltetési dokumentumok), függetlenül azok formátumától (papír vagy elektronikus),

c) a felhasználók által bármely okból használt információhordozó eszközökre és berendezésekre, amennyiben azok a Tankerületi Központ informatikai környezetével vagy a NISZ által üzemeltetett – a Tankerületi Központ részére biztosított – informatikai eszközzel kapcsolatba kerülnek,

d) az a) pontban felsorolt informatikai eszközökön használt vagy tárolt alkalmazásokra és adatokra (ezek különösen: rendszerprogramok, alkalmazások, adatbázisok), ideértve az üzemelő rendszerek adatain kívül az oktatási, teszt és egyéb célra használt adatokat is,

e) a Tankerületi Központ által kezelt és a NISZ által üzemeltetett eszközökön tárolt adatok teljes körére, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

3. A szabályzat jogi háttere és a kapcsolódó belső irányítási eszközök

4. § (1) Az IBSZ jogi alapját az alábbi jogszabályok, közjogi szervezetszabályozó eszközök és belső irányítási eszközök képezik:

a) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.),

b) 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,

c) az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet,

d) az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet,

e) az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet,

f) a Tankerületi Központ Szervezeti és Működési Szabályzata,

g) a Tankerületi Központ Egyedi Iratkezelési Szabályzata,

h) a Tankerületi Központ Adatvédelmi és Adatbiztonsági Szabályzata,

(2) Az Ibtv. és kapcsolódó végrehajtási rendeleteinek előírásaira tekintettel jelen IBSZ-t megismerni kizárólag a jelen szabályzat hatálya alá tartozó meghatározott személyek jogosultak.

II. FEJEZET

4. Értelmező rendelkezések

5. § E szabályzat alkalmazásában az IBSZ-ben alkalmazott, az IBSZ értelmezését, továbbá az informatikai biztonság tárgykörét érintő informatikai fogalmak az Ibtv. figyelembevételével:

1. *adat:* az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas,
2. *adatállomány:* egy nyilvántartásban kezelt adatok összessége,
3. *adatátvitel:* elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat,
4. *adatbázis:* azonos minőségű, azonos jellemzőkkel rendelkező, többnyire strukturált adatok összessége, amelyet a tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.
5. *adatfeldolgozás:* az adatkezeléshez kapcsolódó technikai feladatok elvégzése,
6. *adatgazda:* az a vezető, aki egy meghatározott adatcsoport tekintetében az adatok fogadásában, tárolásában, feldolgozásában, vagy továbbításában érintett szervezeti egységet képviseli és az adott adatcsoport felhasználásának kérdéseiben (például felhasználói jogosultságok engedélyezésében vagy megvonásában) elsődleges döntési jogkörrel rendelkezik,
7. *adathordozó:* az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható. Pl. CD, DAT, DVD, floppy, merevlemez, USB-memória, cloud (felhő),
8. *adatkezelés:* az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása,
9. *adminisztratív biztonsági követelmények:* az informatikai rendszer használata, üzemeltetése vagy fejlesztése során az adatok és a munkafolyamatok nyilvántartását, nyomon követhetőségét, továbbá az ezzel kapcsolatos feladatok ellátásának ellenőrzését lehetővé tevő segédletek és eljárásrendek meglétére, alkalmazására vonatkozó elvárások. Pl. naplók, nyilvántartások vezetése, ellenőrzése, ennek rendje,
10. *archiválás:* adatok, adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése,
11. *autentikáció (azonosítás):* informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi,
12. *autorizáció (feljogosítás):* azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap,

13. *belső felhasználó:* a Tankerületi Központ valamennyi foglalkoztatottja.
14. *belső hálózat (intranet):* a Tankerületi Központ saját, védett hálózata, amely belső szolgáltatásokat biztosít, emellett, strukturáltan, kereshető formában teszi elérhetővé a Tankerületi Központ feladataival összefüggő adatbázisokat, a Tankerületi Központ belső szabályzatait és az általa használt nyomtatványokat,
15. *bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról,
16. *biztonság:* egy adott infrastruktúra, infrastruktúra-elem, vagy elemek olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Részei a fizikai, környezeti, személyi, szervezeti, valamint az információbiztonság, az infokommunikációs infrastruktúrákban kezelt elektronikus adatok és információk biztonsága,
17. *biztonsági esemény:* 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,
18. *biztonsági intézkedések:* illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni eszközök használatát szabályozó, valamint az illetékes személyek jogosulatlan tevékenységével szemben fellépő előírások, tervek és útmutatások összessége,
19. *biztonsági kockázat:* az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti,
20. *biztonsági követelmények:* a kockázatelemzés eredményeként megállapított, elfogadhatatlan mértékű veszély mérséklésére, vagy megszüntetésére irányuló szükségletek együttese,
21. *biztonsági megfelelőség:* az informatikai rendszer mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek,
22. *biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége,
23. *biztonsági szint:* a szervezet felkészültsége az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére,
24. *demilitarizált zóna (a továbbiakban: DMZ):* összekapcsolt hálózatok megbízhatatlan külső és megbízható belső részei között elhelyezkedő terület. A DMZ a benne elhelyezkedő hálózati eszközökhöz mind a megbízható belső, mind pedig a megbízhatatlan külső területről szabályozott mértékben engedélyezi a hozzáférést, de megakadályozza, hogy a külső területről bármilyen hozzáférési kísérlet eljusson a belső hálózatra,
25. *elektronikus információs rendszer:* az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttese, továbbá az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön, egymással összefüggő eljárásokkal azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttese,

26. *értékelés:* az infokommunikációs rendszerekkel kapcsolatos biztonsági intézkedések, eljárásrendek, Magyarországon elfogadott technológiai értékelési szabványok, követelményrendszerek és ajánlások, illetve jogszabályok szerinti megfelelőségi vizsgálata,
27. *fejlesztői rendszer:* olyan informatikai rendszer vagy alkalmazás, amelynek felhasználói informatikusok. Célja felhasználói programok vagy alkalmazások kifejlesztésének támogatása,
28. *felhasználók*: a 2. § (2) bekezdésében meghatározott személyek,
29. *fizikai biztonság:* illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni intézkedések összessége, valamint az illetéktelen személyek, vagy illetékes személyek jogosulatlan tevékenységével szemben az adott struktúrák ellenálló képességét növelő tervek és útmutatások összessége,
30. *folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem,
31. *funkcionális rendszer:* a Tankerületi Központ működését támogató informatikai rendszer vagy alkalmazás,
32. *hardver*: az informatikai rendszer vagy számítógép fizikai elemei,
33. *hálózat:* számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé,
34. *helyreállítás:* valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen,
35. *hitelesítés:* a rendszerbe kerülő, ott lévő és onnan kikerülő adatok forrásának (az adat közlőjének), megbízható azonosítása,
36. *hitelesség:* annak biztosítása, hogy a rendszerbe kerülő adatok és információk eredetiek, a megadott forrásból az abban tárolttal azonos, változatlan tartalommal származnak,
37. *hozzáférés:* az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása,
38. *illetéktelen személy:* olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult,
39. *infokommunikáció:* az informatika és a telekommunikáció, mint konvergáló területek együttes neve,
40. *Gazdálkodási, Üzemeltetési és Pályázati Főosztály:* a Tankerületi Központ informatikáért felelős szervezeti egysége,
41. *informatikai alkalmazás:* számítógépen, illetve egyéb informatikai eszközön futó program,
42. *informatikai biztonság:* az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított,
43. *informatikai biztonsági incidens:* az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, amelynek célja a Tankerületi Központ kezelésében lévő adatok, dokumentumok és egyéb információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása,
44. *informatikai biztonsági követelmények:* az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság,

45. *informatikai biztonsági politika:* a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása meghatározott biztonsági feladatok irányítására és támogatására,
46. *informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere,
47. *informatikai infrastruktúra:* a Tankerületi Központhoz kapcsolódó feladatokat ellátó, illetve a Tankerületi Központ működését biztosító hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese, amely jól körülhatárolható, önmagában is működőképes, önálló szolgáltatás nyújtására képes infrastruktúra elemekből áll,
48. *informatikai rendszer:* a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese,
49. *informatikai vészhelyzet:* a Tankerületi Központ információs infrastruktúrájának leállása, szolgáltatások megszakadása, elérhetetlensége, a Tankerületi Központ nemzeti információs vagyonának jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés,
50. *információ:* bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti,
51. *információbiztonság:* az adatok és információk szándékosan, vagy gondatlanul történő jogosulatlan gyűjtése, károsítása, közlése, manipulálása, módosítása, elvesztése, felhasználása, illetve természeti vagy technológiai katasztrófák elleni védelmének koncepciói, technikái, technikai, illetve adminisztratív intézkedései. Az információbiztonság része az informatikai biztonság is, amelynek alapelvei a bizalmasság, sértetlenség, rendelkezésre állás,
52. *információvédelem:* szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében,
53. *jogosultság:* az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához,
54. *kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye,
55. *kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése,
56. *kockázattal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével,
57. *következmény:* valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát,
58. *külső felhasználó:* a Tankerületi Központtal szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai,
59. *mentés (biztonsági mentés):* biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása,
60. *mobil eszköz:* asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok,

táblagépek, mobiltelefonok és okostelefonok,

61. *munkaállomás:* a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook),
62. *napló:* az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja,
63. *naplózás:* az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében,
64. *NISZ:* a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendeletben meghatározott központi szolgáltató,
65. *NISZ kapcsolattartó:* NISZ által működtetett Ügyfélszolgálat, illetve helyi hibaelhárítás során a közvetlen technikai támogató, illetve a fejlesztési és egyéb, rendszerszintű jelentősebb változáskezelések esetében az ezzel megbízott ügyfélmenedzser,
66. *osztályozás:* adatok, információk, információs infrastruktúra elemek, információs infrastruktúrák biztonsági szempontból való osztályainak kialakítása és ez alapján osztályokba sorolása,
67. *program:* számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából,
68. *rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek,
69. *rendszerelem:* információs infrastruktúra elem,
70. *sebezhetőség:* olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi,
71. *személyi biztonság:* az adott rendszerrel/erőforrással kapcsolatba kerülő személyekre vonatkozó, alapvetően a hozzáférést, annak lehetőségeit és módjait szabályozó biztonsági szabályok és intézkedések összessége a kapcsolat felvétel tervezésétől, annak kivitelezésén keresztül a kapcsolat befejezéséig, valamint a kapcsolat folyamán a személy birtokába került információk vonatkozásában,
72. *szervezeti biztonság:* egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében,
73. *sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható,
74. *SLA:* szolgáltatási szint megállapodás (Service Level Agreement), amely a megrendelő (Klebelsberg Központ) és a szolgáltató (NISZ) között létrejött egyedi szolgáltatási megállapodás része, és amely fő tartalmi elemei:
    a) a szolgáltatótól elvárt feladatok, a szolgáltatás terjedelme,
    b) a szolgáltató rendelkezésre állása,
    c) ügyfél- és rendszertámogatás,
    d) változáskezelés,
    e) felelősségi viszonyok,

f) adatvédelmi követelmények,

75. *Súlyos biztonsági esemény:* olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek,
76. *szoftver:* a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve,
77. *teljes körű védelem:* azon bármilyen típusú aktív, vagy passzív védelmi intézkedések, melyek a rendszer összes elemére kiterjednek,
78. *tesztrendszer:* olyan informatikai rendszer (környezet), amelynek célja a fejlesztés vagy bevezetés alatt álló program kipróbálásának, oktatásának támogatása,
79. *titkosítás:* az informatikai rendszerben kezelt adatok bizalmasságának biztosítására szolgáló, nem a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet hatálya alá tartozó olyan tevékenység vagy eljárás, amelynek során az adatot úgy alakítják át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon, de a megismerésre jogosultak számára az adat az eredeti formájába visszaállítható legyen,
80. *veszély (fenyegetés):* természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett tárgyakra,
81. *védelem:* a biztonság megteremtésére fenntartására, fejlesztésére tett intézkedések, amelyek lehetnek elhárító, megelőző, ellenálló képességet fokozó tevékenységek, vagy támadás, veszély, fenyegetés által bekövetkező kár kockázatának csökkentésére tett intézkedések,
82. *visszaállítás:* az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása,
83. *zárt védelem:* az összes számításba vehető fenyegetést figyelembe vevő védelem.

MÁSODIK RÉSZ

III. FEJEZET

AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI STRUKTÚRÁJA, FELELŐSSÉGI KÖRÖK

5. A tankerületi igazgató feladatai

6. § A tankerületi igazgató felügyeli az informatikai biztonsági feladatok ellátását, felelős azok betartásáért. A tankerületi igazgató:

a) felelős a Tankerületi Központ informatikai tevékenységének jogszerűségéért, beleértve az informatikai biztonsági tevékenységet is,

b) kijelöli vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt, akit az elvégzett feladatokról és ellenőrzésekről évente beszámoltat,

c) kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről,

d) együttműködik a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetével (a továbbiakban: Hatóság vagy NBSZ NKI) és részére tájékoztatást nyújt a jogszabályi követelményeknek megfelelően.

6. Az elektronikus információs rendszer biztonságáért felelős személy feladatai

7. § (1) Az informatikai biztonsági szabályok betartásáról a tankerület igazgató által kijelölt vagy megbízott, az elektronikus információs rendszer biztonságáért felelős személy gondoskodik.

(2) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a tankerületi igazgatónak közvetlenül adhat tájékoztatást, jelentést.

(3) Az elektronikus információs rendszer biztonságáért felelős személy felel a Tankerületi Központnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:

a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,

b) elvégzi, illetve irányítja az a) pont szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,

c) a Tankerületi Központ és szervezeti egységei vonatkozásában ellátja az informatikai biztonsági szakmai irányítási és felügyeleti feladatokat,

d) előkészíti a Tankerületi Központ elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot, gondoskodik naprakészen tartásáról és oktatásáról,

e) elkészíti a Tankerületi Központ elektronikus információs rendszereinek informatikai biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását, gondoskodik a besorolások aktualizálásáról, eltérés esetén a cselekvési terv összeállításáról,

f) közreműködik az informatikai biztonsággal összefüggő döntések előkészítésében az informatikai biztonsági szempontok meghatározásával,

g) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a Tankerületi Központ e tárgykört érintő szabályzatait, szerződéseit,

h) kapcsolatot tart a Hatósággal és a kormányzati eseménykezelő központtal (GovCert), figyeli a kiadott riasztásokat és figyelmeztetéseket, szükség esetén intézkedik,

i) a Tankerületi Központ munkaállomásai informatikai biztonsági felügyeletével összefüggésben működtetési korlátozásokat írhat elő és ellenőrizheti azok betartását,

j) az elektronikus információs rendszert érintő biztonsági eseményről tájékoztatja a jogszabályok szerint meghatározott szervet,

k) informatikai biztonsági ellenőrzéseket hajt végre, az ellenőrzés során, annak tárgyában a Tankerületi Központ szervezeti egységeinek (amennyiben arról jogszabály másként nem rendelkezik) valamennyi – nem minősített – nyilvántartásába, iratába betekinthet, azokról másolatot készíthet, azzal kapcsolatban felvilágosítást kérhet, valamennyi helyiségébe beléphet munkaidőben és munkaidőn kívül,

l) az informatikai biztonság megsértésének észlelése esetén javaslatot tesz az érintett szervezeti egység vezetőjének a szükséges intézkedésekre vonatkozóan,

m) ellátja az informatikai biztonsági képzéssel, továbbképzéssel és tájékoztatással kapcsolatos, az IBSZ-ben számára meghatározott feladatokat.

(4) Az elektronikus információs rendszer biztonságáért felelős személy biztosítja az Ibtv.-ben meghatározott követelmények teljesülését a Tankerületi Központ valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködők, illetve – ha a Tankerületi Központ az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe – a közreműködők Ibtv. hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenysége esetén.

(5) Az egyes szervezeti egységekre vagy rendszerekre kiterjedő, rendkívüli (eseti jellegű) informatikai biztonsági ellenőrzést az elektronikus információs rendszer biztonságáért felelős személy végez vagy rendel el a tankerületi igazgató jóváhagyásával.

(6) Az elektronikus információs rendszer biztonságáért felelős személy ellenőrzi, hogy a Tankerületi Központ az elektronikus információs rendszerek kimeneti információit jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

7. Az informatikai vezető feladatai

8. § (1) A Gazdasági vezető (a továbbiakban: informatikai vezető) jelen szabályzat szerinti, az informatikai biztonságra vonatkozó feladat- és hatásköre a Tankerületi Központ minden informatikai rendszerelemére kiterjed. Jogosult minden olyan megbeszélésen személyesen vagy meghatalmazottja útján részt venni, amelynek informatikai biztonsági, informatikai adatvédelmi vonatkozása van. Ezen megbeszéléseken hozzászólási és javaslattételi joga van. Az informatikai vezető felel:

a) a Tankerületi Központ informatikai rendszerének folyamatos működéséért, a szükséges fejlesztések tervezéséért és kivitelezéséért, illetve az előbbiek sikeres kivitelezése érdekében szükséges döntések meghozataláért,

b) a Tankerületi Központ szervezeti egységei vezetői által a beosztottjaik részére igényelt számítógépes erőforráshoz való hozzáférési jogosultságok engedélyeztetéséért, azok beállításáért – ide nem értve az alkalmazásokon belüli jogosultságokat és

c) az informatikai katasztrófavédelmi terv elkészítéséért.

(2) A szervezeti egység vezetője igényének végrehajtását az informatikai vezető csak informatikai biztonsági okra hivatkozva tagadhatja meg.

(3) Az informatikai vezető felügyeli:

a) a szerverek, valamint a közvetlen hatáskörébe tartozó munkaállomások kiszállítását és az informatikai rendszerekbe állítandó eszközök tesztelését, használatba vételét,

b) közreműködik minden olyan eset kivizsgálásában, ahol a Tankerületi Központ informatikai biztonsághoz fűződő érdeke sérelmet szenved,

c) dönt a személyek IT által védett helyiségekbe (Server helyiség) történő belépési jogosultságairól, azok feltételeiről,

d) ellenőrzi az IT helyiségekhez tartozó kulcsdoboz használatát,

e) gondoskodik az informatikai üzemeltetési feladatkörök ellátásáról kormánytisztviselő kijelölésével vagy szerződéses kapcsolat útján,

f) kezdeményezheti a felhasználók részére az informatikai biztonsági ismeretek oktatását,

g) minden üzemeltető és felhasználó felé köteles és jogosult intézkedni, szabálytalanság esetén a részükre biztosított informatikai szolgáltatást a tankerületi igazgató egyidejű tájékoztatása mellett korlátozhatja; az illetékes szervezeti egység vezetőjével történt egyeztetés alapján módosíthatja a felhasználók jogosultságait, ideértve az új felhasználók informatikai rendszerbe való felvételét is a Klebelsberg Központ Informatikai Főosztálya közreműködésével,

h) az informatikai biztonsági felelőssel és az érintett szervezeti egység vezetőjével együtt évente felülvizsgálja az információvédelmi osztályba sorolásokat, amely alapján javaslatot tesz a szükséges módosításokra,

i) engedélyezi a mentések felhasználását.

8. Az informatikus

9. § (1) Az informatikus (másképpen: rendszergazda) jelen szabályzat szerinti, informatikai biztonságra vonatkozó alapvető feladatai:

a) a szerverek és munkaállomások biztonsági funkcióinak beállítása és kezelése,

b) a rendszerkonfigurációs és rendszerbiztonsági adatok kezelése,

c) a rendszerprogramok telepítése,

d) a biztonsági másolatok és archiválások készítésének irányítása és a központi mentések lefutásának ellenőrzése és

e) hiba esetén az informatikai rendszer irányítása, rendszermodul helyreállítása és tesztelése.

(2) Amennyiben a felhasználó jogszabály által védett adatot tárol a rendszergazda részére javításra átadott eszközön, a felhasználó ilyen irányú írásbeli tájékoztatása esetén, a rendszergazda felel azért, hogy a javításra kiszállított eszköz jogszabály alapján védendő adatot ne tartalmazzon. Az ilyen adatok a felhasználó által megjelölt hálózati tárhelyre kerülnek mentésre.

(3) A rendszergazda minden olyan jogot gyakorol, amely az informatikai rendszer operációs rendszer szintű üzemeltetéséhez szükséges, így különösen

a) elvégzi a felhasználói eszközök beállításainak megváltoztatását az informatikai vezetővel történt egyeztetés alapján,

b) a szervezeti egység és az alkalmazásgazda kezdeményezését követően az informatikai vezető engedélye alapján koordinálja a rendszermentések visszaállítását,

c) a tevékenységét Szolgáltatási Szint Megállapodás (a továbbiakban: SLA, Service Level Agreement) szabályozhatja,

(4) A rendszergazdai feladatokat külső szerződő fél is elláthatja titoktartási nyilatkozattal, amennyiben megfelelő szakirányú tevékenységre jogosító igazolással rendelkezik.

9. Az adatgazda

10. § (1) Az adatgazda szerepét annak a szervezeti egységnek a vezetője tölti be, aki az adott hivatali folyamatért felelős. Több, egymáshoz kapcsolódó, vagy független hivatali folyamat esetén a szervezeti egységek ajánlása alapján az érintett szervezeti egységek közös felső vezetője dönt.

(2) Az adatgazda

a) informatikai biztonságra vonatkozó elsődleges feladata az adatok, az informatikai biztonsági

felelős által meghatározott szempontok szerinti biztonsági osztályba sorolása,

b) feladata az informatikai biztonsági felelős által meghatározott szempontok szerint meghatározni az adott központi alkalmazás üzemeltetésére vonatkozó Szolgáltatási Szint Megállapodás (SLA) követelményrendszerét,

c) köteles az Gazdálkodási, Üzemeltetési és Pályázati Főosztály ügyrendjében meghatározott tevékenységével, feladatkörével kapcsolatban gondoskodni az adatok jogszabályi előírásoknak megfelelő előállításáról, ellenőrzéséről, folyamatos szolgáltatásáról; felelős az adatok tartalmáért és határidőre történő szolgáltatásáért,

(3) Az adatgazda feladatainak ellátásával informatikai alkalmazásonként a szervezeti egységen belül az adott szervezeti egység vezetője írásban mást megbízhat. A megbízás alkalmazásonként lehetséges, amelynek tényéről az informatikai vezető írásban értesítendő.

(4) Több érintett szervezeti egység írásba foglalt javaslata alapján a közös felettes vezető dönt az informatikai adatgazda személyéről, amelyről tájékoztatja az informatikai vezetőt.

(5) Az adatgazda az informatikai vezető jóváhagyásával javaslatot tesz az alkalmazásgazda személyére.

10. Az alkalmazásgazda

11. § A tankerület nem rendelkezik EIR-rel, ezért nincs helyi alkalmazásgazda feladatkör.

11. A felhasználók

12. § (1) Általános felhasználók a Tankerületi Központ foglalkoztatottjai, illetve a külső felhasználók, akik az SLA-ban meghatározott alapjogosultságokat használják.

(2) A kiemelt felhasználók rendelkeznek az általános felhasználókhoz kapcsolódó jogokkal, valamint azon túlmenően a feladatkörüktől és a szakmai területtől függő további egyedi jogosultságokkal is. A kiemelt felhasználókat – az elektronikus információs rendszer biztonságáért felelős személy tájékoztatása mellett – a munkáltató jogokat gyakorló vezető, a szerződéskötést kezdeményező szervezeti egység vezetője jelöli ki.

(3) A Tankerületi Központ időszakos, illetve folyamatos feladatok végrehajtására igénybe vehet állományába nem tartozó külső felhasználókat általános, vagy kiemelt felhasználói jogosultságokkal. A Tankerületi Központ külső felhasználóval való szerződéskötésre vonatkozó rendelkezéseket külön szabályzat tartalmazza, az információbiztonsági követelményekkel kapcsolatos követelmények a 14. pontban kerültek meghatározásra.

(4) A (3) bekezdésben meghatározott igénybevételen túl a külső felhasználó által okozott informatikai, valamint az informatikai biztonsági követelmények betartásának ellenőrzéséért, szükség esetén a felelősségre vonás (illetve jogkövetkezmények bevezetésének) kezdeményezéséért, továbbá az IBSZ szerinti követelmények kommunikálásáért és a vonatkozó szerződésbe történő beépítéséért az a szervezeti egység a felelős, akinek érdekében a külső felhasználó igénybevételére sor került. A külső felhasználó:

a) aki a Tankerületi Központ rendszereivel kapcsolatos vagy azokat érintő munkavégzés céljából érkezett, a Tankerületi Központ területén a szerződés létrejötte után kizárólag a szerződéskötést kezdeményező szervezeti egység vezetőjének tudtával és az általa kijelölt személy felügyelete mellett tartózkodhat,

b) a munkafolyamat egyeztetése során minden olyan munkafolyamatról köteles beszámolni a szerződéskötést kezdeményező szervezeti egység vezetőjének, amely bármilyen módon érinti az informatikai rendszer biztonságát,

c) amennyiben az a munkavégzéshez feltétlenül szükséges, részére a Tankerületi Központ informatikai rendszereihez való hozzáféréshez ideiglenes, meghatározott időre és személyre szóló hozzáférési jogosultságot kell biztosítani, amelyről az érintett szervezeti

egység vezetője gondoskodik, ezen igényét a NISZ által üzemeltetett rendszer esetében a Klebelsberg Központ Informatikai Főosztálya útján jelzi a NISZ kapcsolattartónak.

(5) A Tankerületi Központ külső felhasználóval csak olyan szerződést köthet, amely a külső felhasználó tekintetében biztosítja a vonatkozó titokvédelmi szabályok érvényesülését. A szerződéskötés során figyelembe kell venni az IBSZ előírásait, a jogszabályi előírásokat (különös tekintettel a szellemi alkotásokhoz fűződő, illetve szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogokat).

IV. FEJEZET

AZ INFORMATIKAI BIZTONSÁGRA VONATKOZÓ FŐBB SZABÁLYOK

12. A felhasználókra vonatkozó szabályok

13. § (1) A Tankerületi Központban valamennyi felhasználó – jogosultságtól és állományba tartozástól függetlenül – felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért, így

a) a rá vonatkozó szabályok – elsősorban a Tankerületi Központtal fennálló, foglalkoztatásra irányuló jogviszonyt szabályozó jogszabályi rendelkezésekben foglaltak – szerint felelős az általa elkövetett informatikai vonatkozású szabálytalanságokért, valamint a keletkező károkért és hátrányért, különös tekintettel az informatikai biztonsági incidens fogalomkörébe tartozó cselekményekért,

b) köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,

c) köteles a számára szervezett informatikai biztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni,

d) köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,

e) köteles a belépési jelszavát (jelszavait) az előírt időben megváltoztatni, biztonságosan kezelni,

f) felügyelet nélkül a munkahelyen (munkaállomáson) személyes adatot vagy minősített adatot tartalmazó dokumentumot, adathordozót nem hagyhat,

g) a számítógépét (a munkahelyi munkaállomást) a helyiség elhagyása esetén zárolni köteles oly módon, hogy ahhoz csak jelszó vagy hardveres azonosító eszköz használatával lehessen hozzáférni,

h) információbiztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről köteles tájékoztatni a közvetlen felettesét és elektronikus információs rendszer biztonságáért felelős személyt,

i) köteles a folyó munka során nem használt hivatalos adatokat, dokumentumokat, nem nyilvános anyagokat, adathordozókat elzárni,

j) köteles a munkahelyről történő eltávozáskor az addig használt – kivéve, ha ez a rendszer(ek) más által történő használatát, vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,

k) az elektronikus levelezés és az internet használat során tartózkodni köteles a biztonság szempontjából kockázatos tevékenységektől.

(2) A Tankerületi Központ informatikai rendszerét használó valamennyi felhasználónak tilos:

a) az általa használt eszközök biztonsági beállításait megváltoztatni,

b) a saját használatra kapott számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),

c) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,

d) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,

e) a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra, illetve az elektronikus információs rendszereket összekapcsolni az informatikai rendszert üzemeltetők jóváhagyása nélkül,

f) a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,

g) bármilyen szoftvert installálni, internetről letölteni, külső adathordozóról merevlemezre másolni az elektronikus információs rendszer biztonságáért felelős személy engedélye, illetve az üzemeltető közreműködése nélkül, a munkaállomásokon nem a Tankerületi Központban rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,

h) bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,

i) az általa használt adathordozó (pl. CD, DVD, pendrive stb.) eszköz számítógépben hagyni a munkaállomásáról való távozás esetén,

j) ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni,

k) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket, stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,

l) láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni,

m) a Tankerületi Központ működésével nem összeegyeztethető kereskedelmi célú hirdetéseket, reklámokat a belső címzettek felé továbbítani, bármilyen nem hivatali levelező listára hivatali e-mail címmel – az elektronikus információs rendszer biztonságáért felelős személy külön engedélye nélkül – feliratkozni, kivéve, ha az a munkavégzéshez szükséges:

   ma) a Tankerületi Központ által megrendelt, működtetett, vagy előfizetett szolgáltatásokat,

   mb) belső információs rendszereket,

   mc) közigazgatási, illetve nemzetközi, vagy uniós szervek/szervezetek által biztosított szolgáltatásokat,

   md) közigazgatási szervek által felügyelt szervek, vagy szervezetek által biztosított szolgáltatások levelező listáit.

(3) A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat harmadik személy hajtotta végre, amennyiben erre az IBSZ előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

(4) Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és az operációs rendszerből is kijelentkezett.

(5) A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

(6) A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

13. Vezetőkre vonatkozó szabályok

14. § (1) A Tankerületi Központ szervezeti egységeinek vezetője (a továbbiakban: vezető) jogosult és köteles meghatározni az irányítása alá tartozó foglalkoztatottak munkavégzéséhez szükséges:

a) informatikai, irodatechnikai, multimédiás és kommunikációs eszközök körét,

b) a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.

(2) A Tankerületi Központ szervezeti egységének vezetője köteles együttműködni az elektronikus információs rendszer biztonságáért felelős személlyel annak informatikai biztonsági feladatai ellátása során.

(3) A használatra kiadott informatikai, irodatechnikai, multimédiás vagy adathordozó eszközöknek a feladat végrehajtásra vonatkozó indokoltságát, meglétét az engedélyező vezetőnek évente felül kell vizsgálnia és az indokoltság megszűnése esetén gondoskodnia kell az eszköz visszavétele felől.

(4) A vezető jogosult és köteles az informatikai eszközök munkavégzéshez szükséges használatának biztosítása érdekében a szükséges informatikai eszköz és jogosultság igénylési eljárásokat kezdeményezni a rendszergazda felé.

(5) A vezető köteles gondoskodni az irányítása alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ és az IBSZ-szel kapcsolatos más rendelkezések szükséges mértékű ismeretét is.

(6) A vezető az informatikai biztonsági előírások megsértésének észlelése esetén köteles:

a) azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,

b) kivizsgálni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,

c) a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

(7) A vezető jogosult az irányítása alá tartozó szervezeti egység tevékenységével kapcsolatos informatikai biztonsági feltételrendszerre, vagy azok szabályozására vonatkozóan javaslatot tenni az elektronikus információs rendszer biztonságáért felelős személye felé.

14. Szerződéses partnerekre és külső felhasználókra vonatkozó szabályok

15. § (1) A Tankerületi Központ informatikai rendszereihez és eszközeihez külső felhasználó csak érvényes szerződés alapján, dokumentáltan férhet hozzá.

(2) A Tankerületi Központ informatikai rendszereihez és eszközeihez hozzáférő külső felhasználó egyedileg köteles nyilatkozatot tenni arról, hogy az IBSZ-ben foglaltakat megismerte és az abban foglaltakat magára nézve kötelezőnek ismeri el.

(3) A Tankerületi Központ informatikai rendszereihez és eszközeihez hozzáférést biztosító szerződés csak olyan külső felhasználóval köthető, aki/amely az IBSZ-ben foglaltakat magára nézve kötelezőként elfogadja.

(4) Informatikai fejlesztések során a projekt teljes életciklusára nézve az egyes részeket oly módon kell dokumentálni (pl. fejlesztői dokumentáció, rendszerterv (logikai, fizikai, biztonsági), tesztelési dokumentáció, üzemeltetési dokumentáció), hogy azokból a biztonsági követelmények megvalósulása ellenőrizhető legyen, és biztosítsa a rendelkezésre állást.

(5) Amennyiben a szerződés egyedi szoftverfejlesztési tevékenységre irányul, úgy csak olyan szerződés köthető, amely alapján a fejlesztett szoftver kellő mélységben kommentezett forráskódját a Tankerületi Központ részére átadják, és a szerzői jogi védelem alá eső szoftver esetén a vagyoni jogokat a jogszabályok által engedélyezett legszélesebb körben átruházzák. Ettől csak különösen indokolt esetben lehet eltérni azzal, hogy a szerzői jogi védelem alá eső szoftver kizárólagos felhasználási joga a jogszabályok által engedélyezett legszélesebb körben a Tankerületi Központ részére ebben az esetben is átruházásra kerül.

(6) Az informatikai rendszerek üzemeltetése során külső felhasználó – a NISZ kivételével – kizárólag a Tankerületi Központ kijelölt munkatársának jelenlétében férhet hozzá a Tankerületi Központ informatikai rendszereihez.

(7) A Tankerületi Központban történő helyszíni munkavégzés felügyelet mellett történhet.

(8) Az informatikai rendszerek fejlesztése során külső felhasználó a teszt környezetben lévő, informatikai rendszerhez az elektronikus információs rendszer biztonságáért felelős személy engedélyével távoli eléréssel hozzáférhet. Az engedélyt elektronikus írásbeli formában a fejlesztést végző szervezeti egység vezetője igényli a fejlesztés kezdetekor.

(9) Szerződés kötése esetén az érintett elektronikus információs rendszereket, hálózatokat, architektúra elemeket, és az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket és eljárásokat, felelősségeket a felek között létrejött szerződésekben rögzíteni kell. A Tankerületi Központ a biztonsági osztályba sorolásait figyelembe veszi a szerződések megkötése előtt, és az elvárt biztonsági osztálynak megfelelő védelmi intézkedéseknek való megfelelést érvényesíti.

(10) A szerződéseknek tartalmaznia kell a részletszabályokat arra az esetre, ha a Tankerületi Központ Információs Vagyonelem Leltárában szereplő elemet a másik fél rendelkezésére bocsát. A szerződéseknek tartalmaznia kell a biztonsági előírások megsértése esetére vonatkozó szabályokat és a szankciókat.

(11) A szerződéseknek tartalmaznia kell a személyi változások esetén eszközölendő teendőket (például: munkatárs kilépése esetén az egyedi jelszavak, vagy hitelesítő eszközök visszavonása), az információbiztonságot érintő szerepköröket és felelősségeket. Amennyiben a felelősség megosztott, abban az esetben a részleteket minden esetben ki kell bontani, hogy az elszámoltathatóság elve ne sérüljön. Szerződéses követelményként kell továbbá megkövetelni a partnerektől, hogy a Tankerületi Központ hálózatát vagy valamely elektronikus információs rendszerét távolról elérő személy vagy szervezet milyen védelmi intézkedést kell, hogy foganatosítson a távoli eléréshez igénybe vett munkaállomásokon, eszközökön (például: kártékony kódok elleni védelem).

(12) Kötelező meghatározni a szerződésekben az incidensek és biztonsági események jelentésének részletszabályait. Ez jelenti a kapcsolattartó személyek és elérhetőségek, a bekövetkezett biztonsági esemény időpontját, helyét, hatását, várható hatását, a kockázatok mérséklésére megtett intézkedéseket, és kapcsolódó technikai adatokat, információkat. Azonnali jelentési kötelezettség csak a biztonsági esemény bekövetkeztére kell, hogy vonatkozzon, a részletes további információk az eseménykezelés után is tudomására hozható a másik félnek.

(13) A szerződésekben minden esetben ki kell kötni az ellenőrzések lehetőségének meglétét, amely garanciát nyújt a védelmi intézkedések betartásának biztosítására, illetve a megfelelő SLA-kat. Ha az ellenőrzés nem lehetséges, vagy nem célszerű, esetleg nem áll rendelkezésre a megfelelő erőforrás a Tankerületi Központ részéről, a megfelelő információbiztonsági tanúsítvány meglétének ellenőrzése is megfelelő bizonyosságot nyújthat.

(14) A jelen IBSZ-ben megfogalmazott szabályok megsértése esetén a Tankerületi Központ a szerződésben lefektetett feltételek fennállása esetén jogosult a szerződést megszüntetni vagy a szerződésben megfogalmazott szankciókat alkalmazni.

V. FEJEZET

INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK TELJESÜLÉSE

15. Szervezeti biztonsági követelmények

16. § (1) Az egyes informatikai rendszerekkel és adathordozókkal kapcsolatos fejlesztési, üzemeltetési és biztonsági tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, működtetési és védelmi terveket, dokumentumokat, előírásokat úgy kell elkészíteni, hogy azok a biztonsági osztályozási előírások figyelembevételével garantálják az információbiztonság szükséges és elégséges szintjét. Ezen elvek alapján kockázatarányos, differenciált, többszintű informatikai védelmi rendszert

kell kialakítani és működtetni.

(2) Az összeférhetetlenség elvét érvényesíteni kell oly módon, hogy a feladategyesítésből eredő hibák és rosszindulatú tevékenységek kockázatát kizárják, vagy elfogadható szintre csökkentsék.

(3) Minimális összeférhetetlenségi szabályok különösen:

a) az informatikai rendszerek felügyelete és üzemeltetése vonatkozásában érvényesíteni kell azt, hogy az információbiztonsági felelős és a rendszergazda az informatikával összefüggő feladatain kívül ne lásson el más szakmai (például köznevelés-igazgatási, szakképzés-szervezési stb.) feladatokat,

b) a szakmai és funkcionális informatikai alkalmazás szakmai felügyeletét kizárólag a Tankerületi Központ Gazdálkodási, Üzemeltetési és Pályázati Főosztálya láthatja el,

c) a fejlesztési, a minőségbiztosítási és az üzemeltetési feladatokat ellátó egységeket a visszaélések megelőzése érdekében szervezeti szinten el kell különíteni egymástól,

d) az informatikai szerepkörök/feladatok személyre (véglegesen vagy átmeneti időszakra történő) telepítését belső felhasználók esetében úgy kell végrehajtani, hogy az üzemeltetési, fejlesztési, változáskezelési, minőségbiztosítási, információbiztonság felügyeleti feladatok ellátásának egymástól való függetlensége biztosított legyen,

e) az informatikai szerepkörök/feladatok személyre telepítésekor kötelező gondoskodni a helyettesítésről oly módon, hogy e feladatokat a Tankerületi Központ más foglalkoztatottja is el tudja látni,

f) a feladatok és felelősségek személyekhez rendelésekor biztosítani kell a felelősségi viszonyok egyértelmű megállapíthatóságát.

(4) Összeférhetetlen szerepkörök az adatgazdai, az informatikai rendszerszolgáltatói és a felügyeleti szerepkörök.

(5) A Tankerületi Központ munkavállalói biztonsági szempontból két csoportba kerülnek besorolásra. A fokozott biztonsági szempontú munkakörök/álláshelyen ellátandó feladatok a következők: tankerületi igazgató, szakmai vezető, gazdasági vezető és a szervezeti egységek vezetői. Általános biztonsági szempontú munkakörök, álláshelyen ellátandó feladatok: ügyintéző, kormányzati ügykezelő, technikai dolgozó. A fokozott biztonsági szempontú munkaköröket/álláshelyen ellátandó feladatokat betöltő személyek információbiztonsági tájékozottságára az oktatások és tudatosító tevékenységek során kiemelt figyelmet kell fordítani, mivel fokozott fenyegetésnek vannak kitéve döntési és egyéb privilegizált jogköreik miatt.

16. Személyi biztonsági követelmények, oktatás, jogosultságkezelés

17. § (1) A foglalkoztatottakat a Tankerületi Központban végzendő tevékenység megkezdése előtt informatikai biztonsági képzésben kell részesíteni.

(2) Az informatikai biztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá, ha a Tankerületi Központ informatikai biztonságát, illetve az IBSZ tartalmát érintő jelentős változás következik be, az IBSZ hatályba lépését, illetve a jelentős változását követő 90 napon belül a felhasználókat informatikai biztonsági továbbképzésben, a külső felhasználókat informatikai biztonsági tájékoztatásban kell részesíteni (a továbbiakban együtt: oktatás).

(3) Az oktatás tematikájának összeállításáért a Tankerületi Központ elektronikus információs rendszer biztonságáért felelős személye, az oktatás megszervezéséért, végrehajtásáért a szervezeti egység vezetője a felelős. A Tankerületi Központban a szervezeti egység vezetője által kijelölt személy látja el az oktatási feladatot. A fokozott biztonsági szempontú munkaköröket, álláshelyen ellátandó feladatokat ellátó személyek oktatása során a 16. § (5) bekezdésében foglaltakra kiemelt figyelmet kell fordítani.

(4) Az oktatáson történt részvételt a megjelent személyek a részvételről szóló nyilatkozat és az informatikai biztonsági oktatási nyilvántartó lap (1-2. melléklet) aláírásával igazolják. Az oktatáson való

részvételről szóló nyilatkozatban az oktatáson történt részvétel igazolása mellett a résztvevők kötelesek nyilatkozni arról, hogy az informatikai biztonsági előírásokat megismerték és azok betartását magukra nézve kötelezőnek fogadják el. Az oktatáson való részvételről szóló nyilatkozatot foglalkoztatottak esetében a személyügyi anyaggal együtt, külső felhasználó esetében a szerződéssel együtt kell őrizni.

(5) A külső felhasználók IBSZ-szel való megismertetése a szerződéskötést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.

(6) Amennyiben egy felhasználó minősített adatok elérésére, olvasására vagy kezelésére kap jogosultságot, akkor e tekintetben a külön jogszabály rendelkezései szerint kell eljárni.

(7) Jogosultság létrehozása a kinevezési dokumentumok aláírását, valamint a Szolgáltatási és Ellátási Alapadat Tár (a továbbiakban: SZEAT)-ba történő felvételt követően, a Klebelsberg Központ személyi ügyekért felelős szervezeti egysége közreműködésével történik.

(8) A jogosultságok kiosztása előtt, amennyiben az adott munkakörben álláshelyen ellátandó feladat, megköveteli a tipikus jogoktól – ide nem értve a munkavégzéshez szükséges adatbázisok elérését – történő eltérést a Tankerületi Központ gazdasági vezetőjének egyetértését kell kérnie.

(9) A hozzáférési jogosultság – vezetői döntést követően – zárolásra, megszüntetésre kerül a felhasználó hozzáférést megalapozó jogviszonyának azonnali hatályú megszüntetésekor. A jogviszony más jogcím alapján történő megszüntetése, illetve megszűnése esetén a hozzáférési jogosultság a jogviszony megszűnése – vagy amennyiben előbb bekövetkezik a munkavégzési kötelezettség alóli mentesítés – napjától kerül zárolásra.

(10) A hozzáférési jogosultság a foglalkoztatott jogviszonyának fennállása alatt zárolásra, megszüntetésre vagy módosításra kerül a szervezeti egység vezetőjének – az informatikáért felelős szervezeti egysége felé tett – erre irányuló kérése esetén is.

(11) A felhasználó hozzáférést megalapozó jogviszonyának megszűnésekor a munkáltatói jogkör gyakorlója, illetve a szerződéskötést kezdeményező szervezeti egység vezetője a felhasználó tájékoztatása mellett köteles rendelkezni a felhasználó adatainak, munkavégzéssel kapcsolatos dokumentumainak további kezeléséről (archiválás, törlés, harmadik személy általi hozzáférhetőség).

(12) Amennyiben a foglalkoztatási jogviszony – amely alapján valamely személy hozzáféréssel rendelkezett a Tankerületi Központ nem nyilvános besorolású adataihoz – bármely okból megszűnik, akkor:

a) a jogosultság kiadásáért felelős vezetőnek legkésőbb a felhasználó foglalkoztatotti jogviszonyának megszűnésével egyidejűleg, illetve a munkavégzés alóli mentesülés napján kezdeményeznie kell a jogosultságok megvonását a Klebelsberg Központ személyügyekért felelős szervezeti egységénél,

b) a gazdasági vezető a jogviszony megszűnéséről értesíti a NISZ-t annak érdekében, hogy az érintett személy által használt, a NISZ vagyonkezelésében lévő informatikai eszközök a NISZ raktárába vagy más felhasználó használatába kerüljenek, továbbá az adatokhoz és rendszerekhez való hozzáférési jogosultságának törlése iránt a NISZ haladéktalanul intézkedhessen.

(13) Kérés esetén mind az informatikáért felelős szervezeti egység, mind a NISZ a saját maga által kezelt rendszerekkel kapcsolatban elvégzi az ezeken az adathordozókon tárolt nem nyilvános adatok megfelelő kezelését.

(14) Azonosítás és hitelesítés nélküli tevékenység végzése a Tankerületi Központ elektronikus információs rendszereinek használata tekintetében nem engedélyezett, kizárólag az azonosított és hitelesített személyek általi tevékenységek végzése megengedett.

17. Fizikai biztonsági követelmények

18. § (1) Az informatikai eszközöket úgy kell telepíteni és tárolni, hogy azokhoz a foglalkoztatottakon, külső felhasználókon kívüli más személy hozzáférése kizárt legyen.

(2) A Tankerületi Központ tulajdonát képező vagy az általa használt informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót a Tankerületi Központ objektumaiból kivinni csak hivatali feladat ellátására lehet.

18. Informatikai biztonsági követelmények

19. § (1) Az informatikai rendszerekben csak jogtiszta szoftver telepíthető. Szoftverek telepítését kizárólag a NISZ, vagy a Tankerületi Központ informatikáért felelős szervezeti egységének munkatársa végezheti.

(2) A hivatali feladatok ellátásához szükséges felhasználáson kívül informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót az informatikai rendszerekhez csatlakoztatni tilos.

(3) Nem a Tankerületi Központ tulajdonát képező informatikai, irodatechnikai, multimédiás eszközt az informatikai rendszerekhez vagy azok elemeihez csatlakoztatni tilos. Kivételt képeznek a Tankerületi Központ alap- vagy funkcionális tevékenységével összefüggésben a Tankerületi Központtal együttműködő partnerektől hivatalos tevékenységük során átvett eszközök.

(4) A Tankerületi Központ területén a Tankerületi Központ által kezelt adatok védelmére vonatkozó rendelkezéseket vagy személyiségi jogokat sértő, továbbá a Tankerületi Központ működésére vonatkozó magáncélú adatrögzítés – beleértve a hang- és képfelvétel készítését is – tilos.

(5) Az informatikai rendszerekben végrehajtott műveleteket a felhasználó azonosítását lehetővé tevő módon naplózni kell.

19. Adminisztratív biztonsági követelmények

20. § (1) Az informatikai rendszerek teljes életciklusát dokumentálni kell, így a tervezés, a fejlesztés és továbbfejlesztés, a tesztelés és ellenőrzés, az üzemeltetés és karbantartás, valamint a megszüntetés fázisait is.

(2) A dokumentáció teljességéért és naprakészségéért az informatikai rendszert fejlesztő, a rendszer üzemeltetésének megkezdésétől a szakmai felügyeletet ellátó szervezeti egység vezetője felel.

(3) Az informatikai rendszer dokumentációja akkor teljes, ha tartalmazza mind a funkcionális, mind a biztonsági megfelelőségre vonatkozó valamennyi lényeges adatot.

(4) Az elektronikus adatokat tároló eszközöket a rajtuk tárolt vagy tárolandó adatokat a jogszabályi előírásoknak megfelelően kell kezelni.

(5) Az elektronikus adatokat tároló eszközök azonosítását, mozgásuk nyomon követhetőségét az átadás-átvétel, továbbítás, selejtezés, megsemmisítés dokumentálásával biztosítani kell.

(6) Az elektronikus adathordozók kezelése vonatkozásában az IBSZ-ben nem szabályozott kérdésekben az Iratkezelési Szabályzat előírásai értelemszerűen irányadóak.

(7) A papír alapú dokumentumok előállítására alkalmas eszközök (nyomtató, plotter, fax) használatára az informatikai eszközökre vonatkozó szabályozások érvényesek. A felhasználók számára tiltott tevékenységek a Tankerületi Központ adatait nyomtatott formában megjelenítő eszközök esetén is irányadóak.

VI. FEJEZET

AZ INFORMÁCIÓBIZTONSÁG MŰKÖDTETÉSE

20. Megfelelés az IBSZ-nek, fenyegetettségek

21. § (1) A Tankerületi Központ információbiztonsági fenyegetettségének elemzését és a kockázatok meghatározását évente el kell végezni.

(2) Az IBSZ-nek megfelelő működést igény szerint, de legalább évente teljeskörűen ellenőrizni kell.

(3) A fenyegetettségek elemzését és a kockázatok meghatározását az elektronikus információs rendszer biztonságáért felelős személy hajtja végre, szükség szerint független külső szakértő bevonásával.

21. Az IBSZ felülvizsgálata, aktualizálása

22. § (1) Az IBSZ-t szükség szerint – de legalább évente – felül kell vizsgálni és aktualizálni kell, így különösen:

a) minden olyan szervezeti változás esetén, amely a Tankerületi Központ szervezeti egységei (főosztályok) megszűnésével vagy jelentős átalakulásával jár,

b) súlyos informatikai biztonsági eseményeket (incidensek) követően, az esemény tanulságaira figyelemmel,

c) a szabályozási környezet változása esetén, amennyiben az az IBSZ-ben foglaltakat érinti.

(2) Amennyiben az IBSZ rendkívüli módosítása szükséges – a módosítás jellegétől vagy terjedelmétől függetlenül – az elektronikus információs rendszer biztonságáért felelős személy közvetlenül jelzi ezt a tankerületi igazgatónak.

22. Az informatikai biztonsági események felismerése, jelentése

23. § (1) Minden felhasználó kötelessége – amennyiben kellő gondossággal eljárva azt felismerhette – a lehetséges legrövidebb időn belül közvetlen vezetőjén keresztül bejelenteni az elektronikus információs rendszer biztonságáért felelős személy részére minden olyan veszélyforrást, amely az elektronikus információbiztonságra nézve érdemi fenyegetést jelent vagy jelenthet.

(2) A felhasználó részéről különösen a következő veszélyforrások jelzése kötelező:

a) az IBSZ-ben, a vonatkozó jogszabályokban előírt elektronikus információbiztonsági rendszabályok lényeges megszegése, illetve ennek gyanúja,

b) a felismert vagy felismerni vélt, az elektronikus információbiztonságot lényegesen veszélyeztető esemény, ezen belül különösen:

ba) nem nyilvános adat illetéktelen személy általi megismerése,

bb) informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,

bc) informatikai rendszer működésének, használatának jogosulatlan akadályozása,

bd) nem engedélyezett vagy licenccel nem rendelkező szoftver telepítése,

be) felhasználói jelszavak egymás közötti megosztása, hozzáférhetővé tétele,

bf) vírusfertőzés, kémprogramok, billentyűzetleütést figyelő alkalmazások megjelenése,

bg) mobil eszköz elvesztése, ellopása esetén,

bh) fentiek bármelyikére tett kísérlet

(a továbbiakban együtt: biztonsági események).

(3) Nem számít informatikai biztonsági eseménynek az informatikai hiba, meghibásodás vagy rendszeresemény, amely nem érinti az informatikai szolgáltatások minőségét és azt az üzemeltetők képesek megoldani.

(4) A bejelentés során minimálisan megadandó információk:

a) az informatikai biztonsági esemény pontos leírása,

b) érintett informatikai szolgáltatás pontos megnevezése,

c) érintett informatikai eszköz gyári száma, leltári száma, típusa,

d) telephely neve, pontos címe (emelet, ajtó),

e) észlelő neve, elérhetősége (opcionális),

f) a szervezeti egység vezetője által kijelölt helyszíni kapcsolattartó neve, elérhetősége.

(5) A KK Informatika szükség esetén támogatást nyújt az elektronikus információs rendszer felhasználóinak a biztonsági események kezeléséhez és jelentéséhez.

23. Biztonsági események kivizsgálása és azt követő tevékenységek (biztonsági eseménykezelési terv)

24. § (1) A biztonsági eseményeket soron kívül ki kell vizsgálni. A vizsgálatot az elektronikus információs rendszer biztonságáért felelős személy folytatja le, szükség szerinti mértékben bevonva a NISZ által a vizsgálat támogatására kijelölt képviselőit.

(2) A vizsgálat eredményét az elektronikus információs rendszer biztonságáért felelős személy írásban dokumentálja, amelyből 1-1 példányt kap az elektronikus információs rendszer biztonságáért felelős személy, illetve a biztonsági eseményben közvetlenül érintett(ek).

(3) A biztonsági eseménykezelésre történő felkészülés során a lehető legalaposabban kell eljárni, ehhez szükséges a biztonsági eseménykezelést támogató erőforrások meghatározása:

a) humán erőforrás: a biztonsági eseménykezelésben kötelezően résztvevő személyek, illetve az általuk a biztonsági eseménykezelésbe bevont személy, aki lehet a jelen IBSZ személyi hatálya alá eső személy, vagy szerződés alapján meghatározott személy, aki részt vehet a Tankerületi Központ biztonsági eseményeinek a kezelésében,

b) a biztonsági események észleléséhez szükséges a rendelkezésre álló riasztást generáló rendszerek rendelkezésre állása vagy az üzemeltető jelzése,

c) a Tankerületi Központ honlapja alkalmas az elektronikus információs rendszerekben történt biztonsági események érintettek részére történő kommunikációjára; alternatív megoldásként további platformok használatosak az érintett felek felé történő adatok, információk közlésére (például közösségi média platformok),

d) jelen IBSZ személyi hatálya alá tartozó személyek saját hordozható számítógépei (laptopjai) felhasználhatók az incidenskezelés során az IBSZ-ben meghatározott szabályoknak megfelelően,

e) biztonsági események elemzéshez a források: port lista; operációs rendszerek, alkalmazások, protokollok, behatolás érzékelő és antivírus megoldások dokumentációi; hálózati diagramok, információs vagyonelem leltár; kritikus fájlok, stb.

(4) A biztonsági eseményeket értékelni kell. Az értékelés során szükséges megállapítani, hogy súlyos biztonsági eseményről van-e szó. A biztonsági esemény súlyos biztonsági eseménynek nyilvánítása az elektronikus információs rendszerek biztonságáért felelős személy támogatása mellett a tankerületi igazgató feladata.

(5) Egy biztonsági esemény kategorizálásánál figyelembe kell venni, hogy az miből ered, milyen okok vezettek a bekövetkezéséhez. Ennek megfelelően egy esemény lehet:

a) Szándékos vagy nem szándékos cselekmény,

b) Balesetből eredő esemény,

c) Technikai hibából eredő esemény,

d) Környezeti tényező okozta esemény.

Az értékelési eljárás során szükséges figyelembe venni, hogy milyen kategóriába tartozik az adott esemény és a reakciónak ezen információ tudatában kell, hogy történjen.

(6) A súlyosabb működési és biztonsági eseményről (amennyiben a Tankerületi Központ nem képes önerőből vagy a szerződéses partnerek segítségével azt megoldani) az erre a feladatra feljogosított

személye haladéktalanul, de legfeljebb az észlelést követő 4 órán belül értesíti az Eseménykezelő Központot a https://nki.gov.hu/intezet/tartalom/incidens-bejelentes/ honlapon található űrlapon keresztül, vagy a CSIRT@nki.gov.hu e-mail címen. Abban az esetben, ha a biztonsági esemény személyes adatokat is érint, az biztonsági eseménykezelő személy tájékoztatni köteles a Tankerületi Központ Adatvédelmi Tisztviselőjét, aki a Tankerületi Központ Adatvédelmi dokumentációjában meghatározottak szerint köteles eljárni.

(7) A biztonsági esemény megállításához szükséges annak meghatározása, hogy az pontosan honnan ered (fizikailag vagy logikailag), és lehetőség szerint a rendszer szegmentációt biztosítani szükséges, hogy az incidens ne terjedhessen tovább. Ennek megvalósításához használni kell a rendszer leírásokat, konfigurációs beállítások dokumentációit, adat/kommunikációs kapcsolatok rendszer leírásait, ábráit, és minden olyan információt, amely segíthet a biztonsági esemény megállításában.

(8) A biztonsági esemény megszüntetését és káros kód eltávolítását úgy kell intézni, hogy a Tankerületi Központ elektronikus információs rendszereiben ne maradjon hátsó kapu, amelyen további támadások valósíthatók meg. Ennek tényéről szükséges meggyőződni. Ismert támadás esetén nyilvánosan elérhető információkat fel lehet használni, egy támadás mechanizmusának feltérképezéséhez.

(9) A biztonsági eseményt követő helyreállítási tevékenységet sikeres megszüntetést követően lehet csak megkezdeni. Abban az esetben, ha a biztonsági esemény nem megszüntethető, vagy csak aránytalan erőforrás felhasználásával lehetséges, akkor az nem kerül lezárásra. A helyreállítás lépéseit a biztonsági esemény nyilvántartásában a megfelelő részében fel kell sorolni.

(10) A biztonsági eseményt követően a kapcsolódó kockázatokat fel kell tárni és amely kockázatot eddig a Tankerületi Központ kockázatelemzése nem tartalmazott, azzal a kockázatelemzést módosítani/kiegészíteni szükséges. Ha tartalmazta a kockázatelemzés az adott kockázatot, akkor a bekövetkezés miatt módosítandó a bekövetkezési valószínűsége a kockázatnak, a hatás pedig a ténylegesen megállapított hatás értékének megfelelően módosítandó.

(11) A biztonsági esemény lezárása annak a függvénye, hogy sikeresen megszüntetésre került-e, illetve a helyreállítási tevékenységeket elvégezte-e a Tankerületi Központ, valamint a következtetések levonásra kerültek. Ha az előzőben említettek bármelyike nem történt meg, úgy a biztonsági esemény nem tekinthető lezártnak, és a továbbiakban is szükséges azzal foglalkozni. Amennyiben egy biztonsági esemény nem zárható le az biztonsági események nyilvántartásának megőrzési idején belül, akkor lezáratlanul törölni kell a nyilvántartásból az azzal kapcsolatos adatokat, információkat.

(12) A biztonsági eseménykezelés jövőbeli sikeressége érdekében tesztelni kell a jelen pontban foglaltakat. Legalább évente egy alkalommal szükséges egy olyan szcenárióval tesztelni az eljárásrend megfelelőségét, amely az adott évben kihívás elé állította a hasonló állami szereplőket. Előzőre tekintettel az elektronikus információs rendszerek biztonságáért felelős személy figyelemmel kíséri az állami szereplőket érintő biztonsági eseményeket, amelyeket felhasználva elkészíti a teszteléshez szükséges forgatókönyvet. A tesztelésbe be kell vonni azon személyeket is, akik nem vettek még részt ilyen tesztelésben. Annak érdekében, hogy mindenki tudja, hogy mi a teendő egy biztonsági esemény bekövetkezése esetén, szükséges a jelen eljárásrend ismerete, annak oktatása. A biztonsági eseménykezelési eljárás megfelelő ismerete érdekében szükséges minden évben az információbiztonsági oktatási tervbe beépíteni az ezzel kapcsolatos oktatási kötelezettséget. A teszt elvégzését követően a hibákat, hiányosságokat fel kell tárni, és az eljárásrend felülvizsgálata alkalmával javítani szükséges a nem megfelelőségeket. Amennyiben a tesztelés során egyéb szabályozói vagy eljárásrendbeli hiányosság, vagy információbiztonsági nem megfelelőségre derül fény, azt szintén javítani kell. A tesztelésről záró jegyzőkönyv és jelentés készül, ami tartalmazza minden, a teszteléssel kapcsolatos adatot és információt, továbbá a javaslatokat a Tankerületi Központ információbiztonsági rendszerének fejlesztésére.

24. Biztonsági események nyilvántartása

25. § (1) A biztonsági események kapcsán tett bejelentések, a lefolytatott vizsgálatok, valamint a végrehajtott intézkedések adatait külön nyilvántartás tartalmazza, amelyet az elektronikus információs

rendszer biztonságáért felelős személy vezet.

(2) A Biztonsági Nyilvántartás adatait fel kell használni:

a) a bekövetkezett biztonsági esemény következményeinek enyhítésére,

b) a jövőben várható hasonló biztonsági események megelőzésére, bekövetkezési gyakoriságának csökkentésére,

c) a vizsgálat során feltártakhoz hasonló védelmi gyengeségek kezelésére, a védelmi intézkedések fejlesztésére.

(3) A biztonsági eseményeket a nyilvántartásban priorizálni szükséges, annak érdekében, ha egyszerre két biztonsági eseményt is kell kezelni, akkor a meghatározott sorrendben történjen az eseménykezelés. Ennek megfelelően a biztonsági esemény megítéléséhez a következő prioritási lista nyújt segítséget (két azonos besorolású biztonsági esemény bekövetkezése esetén a tankerületi igazgató dönt az elektronikus információs rendszer biztonságáért felelős személy javaslatára a prioritási sorrendről):

a) alacsony szintű a biztonsági esemény hatása, ha személyes adatok nem érintettek. Például: az irodahelyiségben, ahol ebédszünet alatt eltűnik egy személyes adatokat nem tartalmazó eszköz, ám az IBSZ információvagyon felmérése és osztályozása részében meghatározottak szerint „Elhanyagolható” osztályú adatokról van szó,

b) közepes szintű a biztonsági esemény hatása, ha rövid ideig tartó hatást gyakorol a bizalmasság, sértetlenség és rendelkezésre állás követelményeire. Néhány személyes adat érintett és az irodai rendszerek vannak a középpontban. Például zsarolóvírus támadás egy munkaállomás ellen. Az IBSZ információvagyon felmérése és osztályozása részében meghatározott „Alap” osztályú adatokról van szó,

c) magas szintű a biztonsági esemény hatása, ha magas és hosszan tartó hatás a bizalmasság, sértetlenség és rendelkezésre állás követelményeire. Magas számú személyes adat érintett benne, a használt és/vagy üzemeltetett rendszerek több, mint a fele nem működik. Például zsarolóvírus támadás az elektronikus információs rendszerek ellen. Minden szándékos cselekmény, amely személyes adatokat érint, magas súlyossági fokúnak minősül. Az IBSZ információvagyon felmérése és osztályozása részében meghatározott „Fokozott” osztályú adatokról van szó.

(4) A biztonsági esemény nyilvántartásnak része a biztonsági esemény megállítását követően begyűjtött bizonyítékok. Bizonyítékul szolgálhat: naplóbejegyzés, log, riasztási értesítés, e-mail (csatolmánnyal, káros linkkel stb.), fénykép, videó, képernyőkép stb., feljegyzés, titkosított-, vagy egyéb módon sérült fájl/fájlok, dokumentumok, dokumentációk, rögzített telefonbeszélgetés, kamera felvétel, patch telepítésről bizonyíték, nyilvántartás stb., egyéb bizonyítékok. A biztonsági eseménykezelés során begyűjtött bizonyítékok segíthetnek az azt követő egyéb eljárás során a bizonyításra, ezzel segítve az elszámoltathatóság biztosítását, továbbá a lehetséges további károk mérséklését. A bizonyítékok kapcsán szükséges annak biztosítása, hogy az alkalmas legyen a bizonyításra, egyértelmű és mások által (ez lehet szakértő) értelmezhető legyen.

(5) A nyilvántartásból törlésre kell kerülnie azon biztonsági eseménnyel kapcsolatos minden adatnak és információnak, amelyek megőrzési ideje lejárt. Az Eseménykezelő Központ felé jelentett biztonsági események adatai és információi 10 évig megőrzendők a bejelentés napjától számítva.

25. A biztonsági szabályok megszegésének következményei

26. § (1) Az informatikai biztonsággal kapcsolatos szabályok megszegése esetén a szabályszegőkkel szemben érvényesítendő jogkövetkezmények tekintetében elsősorban annak súlyosságára tekintettel vagy etikai, vagy munkáltatói fegyelmi jogkörben kell eljárni.

(2) Az információbiztonsággal kapcsolatos szabályok súlyos megszegése vagy annak gyanúja esetén az elektronikus információs rendszer biztonságáért felelős személy javaslatára – érintett foglalkoztatott közvetlen vezetője, illetve az utasítási joggal rendelkező vezető véleményének kikérésével – a

tankerületi igazgató jogosult a megfelelő jogkövetkezmények érvényesítése érdekében fegyelmi eljárást indítani, illetőleg szabálysértési, vagy büntető eljárás megindítását kezdeményezni.

26. Adatok mérése, kiértékelése, mérési pontok meghatározása

27. § (1) Az informatikai biztonság szempontjából kritikus pontokon – lehetőség szerint – mérési és ellenőrzési rendszert kell kiépíteni, továbbá a mérési eredmények tárolását ki kell alakítani és az évente elvégzendő felülvizsgálat elősegítése érdekében a vizsgálatban részt vevő személyek részére hozzáférhetővé kell tenni.

(2) Az ellenőrzési rendszer technikai feltételeinek biztosításáig az IBSZ személyi hatálya alá tartozók tekintetében az elektronikus információs rendszer biztonságáért felelős személy – szükség esetén a NISZ bevonásával – az alábbi táblázat szerinti kontrollpontokon végez eseti ellenőrzést.

IT-tevékenység (inf. biztonsági esemény, inf. bizt. ellenőrzés előkészítéséhez eseti jelleggel)	rendszerbe történő belépési jogosultságok ellenőrzése
	internet-hozzáférések elemzése
	észlelt behatolási kísérletek száma
vírusvédelem	észlelt kártékony kódok száma
	hatástalanított kártékony kódok száma
	nem internetről beérkezett vírustámadások, spyware-ek száma, illetve a megtett intézkedések (tiltás, karantén, törlés),
mentési rendszer	mentési logok, a tesztvisszatöltések eredményei
rendelkezésre állás (hálózat, IT)	rendszerek kieséseinek száma, időtartama, ezek oka, javítási költsége (eseti jelleggel) kliens elhelyezési információk (Eszközök darabszáma, valamint típusa, az egyes Felhasználókhoz rendelten)
	tárolóegységek kapacitásainak kihasználtságára vonatkozó információk
eszközinformációk	tárolóegységek kapacitásainak kihasználtságára vonatkozó információk IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei
kapacitásinformációk	tárolóegységek kapacitásainak kihasználtságára vonatkozó információk IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések
ellenőrzések eredményei	IT-biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák IT biztonsági oktatásban részt vett személyek száma, a beszámoltatás eredményei
oktatás helyzete	az IT-rendszer szintjére vonatkozó megállapítások, javaslatok IT-biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák
IT-biztonsággal kapcsolatos fegyelemsértések	az IT-rendszer szintjére vonatkozó megállapítások, javaslatok
	javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági szint emelésére

az IT-biztonsági rendszer összesített értékelése	
javaslatok	

27. Azonosítás, hitelesítés és feljogosítás az informatikai rendszer használatára

28. § (1) A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.

(2) Az informatikai rendszer használata során a felhasználók és tevékenységeik egyértelmű azonosítását folyamatosan biztosítani kell.

(3) Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez minimálisan egyedi jelszót kell rendelni. További azonosítási lehetőségek is elfogadottak, amelyek az elektronikus információs rendszer biztonságáért felelős személy engedélyével vezethetők be.

(4) A felhasználók azonosítójának a felhasználói nevet tartalmaznia kell. Kivételt képeznek az operációs rendszerek különleges, előre rögzített azonosítói és a különleges informatikai feladatkört ellátók által használt speciális és teszt, vagy szerviz felhasználói nevek. A felhasználói névben törekedni kell a családi és utónév használatára, névazonosság esetén harmadik név vagy emelkedő számozás szolgáljon a felhasználói nevek megkülönböztetésére.

(5) A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell:

a) a felhasználói jelszavak legalább 10 karakter hosszúságúak legyenek,

b) a jelszavak tartalmazzanak legalább egy kis-, és egy nagybetűt, valamint egy számot,

c) a jelszavak nem lehetnek személynevek, szótárban megtalálható szavak, felhasználói azonosítók, nem tartalmazhatnak könnyen kitalálható, ismétlődő karaktersorozatot,

d) nem utalhat a felhasználó személyére,

e) a jelszavakat legalább 90 naponta cserélni kell,

f) nem lehet jelszó az utolsóként használt 12 jelszó egyike sem,

g) maximum 5 téves próbálkozás után a fiókot, munkaállomást zárolni kell 15 perc időtartamra,

h) beírásakor az elektronikus információs rendszereknek fedett visszacsatolást kell biztosítani a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

(6) A jelszó megváltoztatása kötelező:

a) a felhasználói azonosító informatikai rendszerbe történt felvételét követő első bejelentkezéskor,

b) az informatikai üzemeltető szervezeti egység munkatársa általi újbóli jelszóbeállítást, felülírást követően,

c) ha a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett,

d) az érvényességi idő lejártakor.

(7) A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni.

(8) Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

(9) Az informatikáért felelős szervezeti egység ellenőrzi, és vezetője felel azért, hogy a felhasználók kizárólag a vezetőjük által igényelt és megjelölt informatikai jogosultsággal rendelkezzenek. Szükség

esetén gondoskodnia kell a jogosultság törléséről.

(10) A felhasználót, annak vezetőjét a felhasználó élesített jogosultságairól, illetve azok részleges vagy teljes megszűnéséről e-mailben tájékoztatni kell. A tájékoztatási kötelezettség a jogosultság technikai beállítóját terheli.

(11) A (4) bekezdésben meghatározott, úgynevezett privilegizált jogosultságok tekintetében biztosítani szükséges a többtényezős azonosítást, a hálózaton keresztüli hozzáférés biztosításához.

(12) Csoport azonosítók tekintetében a részletszabályokat az elektronikus információs rendszer biztonságáért felelős személy alakíthatja ki, az adott csoport (szervezeti egység) vezetőjével történő egyetértésben, aki a folyamat- vagy az adatgazda. Csoport azonosítók alkalmazása során különös figyelemmel kell lenni a távozó kollégák-, vagy változó munkakörben, álláshelyen ellátandó feladat miatti jogosultság megszűnés miatt a belépést biztosító jelszavak megváltoztatására. A csoport azonosítókkal elkövetett bármely cselekményért az adatgazda a felelős.

(13) Ha valamely hozzáférés biztosítása érdekében hitelesítő eszköz szükséges a kockázatokra tekintettel, akkor az azt kiadó szervezeti egységnek nyilvántartást kell vezetni a kiadott eszközökről egyértelműen azonosítva az átvevő személyt. A hitelesítő eszköz kiadásakor az eszközt átvevő egyén jogosultságát ellenőrizni kell. Az adminisztrációt a 20. § (5) bekezdése szerint kell dokumentálni, mely adminisztráció során a felhasználhatósági feltételeket és időtartamot szükséges feltűntetni.

(14) A hitelesítésre szolgáló eszközök más funkcióval és adattartalommal kiadásukkor nem rendelkezhetnek, mint ami a megvalósítandó cél eléréséhez szükséges. A felhasználói jogosultságok szabályai a hitelesítő eszközök tekintetében a 17. §-ban kerültek meghatározásra. A hitelesítésre szolgáló eszközt annak kompromittálódása, vagy elvesztése esetén azonnal jelezni kell az elektronikus információs rendszer biztonságáért felelős személynek, aki megteszi a szükséges intézkedéseket. Kompromittálódott, vagy elvesztett hitelesítő eszköz használatának a lehetőségét azonnali hatállyal tiltani kell. A hitelesítő eszközök visszaszolgáltatásakor az azon tárolt adatokat törölni szükséges a következő kiadás előtt. Az eszközök visszavétele a 14. §-ban megfogalmazottak szerint történik.

(15) A hitelesítésre szolgáló eszközöket titkosítani kell, amennyiben azok elhagyhatják a Tankerületi Központ irodahelyiségeit fizikailag. A titkosítás módját a mindenkori információbiztonsági trendeknek és megoldásoknak a figyelembevétele mellett az elektronikus információs rendszerek biztonságáért felelős személy határozza meg.

(16) A Tankerületi Központ által használt elektronikus információs rendszer csak a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos nyilvántartásában szereplő hitelesítésszolgáltatók által kibocsátott tanúsítványokat fogadhatja el az érintett szervezeten kívüli felhasználók hitelesítéséhez. Ezen előírást a mindenkori rendszerüzemeltetőnek kell biztosítania.

28. Szoftverek telepítése, internethasználat

29. § (1) A munkaállomás csak a felhasználó hivatali feladatainak ellátása miatt kapcsolható össze az internettel. Hálózathoz csatlakozó munkaállomásokról csak központilag biztosított vírus- és kártékony kód elleni védelemmel, szűrési és forgalom ellenőrzési eszközzel ellátott rendszeren keresztül érhető el az internet.

(2) A hálózathoz csatlakozó munkaállomásra csak a munkavégzéshez szükséges adatállományok, programok tölthetők le, illetve telepíthetők.

(3) A hálózathoz csatlakozó munkaállomásra nem telepíthető, nem másolható – ideiglenesen sem –, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,

b) a hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

(4) Az internet felhasználása csak a Tankerületi Központ ügymenete érdekének megfelelően kialakított és betartott szabályok alapján történhet.

(5) Az internet-szolgáltatás minőségének szinten tartása és a Tankerületi Központ érdekeinek biztosítása céljából a NISZ – az elektronikus információs rendszer biztonságáért felelős személy javaslatára vagy engedélyével – korlátozásokkal élhet. A korlátozások a következőkre terjedhetnek ki:

a) bizonyos fájl-típusok letöltésének korlátozása,

b) az alapvető etikai normákat sértő oldalak látogatásának tiltása,

c) a látogatható weboldalak körének behatárolása és a maximális fájl-letöltési méret korlátozása.

(6) A tankerületi igazgató – amennyiben ezt indokoltnak tartja – a szervezeti egység, Tankerületi Központ munkatársainak, egyes felhasználó(k) internet-hozzáférésének letiltását kezdeményezheti írásban az elektronikus információs rendszer biztonságáért felelős személynél. A felhasználók csak az elektronikus információs rendszer biztonságáért felelős személy által ismert és a NISZ által biztosított internet kijáratokon keresztül csatlakozhatnak az internethez. Bármely egyéb módon történő internetelérés létesítése az azt kialakító felhasználó felelősségre vonását eredményezi.

(7) Felhasználók internethasználatára vonatkozó általános szabályok:

a) csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók,

b) tilos a jó ízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak felkeresése, bármely tartalommal kapcsolatos magánvélemény kinyilvánítása (pl. privát blog és chat),

c) a felhasználók nem tölthetnek fel egyénileg – a felelős jóváhagyása nélkül – a Tankerületi Központtal kapcsolatos adatot az internetre,

d) az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, alkalmazások, programok nem,

e) a látogatott oldal nem szokványos működése (pl.: folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő kényszerítés, ismeretlen program futásának észlelése stb.) esetén a közvetlen technikai támogató segítségét kell kérni.

29. Elektronikus levelezőrendszer használata

30. § (1) A Tankerületi Központ feladatainak végrehajtásához alkalmazott elektronikus levelezésben kizárólag a @kk.gov.hu végződésű, hivatali levelezési cím használható.

(2) A Tankerületi Központtal kormányzati szolgálati jogviszonyban vagy munkaviszonyban álló személy kaphat levelezési címet, személyes postafiókot. Külsős munkavállaló esetén a foglalkoztató szervezeti egység vezetője egyedi elbírálás alapján postafiók beállítást igényelhet. Hivatalos levelezés ingyenes, vagy nyilvános alapú szolgáltató rendszerében nem végezhető. (G-Mail, Freemail, Yahoo, stb.) Ilyen célra kizárólag a NISZ által biztosított, vagy intézmények saját domain levelező rendszerében létrehozott postafiók címek alkalmazhatók.

(3) A levelezőrendszerek használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell.

(4) A hivatali levelezőrendszeren kizárólag hivatali célú üzenetek továbbíthatók. Magáncélú üzenetet nem nevesített felhasználóknak (pl. csoport, mindenki) küldeni tilos.

(5) A 27-28. §-ban foglalt előírások betartását a Tankerületi Központ szervezeti egységének vezetője köteles ellenőrizni.

(6) Az elektronikus levelezés biztonságának, működőképességének, stabilitásának és rendelkezésre állásának biztosítása a NISZ feladata.

(7) Csoportos e-mail cím létrehozását a Klebelsberg Központ Informatikai Főosztálya útján papír alapú vagy elektronikus levélben lehet igényelni az igénylő munkatárs szervezeti egysége vezetőjének jóváhagyásával a NISZ kapcsolattartótól.

(8) Az igénylésben meg kell jelölni legalább egy felelős munkatársat (a továbbiakban: felelős), aki a létrehozás után a csoportos e-mail cím karbantartásához szükséges információkat igény esetén biztosítja az üzemeltetés részére, illetve kezdeményezi a csoportos e-mail cím alá történő felhasználói e-mail cím beállítását.

(9) A csoportos e-mail címeket a felelősök félévente felülvizsgálják és szükség esetén gondoskodnak azok módosításáról vagy megszüntetéséről. A csoportos e-mail címek módosításáról vagy megszüntetéséről a felelősök e-mail útján tájékoztatják a tagokat.

(10) Az elektronikus információs rendszer biztonságáért felelős személy évente felülvizsgálja a csoportos e-mail címek fenntartásának indokoltságát.

(11) A Tankerületi Központban és oktatási intézményeiben alkalmazott Microsoft Teams rendszer csoportos e-mail címeinek létrehozását, azokba munkatársak címeinek felvételét, módosítását, törlését, illetve jogosultság változását elektronikus levélben lehet igényelni a rendszergazdától az adott szervezeti egység vezetőjének jóváhagyásával.

30. Informatikai fejlesztések és beszerzések általános követelményei

31. § (1) Az informatikai fejlesztések és beszerzések során betartandó informatikai biztonsági követelmények teljesüléséért a fejlesztést, beszerzést lebonyolító szervezeti egység vezetője felel.

(2) A Tankerületi Központ informatikai rendszereit, az informatikai rendszerekhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközöket és adathordozókat, valamint az előzőekben felsoroltakkal kapcsolatos informatikai és biztonsági tevékenységet érintő fejlesztések és beszerzések megkezdése előtt, az informatikáért felelős szervezeti egységet és az elektronikus információs rendszer biztonságáért felelős személyt a fejlesztés és a beszerzés célját, tartalmát rögzítő, valamint a funkcionális és biztonsági megfelelőség biztosítására tervezett intézkedéseket tartalmazó dokumentum megküldésével tájékoztatni kell.

(3) Szakterületet érintő informatikai rendszer fejlesztése során a fejlesztés folyamatába az adott szakterületet érintő szervezeti egység vezetőjét kötelező bevonni.

(4) Fejlesztési, továbbá tesztelési tevékenység csak ilyen rendeltetésű informatikai rendszerekben végezhető. E rendelkezés alól az elektronikus információs rendszer biztonságáért felelős személy javaslata alapján a tankerületi igazgató indokolt esetben felmentést adhat.

(5) A tesztelési tevékenységek meg kell, hogy előzzék az átadás-átvételeket. A tesztek végrehajtását tesztelési tervek alapján tesztjegyzőkönyv szerint kell lezárni, és ennek eredményét az adott szakterület szervezeti egységének vezetője, az informatikáért felelős szervezeti egység és az elektronikus információs rendszer biztonságáért felelős személy hagyja jóvá.

(6) A fejlesztés és beszerzés során – beleértve a közbeszerzési eljárásokat is – folyamatosan biztosítani kell, hogy az elektronikus információs rendszer biztonságáért felelős személy a beszerezni tervezett eszközök és a megrendelt tevékenység informatikai biztonsági aspektusait ellenőrizhesse.

(7) A fejlesztésekre és beszerzésekre vonatkozó szerződéseket aláírás előtt az elektronikus információs rendszer biztonságáért felelős személy részére informatikai biztonsági szempontból történő véleményezésre meg kell küldeni.

(8) A központi, valamint az európai uniós forrásból megvalósuló fejlesztési projektek informatikai biztonsági követelményeinek teljesítése érdekében a projekt vezetője a projekt tervezési szakaszában, szolgálati úton, a Gazdálkodási, Üzemeltetési és Pályázati Főosztály részére véleményezésre megküldi a vonatkozó biztonsági osztályba sorolást és biztonsági szint meghatározást, továbbá mindazon dokumentációkat, amelyek alapján a biztonsági, és termékminősítési követelmények megvalósulása ellenőrizhető a projekt teljes életciklusára nézve, ideértve az átvétel vagy teljesülés után az elektronikus információs rendszer használata során érvényesítendő elvárásokat is.

(9) A központi, valamint az európai uniós forrásból megvalósuló fejlesztési projektek informatikai biztonsági követelményeinek teljesítése érdekében a projekt mérföldköveinek figyelembevételével, az adott projekt szakasz zárását megelőző legkevesebb harminc nappal a projekt vezetője a Gazdálkodási, Üzemeltetési és Pályázati Főosztály rendelkezésére bocsátja a kapcsolódó elektronikus információbiztonsági dokumentációt, hogy annak észrevételei vagy kifogásai a projekt terveken vagy a projekt tárgyán átvezethető és alkalmazható legyen.

(10) Új szoftver rendszerbe állítását, új informatikai rendszerek, rendszerelemek üzembe állítását a Klebelsberg Központ Informatikai Főosztálya közreműködésével az informatikáért felelős szervezeti egység javaslata alapján, az elektronikus információs rendszer biztonságáért felelős személy felügyelete mellett a NISZ végzi.

(11) Egyes informatikai rendszerek, alkalmazások, modulok vonatkozásában a fejlesztés és az üzemeltetés tekintetében az IBSZ-szel kapcsolatos rendelkezések külön szabályokat állapíthatnak meg.

(12) Az informatikai rendszerek fejlesztésének első lépéseként a szakmai oldal elvárásai alapján el kell készíteni a rendszerspecifikációs dokumentumot, amelynek elkészítése során a jogszabályi és az informatikai biztonsági elvárásoknak történő megfelelést is figyelembe kell venni.

(13) Az informatikai biztonság megőrzése érdekében ki kell dolgozni a rendszerspecifikációra vonatkozó biztonsági követelményrendszert. A követelményrendszer kidolgozásának végrehajtása az elektronikus információs rendszer biztonságáért felelős személy javaslatai alapján a kapcsolódó fejlesztési projekt vezetőjének feladata. A követelményrendszert az alaprendszerbe való illesztéséből adódóan – a rendszerspecifikációs dokumentum kialakítása során – a Klebelsberg Központ Informatikai Főosztálya útján egyeztetni szükséges a NISZ-szel.

(14) A követelményrendszer elkészítése során figyelembe kell venni:

a) a fejlesztendő rendszer bemenő adatait, annak adatvédelmi és adatbiztonsági besorolási szintjeit,

b) a rendszer elvárt rendelkezésre állási idejét,

c) a rendszer azon elemeit, ahol a szerepkör alapú hozzáférési jogosultságok kialakítása szükséges,

d) a rendszer gyenge, betörésre alkalmat adó pontjait, ismert sérülékenységeit,

e) a mentési rendbe való illesztését,

f) a fejlesztői, teszt, oktató és éles rendszer elkülönítését,

g) az adminisztrátori és felhasználói dokumentációt,

h) biztonsági funkciókat és azok hatékony alkalmazási módját, valamint a biztonságos használat módszereit.

(15) Az alkalmazásfejlesztés teljes időintervalluma alatt kiemelt szerepet kell kapnia az információbiztonságot erősítő intézkedéseknek. Mind a szakmai, mind az informatikai követelmények összeállítása során, mind dokumentálás, a teszt és az éles időszak alatt törekedni kell erre. Azon alkalmazások esetében, amelyeket külső fél üzemeltet, a fejlesztés tervezése során egyeztetni szükséges a külső féllel.

(16) A vásárolt és fejlesztett programok esetében figyelembe kell venni a szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő vagy egyéb személyhez fűződő jogra vonatkozó hatályos szabályozást. A tulajdonjogot a licencszerződések szabályozzák.

(17) Biztonsági előírások a vásárolt és fejlesztett programokkal kapcsolatban:

a) a Tankerületi Központ által vásárolt vagy számára kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik személy részére – ha a harmadik fél nem Tankerületi Központ, vagy a licencszerződés ezt kifejezetten nem teszi lehetővé – tilos,

b) a felhasználók/programozók – az elektronikus információs rendszer biztonságáért felelős

személy jóváhagyása nélkül – nem készíthetnek olyan alkalmazásokat, programokat, amelyek a Tankerületi Központ adatbázisait igénybe veszik, ahhoz kapcsolódnak, vagy az IBSZ tárgyi hatálya alatt álló eszközön futnak,

c) a Tankerületi Központ adatbázisából csak úgy hozható létre önálló adatbázis, ha azt az adatgazda írásban jóváhagyta, és az elektronikus információs rendszer biztonságáért felelős személy azzal egyetértett.

(18) Informatikai rendszerek bevezetése előtt gondoskodni kell a Tankerületi Központ belső felhasználóinak olyan ismeretanyagot átadó oktatásáról, amely birtokában a rendszer átvételét követően képesek lesznek további felhasználók oktatására (train to train oktatás). Az oktatást követően az elsajátított anyagot a Tankerületi Központ belső felhasználóktól számon kell kérni.

31. Üzemeltetés-biztonság, valamint a karbantartás általános követelményei

32. § (1) Az informatikai rendszerek rendeltetésszerű működéséért, folyamatos rendelkezésre állásáért a NISZ a Klebelsberg Központtal kötött egyedi szolgáltatási szerződésében foglaltak szerint felel.

(2) Az informatikai rendszerek ütemezett és eseti karbantartását a NISZ munkatársai az egyedi szolgáltatási szerződésében foglaltak szerint végzik.

(3) A szolgáltatási szerződésben foglaltak szerinti rendszeres karbantartási feladatokat ellátó, a NISZ által előre meghatározott szakértő munkatársak részére a Tankerületi Központ állandó bejutási és munkavégzési engedélyt biztosít.

(4) A Tankerületi Központ a telephelyén történő karbantartási munkák elvégzése során állandó személyes kíséretet és felügyeletet biztosít a NISZ szakemberei felett mind az ütemezett, mind az eseti karbantartási munkák elvégzésének teljes időtartama alatt.

(5) A karbantartást elvégző szakemberek jegyzőkönyvet vesznek fel az általuk elvégzett munkáról, amelyet a helyszínen átadnak a Tankerületi Központ erre kijelölt munkatársának, aki haladéktalanul ellenőrzi, hogy az informatikai rendszer az előírásoknak és a rendeltetésének megfelelően működik, valamint biztonsági ellenőrzést végez az informatikai rendszeren.

(6) A Tankerületi Központ erre kijelölt munkatársa az (5) bekezdésben foglaltak teljesítése során szerzett információkat rögzíti és a dokumentumokat csatolja a karbantartási nyilvántartáshoz.

(7) A (2)-(6) bekezdéseiben foglaltak kötelezően alkalmazandóak valamennyi nem NISZ munkatárs külső szakember által a Tankerületi Központ telephelyén végzett karbantartási vagy bármely más munkavégzése során.

(8) A távoli segítségnyújtás (távsegítség) során a kliensoldali programot, amely bármilyen módon lehetővé teszi a felhasználó képernyőjén lévő információk távoli elérését vagy input eszközeinek távvezérlését, csak a felhasználó indíthatja el, azt automatikusan induló programként telepíteni tilos. A távsegítség bevezetése és alkalmazása előtt a szolgáltatás tartalmáról, továbbá a távsegítség során elvégzett beavatkozásról a felhasználókat tájékoztatni kell.

(9) Az informatikai rendszerekben kezelt és tárolt adatok rendelkezésre állását rendszeres és indokolt esetben soron kívüli mentéssel kell biztosítani.

(10) Az informatikai rendszerekben kezelt adatállományokat, amennyiben azok elérése a felhasználók számára napi munkavégzésük során nem szükséges, azonban őrzésük indokolt, archiválni kell.

(11) A mentésre, illetve az archiválásra vonatkozó szabályokat a rendszerelemek üzemeltetési kézikönyveinek mentésre és archiválásra vonatkozó leírásában vagy a Tankerületi Központ Archiválási Szabályzatában kell szabályozni. Az elektronikus információs rendszer üzemeltetője gondoskodik a biztonsági mentések megfelelő rendelkezésre állásáról, a mentések bizalmasságáról és sértetlenségéről, szerződésben meghatározottak szerint.

(12) Az informatikai rendszerek adattárolást megvalósító elemei, a hozzájuk csatlakoztatható, adattárolást is megvalósító informatikai, irodatechnikai, multimédiás eszközök, továbbá az

adathordozók külső felhasználó általi karbantartásra, javításra, cserére csak a tárolt adatállomány biztonságos törlését követően adhatók át. A törlés megvalósításáért a karbantartás, javítás, csere esetén eljáró szervezeti egység vezetője felel.

32. Vírusvédelem

33. § (1) A vírusvédelmi eljárásokat, a vírusvédelemre vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy

a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,

b) támogassa a valós riasztások kiszűrését,

c) alkalmas legyen a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,

d) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,

e) biztosítsa az új fenyegetések időben történő felismerését.

(2) A vírusvédelemmel kapcsolatos üzemeltetési, üzemeltetés-felügyeleti, informatikai biztonsági felügyeleti feladatokat a NISZ látja el.

(3) A hálózat esetében a vírusvédelem központilag biztosított.

(4) Az elektronikus információs rendszer biztonságáért felelős személy az általános vírusbiztonsági helyzet értékeléseként az előző naptári év vírusriasztásainak statisztikai jellemzőiről és a megtett intézkedésekről a Klebelsberg Központ Informatikai Főosztálya útján tájékoztatást kérhet a NISZ-től.

(5) A vírusvédelmi előírások súlyos, szándékos vagy sorozatos megsértése információbiztonsági eseménynek minősül.

VII. FEJEZET

ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

33. Biztonsági szint meghatározás és biztonsági osztályba sorolás

34. § (1) A Tankerületi Központnak, mint központi költségvetési szervnek, a biztonsági osztályba sorolást a bizalmasság, a sértetlenség, a rendelkezésre állás kockázata alapján minden egyes elektronikus információs rendszer esetében önbesorolás útján 1-től 5-ig terjedő számozással ellátott skálán kell elvégezni azzal, hogy a számozás emelkedésével a védelmi előírások fokozatosan szigorodnak az Ibtv. 7. § (2) bekezdésének megfelelően.

(2) A Tankerületi Központ biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolásúnak, de legalább 2-es biztonsági szintűnek kell lenni az Ibtv. 9. § (2) bekezdésnek megfelelően

(3) Amennyiben a rendszer és/vagy az eszköz közvetlenül nem kapcsolódik adatokhoz, illetve csak technológiai használatú adatokhoz kapcsolódik, a Tankerületi Központ feladatteljesítésben betöltött szerepe alapján kell osztályba sorolni.

(4) A rendszerek osztályba sorolását az informatikai rendszer szakmai felügyeletét ellátó szervezeti egységek vezetőinek kötelező együttműködésével az elektronikus információs rendszer biztonságáért felelős személy végzi.

(5) A biztonsági besorolást tartalmazó táblázat (a szervezet és a szervezeti egységek biztonsági szintbe-, és az elektronikus információs rendszerek biztonsági osztályba sorolásai) az IBSZ 3. mellékletét képezi, amelyet az elektronikus információs rendszer biztonságáért felelős személy folyamatosan aktualizál.

(6) A biztonsági osztályba sorolást szükség szerint, de legalább három évenként felül kell vizsgálni. Az informatikai rendszer vagy a benne kezelt adat biztonságát érintő változás esetén a biztonsági osztályba sorolást soron kívül meg kell ismételni.

(7) Az informatikai rendszer szakmai felügyeletét ellátó szervezet vezetője az informatikai rendszer alkalmazását megelőzően köteles tájékoztatni az elektronikus információs rendszer biztonságáért felelős személyt.

34. Az információvagyon felmérése és osztályozása

35. § (1) Annak érdekében, hogy az adatok, információk (információs vagyon) bizalmasságának megfelelően differenciált védelmi intézkedések kerüljenek kialakításra, az informatikai rendszerekben kezelt adatokat, információkat megfelelő információvédelmi kategóriák szerint kell csoportosítani (biztonsági osztályba sorolás).

(2) Az osztályozás alapját a bizalmasság, a sértetlenség, és a rendelkezésre állás sérüléséből vagy elvesztéséből keletkező, a Tankerületi Központ számára kimutatható lehetséges hátrány nagysága képezi.

(3) A besorolást az adatgazdák végzik, az ő feladatuk és felelősségük, hogy felmérjék a kezelt adatvagyon helytelen osztályozásából eredő károkat.

(4) A biztonsági osztályba sorolást Tankerületi Központ valamennyi szervezeti egysége, valamint a Tankerületi Központ által tárolt vagy feldolgozott minden adatcsoport tekintetében el kell végezni.

(5) Az olyan informatikai rendszerek vagy adatbázisok esetén, amelyek több adatcsoportot együtt tárolnak vagy dolgoznak fel, a rendszerben előforduló legmagasabb biztonsági osztály követelményeit kell érvényesíteni.

(6) Amennyiben valamely adat több jellemzőnek is eleget tesz, akkor az előfordulható legmagasabb kár szerint kell osztályba sorolni. Amennyiben egy informatikai rendszeren belül több különböző védelmi osztályba tartozó adat tartozik, akkor a rendszer védelmét az előforduló legmagasabb védelmi osztály szerint kell kialakítani és fenntartani.

(7) Az informatikai rendszerek különböző környezetei (pl. éles-, teszt-, oktatórendszer) más-más biztonsági osztályba sorolhatók.

(8) Amennyiben a kezelt adatok köre bővül, az osztályozást az új adatcsoportokra is végre kell hajtani.

(9) Az egyes rendszerek, rendszerelemek, adatbázisok előírt rendelkezésre állását az SLA tartalmazza.

(10) Az osztályba sorolás alapja a kárértékek meghatározása, melynek során a Közigazgatási Informatikai Bizottság 25. számú ajánlásában meghatározott szinteket kell figyelembe venni. E szerint a következő osztályok használhatók:

Elhanyagolható	
jelentéktelen kár	közvetlen anyagi kár: 0-10.000,- Ft, közvetett anyagi kár 1 embernappal állítható helyre, nincs bizalomvesztés, a probléma a szervezeti egységen belül marad, nyilvános adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Alap	
csekély kár	közvetlen anyagi kár: 10.001-100.000,- Ft, közvetett anyagi kár 1 emberhónappal állítható helyre, társadalmi-politikai hatás: kínos helyzet a szervezeten belül, személyes adatok bizalmassága vagy hitelessége sérül, csekély jelentőségű hivatali információ, adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Fokozott	
közepes kár	közvetlen anyagi kár: 100.001-1.000.000,- Ft,

	közvetett anyagi kár 1 emberévvel állítható helyre, társadalmi-politikai hatás: bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel, személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, közepes jelentőségű hivatali információ vagy egyéb jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Kiemelt	
nagy kár	közvetlen anyagi kár: 1.000.001-10.000.000,- Ft, közvetett anyagi kár 1-10 emberévvel állítható helyre, társadalmi-politikai hatás: bizalomvesztés a szervezet felső vezetésében, középvezetésen belül személyi konzekvenciák, különleges személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül, nagy jelentőségű hivatali információ bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Rendkívüli	
kiemelkedően nagy kár	közvetlen anyagi kár: 10.000.001-100.000.000,- Ft, közvetett anyagi kár 10-100 emberévvel állítható helyre, társadalmi-politikai hatás: súlyos bizalomvesztés, a szervezet felső vezetésén belül személyi konzekvenciák, nagy tömegű különleges személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, kiemelt jelentőségű hivatali információ bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
4+Rendkívüli+	
különösen nagy kár	A „kiemelkedően nagy kár” értéket meghaladó, vagy visszafordíthatatlanul súlyos kár, amely közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását, az államháztartás működését, az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeit, külügyi és nemzetközi kapcsolatait, a szövetséges tagállamokkal közös biztonsági érdekeit.

35. Elektronikus információs rendszerek nyilvántartása és kezelése

36. § (1) A Tankerületi Központ informatikai rendszerei nyilvántartásának az alábbiakra kell kiterjednie:

a) az adat vagy adatcsoport (rendszer) megnevezése, alapfeladata,

b) az érintett rendszerhez tartozó licenc szám (amennyiben az a Tankerületi Központ kezelésében van),

c) az adatosztályozási szint bizalmasság, sértetlenség és rendelkezésre állás szerint,

d) a rendszer felett felügyeletet gyakorló személy személyazonosító és elérhetőségi adatai,

e) a rendszert szállító, fejlesztő és karbantartó szervezetek azonosító és elérhetőségi adatai, valamint ezen szervezetek rendszer tekintetében illetékes kapcsolattartó személyeinek

személyazonosító és elérhetőségi adatai.

(2) A nyilvántartás vezetéséért az elektronikus információs rendszer biztonságáért felelős személy, míg a nyilvántartáshoz szükséges információk szolgáltatásáért az adatgazdák felelősek.

(3) A Tankerületi Központ informatikai rendszereinek hatókörébe tartozó szoftver és hardver elemekről leltárt kell vezetni, amelynek az alábbiakra kell kiterjednie:

a) informatikai eszközt használatba vevő személy neve,

b) eszközök megnevezése, darabszáma,

c) leltári szám, gyári szám,

d) tárolási hely megnevezése, címe

(4) Az elektronikus információs rendszerek hardver és szoftver elemeiről szóló nyilvántartás vezetéséért az informatikáért felelős szervezeti egység felel. A nyilvántartást szükség szerint rendszeres időközönként, de legalább évente aktualizálni kell.

VIII. FEJEZET

INFORMÁCIÓBIZTONSÁGI ELJÁRÁSOK

36. Általános irányelvek

37. § (1) A Tankerületi Központ és az intézmények épületeiben üzemeltetett eszközök logikai védelmét a Klebelsberg Központ által kötött egyedi szolgáltatási szerződésben foglaltak alapján a NISZ látja el.

(2) Az azonosítók képzését, azok nyilvántartását, a jogosultságok kezelését az SLA alapján a NISZ végzi.

(3) Az egyedi felhasználói azonosítót a hozzáférések (jogosultságok) szabályozására, az adatvédelemre és a hitelesítés támogatására kell használni.

(4) A felhasználó azonosítónak meg kell felelnie az egyediség kritériumának. Kivételt képez a szervezeti egységhez kötött ún. csoport e-mailek használata, amelyekhez az adott szervezeti egység vezetőjének írásos felhatalmazásában megnevezett felhasználók férhetnek hozzá.

(5) Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakörben, álláshelyen ellátandó feladat ellátásához szükséges adat- és funkcióelérést biztosíthatják.

(6) A hozzáférési jogosultságok kezelését, a jogosultságigénylés folyamatának részleteit a rendszerelem üzemeltetési kézikönyvében kell meghatározni, ha jelen szabályoktól eltérő vagy ezekhez képest kiegészítésre szorul.

(7) A hozzáférési jogosultságok beállítását a rendszergazda végzi.

(8) A felhasználók a hozzáférésüket megalapozó jogviszonyuk létrejöttét követően (a lehető legrövidebb időn belül) megkapják felhasználói azonosítójukat.

(9) A kiosztott felhasználói azonosítót haladéktalanul használatba kell venni. Ennek első lépéseként az induló (alapértelmezett) jelszót meg kell változtatni.

(10) Amennyiben a felhasználó jogviszonya előreláthatólag három hónapot meghaladóan szünetel, vagy a felhasználó a munkavégzésben előreláthatóan ennyi ideig nem vesz részt, a hozzáférést megalapozó jogviszonyából eredő feladatát tartósan nem látja el, a felhasználói azonosítóját fel kell függeszteni (inaktiválni kell) a munkába állás, az adott tevékenység folytatása napjáig. Az inaktiválást a közvetlen vezető, illetve a szerződéskötést kezdeményező szervezeti egység vezetője kéri – a Klebelsberg Központ személyügyekért felelős szervezeti egysége útján – a NISZ kapcsolattartótól. A felhasználói azonosító újraaktiválási igényének felmerülésekor a hozzáférés helyreállítását szintén a közvetlen vezető, illetve a szerződéskötést kezdeményező szervezeti egység vezetője kérheti.

(11) A felhasználók szervezeten belüli áthelyezése kapcsán felmerülő jogosultsági változásokat a felhasználó közvetlen vezetője, illetve a szerződéskötést kezdeményező szervezeti egység vezetője kéri – a Tankerületi Központ gazdasági vezetője útján – a NISZ kapcsolattartótól.

(12) Külső felhasználó csak meghatározott időre és korlátozott lehetőségeket biztosító (pl. csak írási joggal, vagy csak bizonyos területre érvényes) felhasználói azonosítót kaphat. Külső felhasználó azonosítójának létrehozását, számára jogosultságok megadását a szerződéskötést kezdeményező szervezeti egység vezetője a Klebelsberg Központ személyügyekért felelős szervezeti egységének közreműködésével kezdeményezi a NISZ kapcsolattartónál.

37. Munkaállomások hozzáférésére vonatkozó minimális előírások

38. § (1) A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.

(2) A munkaállomás beállításait adminisztrátori jelszóval kell védeni módosítás ellen.

(3) A képernyőt automatikus védelemmel kell ellátni (munkaállomás zárolás).

(4) Adatbázisokat és programokat – amennyiben megoldható – hardveres azonosítást biztosító eszközzel kell védeni.

38. Szoftvereszközök használatának szabályozása

39. § (1) Az informatikai biztonság teljes körű megvalósításához hozzájárul a jogtiszta szoftverek és a szoftvereszközök jogszerű használata, valamint a szoftverek biztonságos kezelése.

(2) A Tankerületi Központ által használt szoftvereket az elektronikus információs rendszer biztonságáért felelős személy ellenőrzi.

(3) A rendszeres szoftvervizsgálat során ellenőrizni kell:

a) a használatban lévő szoftverek rendelkeznek-e licence-szel (ide nem értve az engedélyezett freeware, shareware szoftvereket),

b) a megvásárolt licencek száma arányos-e a használt szoftverek mennyiségével,

c) a használt szoftverek verziószámát,

d) a ténylegesen használt szoftverek megegyeznek-e az engedélyezett szoftverek listájával.

(4) A szoftvereszközök telepítésére és használatára vonatkozó általános szabályok:

a) a Tankerületi Központ munkaállomásaira csak eredményesen tesztelt szoftverek telepíthetők,

b) tilos a munkaállomásokra licence-szel nem rendelkező vagy a kereskedelmi forgalomban beszerezhető nem engedélyezett vagy nem a Tankerületi Központ által fejlesztett szoftvert telepíteni,

c) a Tankerületi Központ által vásárolt és kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik fél részére tilos, kivéve, ha a licencszerződés ezt külön szabályozza és lehetővé teszi,

d) a felhasználók csak a NISZ által telepített szoftvereket, ideértve az engedélyezett freeware és shareware szoftvereket is (4. melléklet) használhatják,

e) a felhasználók rendelkezésére bocsátott hardver és szoftver eszközök ellenőrzését az elektronikus információs rendszer biztonságáért felelős személy bejelentés nélkül bármikor kezdeményezheti.

39. Tűzfalakkal kapcsolatos szabályozások, betörésvédelem, betörés detektálás

40. § A tűzfalakkal kapcsolatos szabályozások és biztonsági beállítások megtétele egyedi szolgáltatási szerződés alapján a NISZ feladata.

40. Távoli hozzáférés szabályozása

41. § (1) A távoli hozzáférések engedélyezésével, korlátozásával és felügyelet alatt tartásával a Kebelsberg Központ, a Tankerületi Központ és a NISZ közös célja a távoli hozzáférés jellegéből következő információbiztonsági és informatikai szolgáltatás biztonsági kockázatok csökkentése, valamint a távoli hozzáférések és az azok által elérhető funkcionalitások számosságának a lehető legalacsonyabb szinten való tartása. A Tankerületi Központ informatikai rendszerének távoli elérésére csak egyedileg azonosított felhasználók számára , a NISZ által üzemeltetett rendszer esetén csak a NISZ hozzájárulása esetén lehetséges.

(2) A Tankerületi Központ informatikai környezetében jelenleg az alábbi pontokban feltüntetett szolgáltatások sorolhatók távoli elérés alá:

a) WebMail-szolgáltatás – OWA elérésen keresztül,

b) Távsegítség nyújtása (kizárólag NISZ alkalmazottakon keresztül).

41. Mobil IT tevékenység, hordozható informatikai eszközök használata

42. § (1) A mobil eszközök használatával kapcsolatban a következő biztonsági eljárásokat kell alkalmazni:

a) a mobil eszközök átvételéhez átadás-átvételi dokumentumokat kell készíteni,

b) mobiltelefonok, tabletek esetén legalább PIN kód beállítása a feloldáshoz,

c) valamennyi hordozható személyi számítógépet rendszeres szoftver-, adat- és biztonsági ellenőrzéseknek kell alávetni. Rendszeres időközönként (lehetőleg hetente egy alkalommal) a munkahelyi hálózatához kell csatlakoztatni az eszközt az operációs rendszer biztonsági és vírusvédelmi frissítéseinek végrehajtása érdekében. A mobil eszközt szállító felhasználók:

ca) kötelesek azt a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni,

cb) nem hagyhatják őrizetlenül gépjárműben,

cc) repülés vagy vonatút, valamint autóbuszon történő utazás ideje alatt kézipoggyászként kötelesek szállítani.

(2) Azokban az esetekben, amikor az eszközök nem a Tankerületi Központ épületeiben (szálloda, lakás) találhatók, fokozott figyelmet kell szentelni a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása vagy ellopása elleni védelemnek.

(3) Tilos a mobil eszközök:

a) engedély nélküli átruházása vagy adatainak közlése, lementése,

b) megfelelő védelem nélkül nem biztonságos hálózathoz csatlakoztatása,

c) bármilyen indokolatlan veszélynek történő kitétele vagy nem rendeltetésszerű használata.

(4) A Tankerületi Központ adataiból csak azon adatokat szabad mobil eszközön tárolni:

a) amely adatokról központi biztonsági mentés készül,

b) amelyekkel kapcsolatban biztosítani lehet a jogszabályban vagy belső szabályban előírt adatbiztonságot és adatvédelmet.

42. A rendszer dokumentációk védelme

43. § (1) Az informatikai rendszerek, alrendszerek dokumentációjának tartalmaznia kell a rendszerek leírását, azok telepítését, konfigurálását, aktiválását, leállítását és használatát, a fejlesztés, valamint az üzemeltetés során. Az informatikai rendszer, alrendszer dokumentációját csak az informatikai vezető által engedélyezett személyek kezelhetik.

(2) Az illetéktelen hozzáférés megelőzése érdekében

a) gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról,

b) minimálisra kell csökkenteni a rendszerdokumentációkhoz hozzáférők számát,

c) gondoskodni kell a nyilvános hálózaton keresztül elérhető, vagy azon keresztül továbbított dokumentáció védelméről,

d) az informatikai rendszer biztonságával kapcsolatos dokumentációt az informatikai rendszer biztonsági fokozatának megfelelő módon kell kezelni,

e) az informatikai rendszer vagy annak bármely elemének dokumentációját naprakészen kell tartani, melynek során gondoskodni kell az informatikai biztonságot érintő változások, változtatások naplózásáról, valamint

f) az informatikai rendszerekhez kapcsolódó jogosultságok nyilvántartását elkülönítetten kell kezelni.

(3) A szakmai alkalmazások beszerzéssel vagy fejlesztéssel történő kialakításához és üzemeltetéséhez, a rendszer funkcionalitásának és megbízható üzemeltetésének a biztosításához szükséges

a) a rendszerterv,

b) üzemeltetési kézikönyv,

c) a katasztrófa-elhárítási terv,

d) a mentési terv és

e) az üzembehelyezési jegyzőkönyv.

43. Rendszer- és kommunikációvédelmi eljárásrend

44. § (1) A Tankerületi Központ az elektronikus információs rendszerek és a kommunikáció védelmére vonatkozó eljárásrendet az IBSZ-ben, a Tankerületi Központ informatikai rendszereinek felhasználásáról szóló szabályzatában és a NISZ-szel kötött szolgáltatási szerződésben foglaltaknak megfelelően a „Minden tilos, ami nem engedélyezett” elv következetes betartásával és betartatásával az alábbiak szerint állapítja meg.

(2) A túlterhelés, illetve szolgáltatás megtagadás alapú támadás elleni védelem keretében a Tankerületi Központ vagy a Tankerületi Központ által használt elektronikus információs rendszerének üzemeltetője igyekszik a legmagasabb védelmet biztosítani biztonsági intézkedések bevezetésével és a támadástípusok listája alapján korlátozza azok negatív hatását.

(3) A határok védelme érdekében a Tankerületi Központ vagy az általa használt elektronikus információs rendszer tekintetében az üzemeltető:

a) felügyeli és ellenőrzi a külső határain és a rendszer kulcsfontosságú belső határain történő kommunikációt és ennek érdekében tűzfalakat, tartalomszűrőket, meghatározott címek elérésének tiltását és eltérő hozzáférési szintek megállapítását alkalmazza,

b) a nyilvánosan hozzáférhető rendszerelemeket elkülöníti a Tankerületi Központ belső szervezeti hálózatától,

c) csak a Tankerületi Központ és annak szervezeti egységeinek architektúrájával összhangban

elhelyezett határvédelmi eszközökkel felügyelt interfészeken keresztül és kizárólag a szükséges és engedélyezett szolgáltatások igénybevétele érdekében és jóváhagyott tűzfalakon keresztül kapcsolódik bármely külső hálózathoz és külső elektronikus információs rendszerekhez,

d) biztosítja, hogy a Tankerületi Központ hálózatához kizárólag olyan Wi-Fi eszköz csatlakoztatható, amely minimum WPA2 titkosítást alkalmaz.,

e) biztosítja, hogy a Tankerületi Központ belső hálózatához kizárólag olyan eszköz csatlakoztatható, amely a Tankerületi Központ használatában és az üzemeltető felügyelete alatt áll,

f) korlátozza és ellenőrzi a felhasználók hozzáférését bármely engedélyezett információszolgáltatáshoz és elektronikus információs rendszerhez,

g) a Tankerületi Központ internet elérése kapcsán az üzemeltető minden külső internetes elérést naplóz annak érdekében, hogy a Tankerületi Központ elektronikus információs rendszereit veszélyezetető szabálytalan kommunikációt megakadályozza, felderítse és azokból a rendszer- és kommunikációvédelem jövőbeni erősítésre vonatkozó következtetéseket vonjon le,

h) naprakészen tartja az elektronikus információs rendszereinek biztonsági frissítéseit,

i) biztosítja, hogy a felhasználók kizárólag engedélyezett szoftverekkel férjenek hozzá az internethez és ne legyenek képesek a hozzáférés biztonsági beállításait módosítani vagy megkerülni,

j) tiltja a Tankerületi Központ bármely postafiókján a külső elektronikus levelezési címre való automatikus levéltovábbítási szabály beállítását.

(4) A kriptográfia szabályozásával kapcsolatban a Tankerületi Központ és az üzemeltető biztosítja, hogy amennyiben kriptográfiai eljárás használatára kerül sor, úgy ezt az IBSZ és a Tankerületi Központ valamennyi adatvédelmi és informatikai tárgyú szabályzatának figyelembevételével és kizárólag szabványos eljárásban teszi a technológiai standardok alapján elfogadott algoritmusok használatával a lehetőségek szerinti legmagasabb technikai színvonalon.

(5) A Tankerületi Központ elektronikus információs rendszere a 41. §-ban szabályozott távoli hozzáférésre vonatkozó előírások figyelembevételével tiltja és megakadályozza az együttműködésen alapuló számítástechnikai eszközön, így különösen a Tankerületi Központ által üzemeltetett kamerák és mikrofonok engedély nélküli távoli hozzáféréssel való aktiválását és irányítását.

a) Amennyiben a Tankerületi Központ előzetesen engedélyezte az együttműködésen alapuló számítástechnikai eszközök távoli hozzáférést és aktiválást, úgy erről közvetlen és jól észlelhető kijelzéssel kell felhívni mindazok figyelmét, akiket fizikailag érint a kamerás távoli megfigyelés.

b) A Tankerületi Központ munkatársainak számítógépeihez nem csatlakoztatható külső mikrofon és kamera. Azokon az számítógépeken, amelyeken van mikrofon és kamera, azokat inaktiválni kell. A számítógépen mikrofont és kamerát használni kizárólag kifejezett és írásos vezetői engedéllyel és csak az engedélyben meghatározott célból és terjedelemben lehetséges.

(6) A folyamatok elkülönítésének biztosítása érdekében a Tankerületi Központ elektronikus információs rendszere elkülönített végrehajtási tartományt tart fenn minden végrehajtó folyamat számára és elkülöníti a felhasználók által elérhető funkcionalitást az elektronikus információs rendszer menedzsment funkcionalitásától.

(7) A Tankerületi Központ elektronikus információs rendszere a név/cím feloldási kérésekre a hiteles adatokon kívül az információ eredetére és sértetlenségére vonatkozó adatokat is visszaad.

44. Ellenőrzések, rendszeres felülvizsgálatok

45. § (1) Az információbiztonságot folyamatosan kontrollálni kell. A kontroll eljárások kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen.

(2) Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket. Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit. Amennyiben lehetőség van objektív mérőszámok alkalmazására az ellenőrzések során, azt alkalmazni kell. Ebben az esetben előzetesen meg kell határozni, hogy a mérőszámok tekintetében mely adatok az elfogadhatók az ellenőrzés lefolytatása során.

(3) Az ellenőrzés eredményét minden esetben ki kell értékelni és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Szükség esetén felelősségre vonási eljárást kell kezdeményezni. Objektív mérőszámok előzetes meghatározása esetén a mért adatokat össze kell vetni a cél adatokkal és nem megfelelőség esetén az elemzést le kell folytatni, amely meghatározza a nem megfelelőség okait. Nem megfelelőség esetén intézkedési tervet kell felállítani a megfelelőség biztosítására. Az intézkedési terv végrehajtását az elektronikus információs rendszer biztonságáért felelős személy ellenőrzi.

(4) Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

(5) Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

a) megfelelőségi vizsgálat – célja felderíteni, hogy a Tankerületi Központ rendelkezik-e az elégséges személyi, eljárási, tárgyi feltételekkel és azok megfelelően dokumentáltak-e,

b) információbiztonság szintjére vonatkozó vizsgálat – célja felderíteni, hogy az információbiztonság szintje megfelel-e a meghatározott védelmi szintnek,

c) információbiztonsági szabályok betartásának ellenőrzése – célja felderíteni, hogy a Tankerületi Központ információbiztonsági szabályait a felhasználók ismerik-e, illetve betartják-e, – ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető,

d) biztonsági dokumentumrendszer felülvizsgálata – célja a Tankerületi Központ belső szabályrendszerét képező hatályos eljárások felülvizsgálata, hogy azok megfelelnek-e az elvárt jogi, informatikai, szakmai elvárásoknak és az általuk szabályozott területen megfelelő szabályok betartására alkalmazhatóak.

(6) Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

a) az informatikai biztonsági rendszer működése megfelel-e a biztonsági követelményeknek, az informatikai-rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e,

b) az informatikai biztonsági rendszer felépítése, tartalma megfelel-e a vonatkozó szabványnak,

c) az informatikai biztonsági szabályok érvényesülnek-e a folyamatokban,

d) az informatikai-személyzet, illetve a felhasználók rendelkeznek-e a megfelelő informatikai-biztonsági ismeretekkel,

e) az adatokra és a rendszerekre vonatkozó kezelési szabályok betartását,

f) a naplózási rendszer megfelelő alkalmazását,

g) a biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát,

h) a mentési rendszer megfelelő alkalmazását,

i) a hozzáférési jogosultságok naprakészségét, a kiadott jogosultságok szükségességét,

j) a dokumentációk pontosságát, naprakészségét, a változások követését, megfelelő kezelését, nyilvántartását,

k) az alkalmazott szoftverek jogtisztaságát,

l) a szerződések megfelelőségét,

m) a fizikai biztonsági előírások betartását.

(7) Az (5) és (6) bekezdésekben foglaltak, az intézmények esetében történő megvalósulását az elektronikus információs rendszerek biztonságáért felelős személy jogosult ellenőrizni. Az ellenőrzés Megbízólevél alapján történik, melyből két eredeti példány készül. Az első eredeti példány a Tankerületi Központ tulajdona, a második eredeti példány az ellenőrzött intézmény tulajdona. A Megbízólevél az IBSZ 5. mellékletét képezi.

(8) Az elektronikus információs rendszerek biztonságáért felelős személy az általa felállított ütemterv alapján hajtja végre az ellenőrzéseket, melyet a tankerületi igazgató hagy jóvá. Az ütemtervet minden naptári év november 30-ig el kell készíteni a következő naptári évre vonatkozóan, melyben meghatározásra került, mely intézmények kerülnek ellenőrzés alá. Minden intézménynek az ellenőrzésen át kell esnie legalább egyszer, öt éven belül.

(9) Az ellenőrzés helyszíni jelenléttel történik. Az ellenőrzésről minden esetben jegyzőkönyvnek kell, hogy készüljön. A jegyzőkönyvnek minimálisan tartalmaznia kell az ellenőrzés helyszínét, időpontját, az ellenőrzésben résztvevő személyek nevét és pozícióját, az ellenőrzött területeket, a nem megfelelőségeket, a bizonyítékok listáját (dokumentumok, nyilatkozatok, fényképek stb.). A jegyzőkönyv és a bizonyítékok megőrzési ideje legalább 5 év, melynek leteltét követően, amennyiben az ellenőrzéshez kapcsolódóan nincs biztonsági esemény utólagos vagy aktuális kivizsgálása folyamatban vagy felelősségi vonatkozású ügy, akkor törölhető.

(10) A feltárt nem megfelelőségek megszüntetése érdekében az ellenőrzött intézményeknek intézkedési tervet kell készíteni az elektronikus információs rendszerek biztonságáért felelős személy együttműködése és segítségnyújtása mellett az általa meghatározott határidőig, melynek megvalósítása az intézmény feladata. A megvalósult intézkedésekről az elektronikus információs rendszerek biztonságáért felelős személy tájékoztatást kérhet, vagy utóellenőrzés keretében ellenőrizheti.

(11) A tankerületi igazgató az ellenőrzéssel összefüggésben a hiányosságok vagy nem megfelelőségek megszüntetése érdekében intézkedést adhat ki az intézmények részére.

45. Biztonsági rendszerek felülvizsgálata, biztonságelemzési eljárásrend

46. § (1) Az elektronikus információbiztonsági rendszert, illetve annak egyes elemeit rendszeresen felül kell vizsgálni, a következő ütemezés szerint:

Felülvizsgálat tárgya	Felülvizsgálat ciklikussága
Megfelelőségi vizsgálat	1 év
Az információbiztonság szintjére vonatkozó vizsgálat	1 év
Az elektronikus információbiztonsági szabályok betartásának ellenőrzése	1 év
A biztonsági dokumentumrendszer felülvizsgálata	1 év

(2) A Tankerületi Központ által használt elektronikus információs rendszerek, működési környezetük és a kapcsolódó infrastruktúra védelmi intézkedéseit, azok relevanciáját és hatékonyságát, továbbá a működőképességét az előírt biztonsági követelményeknek való megfelelőségét az elektronikus információs rendszerek biztonságáért felelős személy felülvizsgálati tevékenysége keretein belül jogosult ellenőrizni és értékelni, valamint a nem megfelelő védelmi intézkedések kijavítására javaslatot tenni.

(3) A biztonság elemzése során figyelembe lehet venni a szervezet információbiztonsági kockázatelemzését, új rendszer bevezetése esetén a rendelkezésre álló dokumentációt, elektronikus

információs rendszer kivezetésnél a kapcsolódó hatásokat, továbbá változásmenedzsment során a változások okozta kockázatokat, hatásokat, a szervezeti biztonsági eseményeinek dokumentációját, az üzemeltetéssel kapcsolatos szerződéseket és az abban foglalt SLA-kat, illetve bármilyen tényezőt, amely az elektronikus információs rendszerek és az abban kezelt adatok bizalmasságát, sértetlenségét és rendelkezésre állását veszélyeztetheti.

(4) A biztonsági elemzések lefolytatását dokumentálni szükséges, mely dokumentum segítséget nyújt a biztonsági értékelés folyamatában.

(5) A biztonság értékelés során az elemzésekről készített dokumentum felhasználásával az elektronikus információs rendszerek biztonságáért felelős személy összefoglaló jelentést készít a tankerületi igazgató számára, mely jelentés minimálisan a következő adatokat tartalmazza:

a) az értékelendő védelmi intézkedés (adminisztratív, logikai, fizikai),

b) a biztonsági elemzésről készült dokumentációt,

c) az értékelés során figyelembe vett tények, bizonyítékokat.

Az értékelés eredményének függvényében az elektronikus információs rendszer biztonságáért felelős személy javaslatot tehet a tankerületi igazgató részére új védelmi intézkedés bevezetésére vagy meglévő intézkedés módosítására vonatkozóan. Javaslattétel esetén az erőforrások becslését is tartalmaznia kell a jelentésnek.

(6) A biztonsági teljesítmény méréséhez a Tankerületi Központ a következő mérőszámokat és mérési mutatókat alkalmazza (egyedi esetben meghatározható az alábbi felsorolástól eltérő mutató is):

a) adott elektronikus információs rendszer tekintetében rendelkezésre állnak-e a szükséges dokumentációk (igen/nem),

b) az elektronikus információs rendszert ért biztonsági események száma, súlyossága (darab/súlyosság – a 25. § (3) bekezdése szerint),

c) az elektronikus információs rendszerek rendelkezésre állásának hiánya (idő – perc, óra, nap),

d) az elektronikus információs rendszerrel kapcsolatba kerülő személyek képzésének lefedettsége (igen/nem - %-os meghatározás az érintett személyek számának függvényében).

(7) A biztonságértékelési eljárásban a mérések végrehajtásához az elektronikus információs rendszerek biztonságáért felelős személy az elektronikus információs rendszerek üzemeltetőinek és a Klebelsberg Központ Informatikai Főosztályának segítségét is igénybe veheti, továbbá azon személyek segítségét is, akik jelen IBSZ személyi hatálya alá tartoznak. A biztonság értékelése során a mérőszámok és mérési mutatók eredményei felhasználásra kell, hogy kerüljenek, hiánytalanul.

46. Konfigurációkezelési eljárásrend

47. § (1) Az elektronikus információs rendszerek és a kapcsolódó IT infrastruktúra (hardver és szoftver elemek) konfigurációs feladatai az üzemeltető felelőssége. A konfigurációval kapcsolatos minden változásnak dokumentáltnak, nyomon követhetőnek és ellenőrizhetőnek kell lennie. Abban az esetben, ha a konfiguráció módosítással az érintett elektronikus információs rendszer dokumentációja, üzemeltetési leírása megváltozik előre tervezett- vagy nem tervezett módon, arról az érintetteket (felelős vezetők és felhasználók) tájékoztatni kell.

(2) A Tankerületi Központ által használt elektronikus információs rendszereknek az alapkonfigurációjának dokumentációja az üzemeltetőnél rendelkezésre kell, hogy álljon. Ebben az alapkonfiguráció paramétereit rögzíteni szükséges. Az alapkonfiguráció megváltozásáról az elektronikus információs rendszer üzemeltetője tájékoztatja a Tankerületi Központ elektronikus információs rendszerek biztonságáért felelős személyét. Az alapkonfigurációban történt változásoknak utólag megállapíthatónak kell, hogy legyenek.

(3) Az elektronikus információs rendszerek és az IT infrastruktúra további elemeinek a változásának hatásait vizsgálni szükséges és meghatározó mértékű kockázat esetén tesztelni. A változás

végrehajtása minden esetben az üzemeltető feladata és azt az általa felhatalmazott személy/ek hajthatják végre. Bármely az elektronikus információs rendszereket, hardver és szoftver elemeket érő változásnak dokumentáltnak és nyomon követhetőnek kell lennie. A következő változások esetén kell az eljárásrendet alkalmazni:

a) a hozzáférési jogosultságokkal kapcsolatos változások (beállítás, módosítás, visszavonás),

b) az elektronikus információs rendszerek fejlesztése, karbantartása, javítása, bármilyen módosítása (modulok, funkciók hozzáadása, módosítása, elvétele),

c) új elektronikus információs rendszer bevezetése, régi kivezetése,

d) az elektronikus információs rendszer más rendszerrel történő összekapcsolása vagy a rendszer más rendszerről történő leválasztása,

e) az elektronikus információs rendszerek összevonása,

f) a sérülékenység menedzsment feladatainak végrehajtása (frissítések telepítése, biztonsági rések befoltozása).

(4) Az elektronikus információs rendszerek biztonságáért felelős személy jogosult a konfigurációváltozás felügyelet alá eső változtatásokkal kapcsolatos tevékenységek ellenőrzésére, illetve felülvizsgálati tevékenysége során azt ellenőrzési terv alapján auditálhatja.

(5) A Tankerületi Központ elektronikus információs rendszereit érintő változások tekintetében, amennyiben az funkcionalitást érint, előzetes tesztelési eljárást kell lefolytatni annak érdekében, hogy a negatív hatásokat elkerülje az üzemeltető. A tesztelés eredményét ugyanúgy dokumentálni szükséges, mint a változás éles implementációját.

(6) Hardver meghibásodás miatt szükséges rendszerelem csere esetében a beépítésre kerülő új hardverelem műszaki megfelelőségi vizsgálata az üzemeltető feladata. Karbantartás és hibajavítás céljából kizárólag olyan hardverelem építhető be, amely a használt elektronikus információs rendszerek ismert kompatibilitási és konfigurációs igényeinek megfelel.

(7) A Tankerületi Központ hatáskörébe eső változtatások tekintetében biztonsági hatásvizsgálatot kell készíteni, amennyiben a tervezett változtatások meghatározó mértékűek. Ez alól az automatizált változtatások kivételek, amelyek nem változtatnak meg funkcionalitást, vagy nincsenek hatással az elektronikus információs rendszerben zajló adatfeldolgozási, adatkezelési folyamatra és korábban a kockázatok elemzése és kezelése az automatizált változtatás tekintetében megvalósult.

(8) A Tankerületi Központ az általa felügyelt elektronikus információs rendszerek esetében meghatározza a működési követelményeknek megfelelő, de biztonsági szempontból a lehető leginkább korlátozott módon (a szükséges minimum elv alapján, a legszűkebb funkcionalitást figyelembe véve) az alkalmazandó konfigurációs beállításokat, amennyiben erre hatással van. Ezen információkat a rendszerbiztonsági dokumentációkban kell rögzíteni. A beállításokat, amennyiben az a Tankerületi Központ hatáskörébe tartozik, az informatikus látja el és dokumentálja a beállításokat visszakereshető módon. Az elektronikus információs rendszerek biztonságáért felelős személy ezen előírásokat jogosult ellenőrizni.

47. Az adathordozókra vonatkozó különös szabályok

48. § (1) A Tankerületi Központ Információs Vagyonelem Leltárában nyilvántartott adathordozót lehet kizárólag használni a Tankerületi Központ munkatársainak a szervezeten belül, illetve az adatok szervezeten kívülre történő fizikai szállításához, melynek információbiztonságáért a felhasználó felel. Az elektronikus adathordozók nyilvántartását, kezelését, kiadását, visszavételét a rendszergazda végzi.

(2) A felhasználók egyes feladatok elvégzése érdekében, a részükre biztosított, nyilvántartott és egyedi azonosítóval ellátott adathordozóra kimenthetik a feladat elvégzéséhez kapcsolódó állományokat.

(3) Az adatokat az adathordozóról a feladat elvégzése után, a központi kiszolgálóra való felmásolást követően le kell törölni és az adathordozót a tároló helyre vissza kell szolgáltatni. A rendszergazda

gondoskodik az adathordozók újra felhasználása vagy kiadása előtt az adattartalom visszaállíthatatlan törléséről.

(4) A Tankerületi Központ tulajdonában lévő adathordozón kizárólag a Tankerületi Központ kezelésében lévő adat vagy információ tárolható a megengedett ideig, azt magán célra használni és azon magánjellegű adatot tárolni tilos!

(5) Az elektronikus adathordozókat védeni kell a mechanikai-, hő- és mágneses hatásoktól.

(6) Az elektronikus adathordozókra vonatkozó előírásokat az elektronikus információs rendszerek biztonságáért felelős személy ellenőrzi.

48. Naplózási eljárásrend

49. § (1) A Tankerületi Központ olyan elektronikus információs rendszereket használ és vesz igénybe, amelyek biztosítják a következő események naplózását:

a) Rendszer indulás és leállás;

b) A felhasználók adminisztrációs tevékenysége: 1. bejelentkezés, 2. kijelentkezés, 3. jelszómódosítás; (VPN);

c) Az adatállományok (adatbázisok) módosítása az alkalmazási rendszerekben;

d) A rendszergazda a rendszer bármely rétegébe történő be- és kijelentkezése;

e) A rendszergazda tevékenysége a rendszer bármely rétegében;

f) A felhasználói jogosultságok módosítása;

g) Rendszer események, valós események;

h) Kapcsolódó objektumok;

i) Konfigurációs beállítások módosítása.

Abban az esetben, ha valamely elektronikus információs rendszer nem képes a jelen pontban meghatározott események naplózására technikai vagy egyéb okból, akkor az ebből eredő kockázatokat az üzemeltető kockázatelemzési eljárásrendjében foglaltak szerint azonosítani és elemezni kell, és ha a szervezet kockázatéhsége nem bírja el az azonosított kockázatot, akkor kockázatcsökkentési intézkedést kell foganatosítani az eljárásrendben megfogalmazottak szerint.

(2) Az elektronikus információs rendszerek naplózásának kialakításakor be kell vonni a rendszer adatgazdáját is, annak érdekében, hogy adatgazdai oldalról meghatározásra kerüljenek azok a többletinformációk, amelyek a felhasználói tevékenységek nyomon követéséhez szükségesek. A naplózási rendszert az adott elektronikus információs rendszert üzemeltető szervezet alakítja ki az előírásoknak megfelelően. Kiszervezett rendszer esetén gondoskodni kell a kiszervezési szerződésben történő naplózási elvárások szerepeltetéséről. A naplózást úgy kell beállítani, hogy amennyiben a napló tárhely betelik, úgy automatikusan kerüljön archiválásra a napló, ezzel biztosítva a naplóbejegyzések felülírásának megakadályozását. Amely elektronikus információs rendszerek tekintetében a mentések kapcsán nem elvárás meghatározott ideig történő rendelkezésre állás, ott lehetséges a historikus mentések felülírása.

(3) A Tankerületi Központ elektronikus információs rendszereiben a naplóbejegyzések tekintetében elektronikus információs rendszerenként kell meghatározni az adattartalmat.

(4) A naplók tárkapacitását az adott rendszer fejlesztőjének a bevonásával vagy ajánlásai alapján az előzetes kapacitástervezési folyamat során kell kialakítani. A napló tárkapacitás figyelését a rendszerek felügyeleti tevékenység keretein belül az üzemeltető végzi. Kiszervezett elektronikus információs rendszer tekintetében a tárkapacitás figyelését és megfelelőségének biztosítását szerződéses kötelemként kell érvényesíteni.

(5) A Tankerületi Központ elektronikus információs rendszereiben a naplók figyelését oly módon kell kialakítani, hogy naplózási hiba esetén küldjön riasztást a rendszert üzemeltető rendszergazdáknak.

(6) A folyamatos ellenőrzés követelményének történő megfelelés érdekében a szervezet elektronikus információs rendszereiben az eseménynaplókat és biztonsági naplókat a napi üzemeltetési feladatok során át kell vizsgálni. A hibabejegyzéseket és a szokatlan működésre utaló jeleket az IT üzemeltetésnek kell értékelni és kezelni. Amennyiben incidens jeleként értékeli a hibabejegyzést a vizsgálatot végző személy, abban az esetben az incidenskezelési eljárásrendnek megfelelően kell eljárni. A hibajavítást a javító, illetve javítást nyomon követő személynek dokumentálni kell. Jelen dokumentációkat az üzemeltető tartja nyilván, és a felülvizsgálathoz és eljárásrend vagy naplózási tevékenység fejlesztéshez felhasználja a Tankerületi Központ.

(7) A Tankerületi Központ elektronikus információs rendszereiben valamennyi naplóbejegyzését időbélyeggel kell ellátni, melyhez a rendszerórát kell alapul venni. A naplókban található időbélyegek sértetlenségéről gondoskodni kell. A rendszert úgy kell kialakítani, hogy hálózati időszinkron protokoll segítségével szinkronizálja a rendszerórákat az egyezményes koordinált világidőhöz. Az engedélyezett időeltérés 1 perc.

(8) Az elektronikus információs rendszert jelen eljárásrendben foglalt logikai védelmi intézkedések felhasználásával úgy kell kialakítani, hogy a naplóinformációk védettek legyenek a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

(9) A naplóinformációk mentését be kell vonni a Tankerületi Központ és az üzemeltetők mentési rendszerébe. A mentéseket összhangban a napló tárkapacitással úgy kell kialakítani, hogy a naplóbejegyzések nem veszhetnek el. A naplózási adatok és információk tárolása diszkeken és teljes szalagos mentésen is rendelkezésre kell, hogy álljanak.

(10) A Tankerületi Központ elektronikus információs rendszereit fel kell készíteni a következő naplózással kapcsolatos követelmények teljesítésére:

a) Biztosítania kell a naplóbejegyzések előállítási lehetőségét a jelen eljárásrendben meghatározott naplózható eseményekre;

b) Lehetővé kell tennie az üzemeltetésért felelős személyeknek és szükség szerint az információbiztonsági felelősnek is, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az információs rendszer egyes elemeire;

c) Naplóbejegyzéseket kell tudnia előállítania a jelen eljárásrendben meghatározottak szerinti eseményekre a jelen eljárásrendben meghatározott tartalommal.

A naplógeneráló rendszer üzemben tartása az elektronikus információs rendszert üzemeltető szervezet és személy kötelezettsége.

(11) A naplózást végző a naplózással kapcsolatos minden adatról és információról nyilvántartást vezet (Naplózási tevékenységek nyilvántartása), mely nyilvántartás elektronikus információs rendszerenként tartalmazza a következőket:

a) szolgáltatás,

b) szerver/erőforrás,

c) naplózásra kerülő események,

d) naplóbejegyzések pontos adattartalma,

e) naplózási hibák kezelésének eljárása,

f) naplóinformáció védelem megvalósításának módja,

g) naplóbejegyzések megőrzésének ideje.

49. Nyilvánosan elérhető tartalom

50. § (1) A Tankerületi Központ erre a feladatra kijelölt munkatársai a belső utasításoknak és eljárásoknak megfelelően a közérdekű- és közérdekből nyilvános adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény előírásainak

megfelelően tehetik nyilvánosan elérhetővé.

(2) A közérdekű- és közérdekből nyilvános adatoktól eltérő minden, a Tankerületi Központ kezelésében lévő adat és információ tekintetében a tankerületi igazgató által engedélyezett adatok és információk hozhatók nyilvánosságra a tankerületi igazgató által meghatározott platformokon, kommunikációs csatornákon (például a Tankerületi Központ honlapja), az erre kijelölt személyek által.

(3) A tankerületi igazgató, vagy az általa erre a feladatra kijelölt személy feladata és felelőssége a közzétételre javasolt tartalom ellenőrzése, valamint a közzétételre feljogosított munkavállalók képzése a közzététel tartalmával kapcsolatban (mely adat minősül közérdekű- és közérdekből nyilvános adatnak, mely adat, vagy információ minősül a Tankerületi Központ tekintetében érzékenynek, bizalmasnak).

(4) A Tankerületi Központ elektronikus információs rendszerek biztonságáért felelős személye – egyeztetve az adatvédelmi tisztviselővel – jogosult és köteles a jogszabály által előírt gyakorisággal megvizsgálni a nyilvánosan hozzáférhető és a honlapon közzétett adatokat és információkat, s amennyiben nem nyilvános információtartalmat talál, intézkedni annak eltávolításáról, valamint tájékoztatni a vizsgálat eredményéről a tankerületi igazgatót.

(5) A honlap üzemeltetése az adatok és információk közzétételében, illetve eltávolításában köteles együttműködni a Tankerületi Központ munkatársaival.

HARMADIK RÉSZ

ZÁRÓ ÉS HATÁLYBA LÉPTETŐ RENDELKEZÉSEK

51. § (1) Jelen Szabályzat a Klebelsberg Központ elnökének jóváhagyását követő 5. munkanapon lép hatályba.

1. melléklet

Felhasználói nyilatkozat

Foglalkoztatott neve:	
Születési helye, ideje:	
Anyja neve:	

Jogi felelősségem tudatában kijelentem, hogy a Szolnoki Tankerületi Központ (a továbbiakban: Tankerületi Központ) informatikai biztonsági oktatásán részt vettem, illetve a Tankerületi Központ Informatikai Biztonsági Szabályzatában és a kapcsolódó előírásokban foglaltakat a feladatkörömre, illetve a munkakörömre, álláshelyen ellátandó feladatomra vonatkozóan áttanulmányoztam, megértettem, azokat betartom és tudomásul veszem az alábbiakat:

- Az általam átvett informatikai és telekommunikációs eszközök kizárólag a feladatköröm, illetve munkaköri feladataim, álláshelyen ellátandó feladataim ellátását hivatottak támogatni.
- Az általam átvett informatikai és telekommunikációs eszközöket megőrzöm és rendeltetésszerűen használom, azokon jogosulatlanul semmiféle beavatkozást, programtelepítést nem végzek.
- Az informatikai rendszerekben az azonosításomra szolgáló információk (pl. jelszó) titkosságának megőrzésére kötelezettséget vállalok, azt senki tudomására nem hozom, más személyek számára hozzáférhető helyen nem tartom.
- A nem nyilvános, vagy nyilvánosságra nem hozható adatok, információk bizalmasságát (titkosságát) megőrzöm, a vonatkozó előírások megszegése esetén jogi, fegyelmi és kártérítési felelősséggel tartozom.
- Az informatikai rendszerek biztonsága érdekében az elektronikus adatok áramlása, az elektronikusan kezelt adatokból nyomtatott dokumentum előállítása, az internet használata és az elektronikus levelezés naplózásra, ellenőrzésre és szűrésre kerül.
- Az informatikai és telekommunikációs rendszerekkel, szolgáltatásokkal történő visszaélések visszakereshetősége érdekében az eszközök, informatikai és alkalmazói rendszerek és szolgáltatások használata, az elektronikusan kezelt adatokkal végzett műveletek, az adatmozgások rögzítésre (naplózásra) kerülnek.
- Az IT erőforrások használata szükség esetén korlátozásokkal járhat, indokolt esetben a beállított jogosultságok előzetes értesítés nélkül azonnal letiltásra kerülnek.
- A munkavégzés céljából a Tankerületi Központ által rendelkezésre bocsátott informatikai és telekommunikációs eszközök és szolgáltatások a feladatkörbe tartozó, illetve a munkakörben, álláshelyen ellátandófeladatok ellátását hivatottak támogatni, ezért az azokban kezelt, tárolt, illetve továbbított információkat, beleértve az egyéni személyes adatokat is a Tankerületi Központ jogosult megismerni, szűrni.
- A szabálytalan használatból, a szabályok megsértéséből eredő károkért kártérítési felelősséggel tartozom.

Kelt, Szolnok, 20……..……

_____

Foglalkoztatott aláírása

Adatkezelési tájékoztató

Jelen „Felhasználói nyilatkozat” alapján a Szolnoki Tankerületi Központ (5000 Szolnok, Béla Király út 4., szolnok@kk.gov.hu), mint **adatkezelő**, az alapvető elektronikus információbiztonsági követelmények érvényre juttatása, így különösen az adminisztratív védelem, a tudatosságnövelés, a felelősségre vonhatóság, valamint ezek igazolása érdekében vezetett nyilvántartás **céljából** kezeli a személyes adatokat.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) 6. cikk (1) bekezdés e) pontja alapján az adatkezelés a Tankerületi Központ közfeladatának végrehajtásához, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 5-6. § és a 11. § (1) bekezdés g) pontjában meghatározott kötelezettség teljesítése érdekében szükséges (az **adatkezelés jogalapja**).

A „Felhasználói nyilatkozat” a személyi iratanyag része. Az adatkezelés időtartama: a Tankerületi Központ a foglalkoztatott jogviszonyának megszűnését követő öt évig kezeli a „Felhasználói nyilatkozatot”.

Érintetti jogok, jogorvoslati lehetőségek: a foglalkoztatott kérelmezheti a rá vonatkozó személyes adatokhoz való

- *hozzáférést*, így jogosult arra, hogy a Tankerületi Központtól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a GDPR-ban meghatározott információkhoz hozzáférést kapjon;
- *helyesbítést*, vagyis jogosult arra, hogy kérésére a Tankerületi Központ indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat;
- *kezelésének korlátozását*: így jogosult arra, hogy kérésére a Tankerületi Központ korlátozza az adatkezelést, a GDPR 18. cikkében foglalt valamely feltétel teljesülése esetén.
- A foglalkoztatott csak akkor élhet a *törléshez* való jogával, ha az adatkezelési cél eléréséhez az adat nem szükséges.
- A foglalkoztatott a saját helyzetéből adódó indokok miatt *tiltakozhat* az adatkezelés ellen, ha álláspontja szerint a Tankerületi Központ a személyes adatát jelen adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelné.
- A foglalkoztatottat – tekintettel az adatkezelés jogalapjára – nem illeti meg az *adathordozhatósághoz* való jog.

Az érintetti jogok gyakorlásának módja: a foglakoztatott a Tankerületi Központ adatvédelmi tisztviselőjéhez eljutatott kérelmében gyakorolhatja a jelen adatkezeléssel kapcsolatos jogait. Az adatvédelmi tisztviselő elérhetősége megtalálható a Tankerületi Központ weboldalán.

A Tankerületi Központ az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb egy hónapon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

Amennyiben úgy ítéli meg, hogy a Tankerületi Központ a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, abban az esetben panaszt nyújthat be a Szolnoki Tankerületi Központhoz, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (1055 Budapest, Falk Miksa utca 9-11., ugyfelszolgalat@naih.hu), illetőleg a Fővárosi Törvényszékhez (1055 Budapest, Markó u. 27.) fordulhat.

……

foglalkoztatott

Kelt, Szolnok, 20……..……

Készült 2 eredeti példányban.

1. példány – Szolnoki Tankerületi Központ

2. példány – foglalkoztatott

2. melléklet

Informatikai biztonsági oktatási nyilvántartó lap

új belépők részére

Foglalkoztatott neve:	
Születési helye, ideje:	
Anyja neve:	
Szervezeti egysége:	
Munkakör/álláshelyen ellátandó feladat:	
Szervezeti egység vezetőjének neve :	
Foglalkozatási jogviszonyának kezdő időpontja:	
Az oktatás időpontja:	
Az oktatást végző neve :	**……** információbiztonsági felelős

AZ OKTATÁS TEMATIKÁJA

- Az informatikai eszközök, rendszerek, használata munkahelyi feladatokra,
- Internet, e-levelezés használata,
- A vezető (adatgazda) joga, kötelessége az IB szabályok betartásával kapcsolatban,
- A felhasználó joga, kötelessége az IB eszközök használata során,
- A felhasználó azonosító adatainak kezelése, jelszóhasználati rend,
- A jogosultságok igénylése, használata, kezelése,
- Vírus- és végpontvédelmi feladatok,
- Az eszközök fizikai védelme, a felhasználó kötelességei (képernyővédelem, munkaállomás lezárása),
- Szoftverhasználat szabályai,
- Saját (nem munkahelyi) adatok kezelésével kapcsolatos szabályok,
- Munkahelyi adatok kezelése,
- Mobil eszközök, adathordozók használata, távmunka, otthoni munkavégzés szabályai,
- Adatok védelme (biztonsági osztályok, fénymásolók, hálózati nyomtatók használata, titkosítás, elektronikus aláírás),
- IB események és jelentésük,
- Az informatika és IB területére vonatkozó szabályzók, azok elérhetősége.

Kelt, Szolnok, 20 ……

....

információbiztonsági felelős foglalkoztatott

Adatkezelési tájékoztató

Jelen „Informatikai biztonsági oktatási nyilvántartó lap” alapján a Szolnoki Tankerületi Központ (5000 Szolnok, Béla Király út 4., szolnok@kk.gov.hu), mint **adatkezelő**, az információs rendszer adminisztratív védelme, továbbá a tudatosságnövelés érdekében, a munkáltatói feladatainak teljesítése és ennek igazolása **céljából vezetett nyilvántartás érdekében** kezeli a személyes adatokat.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) 6. cikk (1) bekezdés e) pontja alapján az adatkezelés a Tankerületi Központ közfeladatának végrehajtásához, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11. § (1) bekezdés g) pontjában meghatározott kötelezettség teljesítése érdekében szükséges.

Az „Informatikai biztonsági oktatási nyilvántartó lap” a személyi iratanyag része. Az **adatkezelés időtartama**: a Tankerületi Központ a foglalkoztatott jogviszonyának megszüntetéséig kezeli az „Informatikai biztonsági oktatási nyilvántartó lap”-ot.

Érintetti jogok, jogorvoslati lehetőségek: a foglalkoztatott kérelmezheti a rá vonatkozó személyes adatokhoz való

- *hozzáférést*, így jogosult arra, hogy a Tankerületi Központtól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a GDPR-ban meghatározott információkhoz hozzáférést kapjon;
- *helyesbítést*, vagyis jogosult arra, hogy kérésére a Tankerületi Központ indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat;
- *kezelésének korlátozását*: így jogosult arra, hogy kérésére a Tankerületi Központ korlátozza az adatkezelést, a GDPR 18. cikkében foglalt valamely feltétel teljesülése esetén.
- A foglalkoztatott csak akkor élhet a *törléshez* való jogával, ha az adatkezelési cél eléréséhez az adat nem szükséges.
- A foglalkoztatott a saját helyzetéből adódó indokok miatt *tiltakozhat* az adatkezelés ellen, ha álláspontja szerint a Tankerületi Központ a személyes adatát jelen adatkezelési tájékoztatóban megjelölt céllal összefüggésben nem megfelelően kezelné.
- A foglalkoztatottat – tekintettel az adatkezelés jogalapjára – nem illeti meg az *adathordozhatósághoz* való jog.

Az érintetti jogok gyakorlásának módja: a foglakoztatott a Tankerületi Központ adatvédelmi tisztviselőjéhez eljutatott kérelmében gyakorolhatja a jelen adatkezeléssel kapcsolatos jogait. Az adatvédelmi tisztviselő elérhetősége megtalálható a Tankerületi Központ weboldalán.

A Tankerületi Központ az érintett jogai gyakorlására irányuló kérelmét az annak beérkezésétől számított legfeljebb egy hónapon belül teljesíti. A kérelem beérkezésének napja a határidőbe nem számít bele.

Amennyiben úgy ítéli meg, hogy a Tankerületi Központ a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, abban az esetben panaszt nyújthat be a Szolnoki Tankerületi Központhoz, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (1055 Budapest, Falk Miksa utca 9-11, ugyfelszolgalat@naih.hu), illetőleg a Fővárosi Törvényszékhez (1055 Budapest, Markó u. 27.) fordulhat.

.....

foglalkoztatott

Szolnok, 20

Készült 2 eredeti példányban.

1. példány – Szolnoki Tankerületi Központ
2. példány – foglalkoztatott

3. melléklet

Biztonsági szintbe és osztályba sorolás

Szervezet/szervezeti egység	Ibtv. szerinti biztonsági szint
Szolnoki Tankerületi Központ	3

Elektronikus információs rendszer megnevezése	Bizalmasság	Sértetlenség	Rendelkezésre állás	Biztonsági osztály
SzEAT rendszer - Szolgáltatási és Ellátási Alapadat Tár (SzEAT) személyügyi nyilvántartása	3	3	2	3
KRÉTA SAP GR Modul - KRÉTA Gazdasági Rendszer Modul	3	3	3	3
KRÉTA SAP HR Modul - KRÉTA Humánerőforrás modul	3	3	3	3
KRÉTA Tanulmányi Modulcsoport - KRÉTA Intézményi Adminisztrációs Rendszer modul, KRÉTA Elektronikus Napló modul, KRÉTA Elektronikus Ellenőrző modul, KRÉTA Előzetes Tantárgyfelosztás (ETTF) modul, KRÉTA Végleges Tantárgyfelosztás (TTF) modul, KRÉTA Központi Rendszer modul, KRÉTA Ösztöndíj modul, KRÉTA Akadálymentes modul, KRÉTA Lázár Ervin Program, KRÉTA Projekteszköz nyilvántartó, KRÉTA eÜgyintézési modul	3	3	3	3
Microsoft rendszerek - Microsoft Exchange, Sharepoint, Microsoft Office, Skype for Business	2	2	2	2
Poszeidon Irat és Dokumentum Kezelő Rendszer	3	3	3	3
Kincstári Vagyonkataszter	2	2	1	2
Electra	2	2	2	2
Primon6	2	2	2	2
Redmine	1	1	1	1

4. melléklet

A NISZ által telepített szoftverek jegyzéke

Program	License	Megjegyzés
CDBurnerXP	free	CD, DVD író program
e-Signó	free	Digitális aláírtó, és tartozéka egy scanner program, ami több oldalas TIFF dokuemtum megtekintésére alkalmas oldalra ugrási funkcióval. (KIM, NGM, KEF, NETZrt, ME, EMMI, VM, NISZ) https://srv.e-szigno.hu/ e-akta dokumentum megnyitásához szükséges: https://srv.e-szigno.hu/index.php?lap=eakta
Calibre	opensource	E-book olvasó, ami különböző formátumok közötti konvertálásra is alkalmas, és rendelkezik e-book könyvtár funkcióval is. Támogatott formátumok: LIT, MOBI, AZW, EPUB, AZW3, FB2, HTML, PRC, RTF, PDB, TXT, PDF Olvasási formátum: CBZ, CBR, CBC, CHM, DJVU, EPUB, FB2, HTML, HTMLZ, LIT, LRF, MOBI, ODT, PDF, PRC, PDB, PML, RB, RTF, SNB, TCR, TXT, TXTZ Mentési formátum: AZW3, EPUB, FB2, OEB, LIT, LRF, MOBI, HTMLZ, PDB, PML, RB, PDF, RTF, SNB, TCR, TXT, TXTZ
Free Commander	free	Ingyenes kétablakos fájlkezelő. Fájlok másolására, áthelyezésére, átnevezésére, törlésére, mappák kezelésére, törlésére szolgáló program. Windows intéző, Total Commander, Norton Commander helyettesítésére szolgál.
BizAgi Process Modeller	free	Ingyenes üzleti folyamatkészítő alkalmazás. regisztrációt igényel az emlékeztetők (Pro verzió vásárlása) elkerüléséhez A programmal egyszerűen és gyorsan lehet, BPMN szabvány alapján folyamat modellt készíteni. Felhő technológiát is támogat.
Dia	opensource	folyamatábra, áramköri ábra készítő, sematikus ábra (elvi kapcsolási rajz)
GanttProject	opensource	Gantt ábra készítő Project menedzsment program
Inkscape	opensource	Vektor grafikai program: képek létrehozására, szekesztésére, módosítására. SVG kiterjesztésű képek szerkesztéséhez.
Gimp	free	képszerkesztő Raszteres grafikai program: képek létrehozására, szekesztésére, módosítására Adobe Photoshop kiváltására szolgál.
JPEGview	free	Képnézegető
Scribus	opensource	Kiadványszerkesztő program Adobe Indesign szoftver kiváltására szolgál. http://www.scribus.net/canvas/Scribus
Dynare	opensource	Gazdasági (statisztikai) számítások (dinamikus sztochasztikus egyensúly (DSGE), egymást átfedő számítások (OLG)), és hipotézis vizsgálatra elvégzésére alkalmas.
Microsoft Silverlight	free	web-es video lejátszó
VLC videó lejátszó szoftver	free	video lejátszó
FreeMind	opensource	Csoportos ötletesést támogató alkalmazás. (http://freemind.sourceforge.net/wiki/index.php/Main_Page)
FirstPDF	free	Mihez kérték: Magyar közlöny www.magyarkozlony.hu, www.mhk.hu PDF dokumentumból készíthető vele Word, Rich Text dokumentum, Plain Text fájl, és kép.

		Szerkesztés után Word, kép, és TXT fájlba lehet menteni. (KIM (555,963) részére Omnibus program PDF-be tud csak menteni)
PDF Creator	free	PDF konverter: Word, PDF dokumentummá alakító program. A Microsoft Office PDF nyomtónak is felismeri. PDF dokumentumokat más kiterjesztésű dokumentummá tudja alakítani, mint TIFF, JPEG, GIF.
Free PDF to Word Converter	free	Kép PDF-ként scanner-elt dokumentum PDF fájlok konvertálása Wordbe ! Ha a pdf fájl kép, akkor azt nem tudja.
PDF Tools	free	PDF dokumentum szerkesztő program PDF fájlok összeillesztésére, szétválasztására alkalmas, és titkosítására
PDF to Excel converter	free	Táblázatos PDF dokumentumok Excel dokumentummá alakítása. (Van fizetős változata is, a telepítési állomány ingyenes így csökkentett funkcionalitású)
Shape Chollage	free	fényképekből formakészítő
Mpp Viewer	opensource	Microsoft Project dokumentumok (.mpp fájlok) megnézésére szolgál
DiffPDF	opensource	Telepítés nélkül Linux, Mac OS X, Windows, és OS/2 környezetben futtatható, nyílt forráskódú (GNU) PDF dokumentumok tartalmi összehasonlítására alkalmas program.
Demetra	opensource	http://en.wikipedia.org/wiki/Demetra%2B | http://joinup.ec.europa.eu/software/demetraplus/description
GRETL	opensource	A GRETL (Gnu Regression, Econometrics and Time-series Library), egy C nyelven írt, nyílt forráskódú, felhasználóbarát ökonometriai szoftver.
Octave	opensource	A GNU Octave egy magasszintu nyelv, mely elsosorban numerikus számításokra használható. Egy olyan kényelmes parancssoros interfészt szolgáltat, lineáris és nemlineáris problémák numerikus megoldásához, illetve egyéb numerikus kísérletek véghezviteléhez, ami a Matlab-bal nagyrészt kompatibilis. Ugyanakkor felhasználható script-nyelvként is.
Statcan	free	Statisztikai program mikroszimulációs modellek futtatásához.
Cran R	opensource	Statisztikai programcsomag - ingyenes Matlab szintű, jobb az SPSS-nél
AAGISView	free	A Magyar Országos Levéltár Arcanum Adatbázis Kft. (http://mol.arcanum.hu/) DigiDat (web-es alkalmazás, ami a dokumentum adatbázisban történő keresésre és megtekintésére szolgál) alkalmazásának a része, amit a digitális dokumentumaik megtekintésére alkalmaznak. Nyilvános adatbázis.
ArcGIS Explorer Desktop	free	Ingyenes térinformatikai alkalmazás. GIS információkat lehet megosztani (fotó, riport, video) a térképhez történő hozzárendeléssel, az Online alap térkép és felület használatával. Kész speciális elemzéseket lehet használni vele, mint láthatóság, felépítés, közelség keresés.
QuantumGIS	opensource	Térinformatikai rendszer. Programba betöltött térképeken területek megjelölésére alkalmas.
AxCrypt	opensource	Windows platformra, nyílt forráskódú titkosító program. Zökkenőmentesen telepíthető a Windows környezetben, és az összevonás, titkosítás, visszafejtés, tárolás, küldés munka elvégezhető egyedi fájlokkal. \\kdmgmt01\install$\other\AxCrypt http://www.axantum.com/axcrypt/
7Zip	free	Tömörítő: bármilyen formátumú fájl tömörítésére alkalmas (7z, tar, wim, zip kiterjesztésű fájlokká alakítja). Egy vagy több kötegben is lehetséges a tömörítés. Tömörített fájlokat, akár jelszóval is el lehet látni (ZipCrypto, AES-256 titkosítási eljárással) Szöveges fájlokat nagyobb hatékonysággal lehet tömöríteni, mint video, vagy hang fájlokat, az utóbbiak már többségében tömörítettek.

5. melléklet

<Szervezet neve>

<Iktatószám:>

Megbízólevél

Megbízom **<Név, beosztás>** vizsgálatvezetőt / szakértőt (regisztrációs száma, szolgálati igazolványának, illetve – amennyiben szolgálati igazolvánnyal nem rendelkezik – a személyazonosító igazolványának vagy más személyazonosításra alkalmas igazolványának számát), hogy a <Ellenőrzött szervezeti egység neve>-nál/-nél a Szolnoki Tankerületi Központ 6/2024. (IV.24.) számú Informatikai Biztonsági Szabályzata 45. §-ban foglalt

< megfelelőségi vizsgálatot / információbiztonság szintjére vonatkozó vizsgálatot / információbiztonsági szabályok betartásának ellenőrzésére vonatkozó vizsgálatot / biztonsági dokumentumrendszer felülvizsgálatát > tárgyban folytassa le **a 20xx év xx hó xx. napjától- 20xx év xx hó xx**. napjáig terjedő időszakban a szervezet székhelyén / telephelyén.

Az ellenőrzés célja a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályi és információbiztonsági megfelelőségének vizsgálata.

Az ellenőrzés lefolytatására a Szolnoki Tankerületi Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás felhatalmazása alapján <20xx évi Informatikai ellenőrzési terv keretében> / <Szolnoki Tankerület Központ tankerületi igazgatójának döntése> szerint kerül sor.

A vizsgálatot végző ellenőrök az ellenőrzés során az ellenőrzött szervezeti egység helyiségeibe beléphetnek, ott minden vonatkozó iratba betekinthetnek, azokról másolatot készíthetnek vagy kérhetnek, illetve azokat a helyszínről elvihetik.

Az ellenőr a helyszíni ellenőrzés megkezdésekor köteles átadni a megbízólevél egy példányát és bemutatni az azonosító okmányát az ellenőrzött szervezeti egység helyszínen tartózkodó képviselőjének.

Az ellenőr a vizsgálat során a vonatkozó jogszabályok – különös tekintettel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, valamint 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 a 41/2015. (VII. 15.) BM rendeletben –, és a Szolnoki Tankerületi Központ informatikai és információbiztonsági tárgyú belső szabályzatai szerint jár el.

Jelen megbízólevél 20. év … ……hó … napjáig érvényes.

Jóváhagyta:
Név: <tankerület igazgató
Aláírás:
Dátum:
Bélyegző: