ESZTERGOMI
TANKERÜLETI
KÖZPONT

Iktatószám:TK/106/13-35/2018.

Az Esztergomi Tankerületi Központ

17/2018. (VII.30.) szabályzata

Az Esztergomi Tankerületi Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata

Készítette: Muszela Szabolcs mb. tankerületi igazgató

Esztergom, 2018. július 30.

Esztergomi Tankerületi Központ

Muszela Szabolcs
mb. tankerületi igazgató
Esztergomi Tankerületi Központ

Az Esztergomi 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. § (2) bekezdés 9. pontjában biztosított középirányítói hatáskörömben eljárva, a Klebelsberg Központ Szervezeti és Működési Szabályzatáról szóló 61/2016. (XII. 29.) EMMI utasítás 40. §-a alapján jóváhagyom:

Budapest,

utólagosan jóváhagyva
2020 JÚN 02.

Klebelsberg Központ

Hajnal Gabriella
elnök
Klebelsberg Központ

TARTALOM

Az Esztergomi Tankerületi Központ Szervezeti és Működési Szabályzatának 5. § (2) bekezdés f) pontjában biztosított jogkörömben eljárva a Tankerületi Központ (a továbbiakban: Tankerületi Központ) informatikai rendszereinek biztonságos felhasználásának rendjét az alábbiak szerint szabályozom:

ELSŐ RÉSZ

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. A szabályzat hatálya

1. § (1) A Tankerületi Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzatában (a továbbiakban: IBSZ) meghatározott előírások, feladatok, magatartási szabályok – munkakörre való tekintet nélkül – kötelező érvényűek.

(2) Az IBSZ személyi hatálya kiterjed:

a) Tankerületi Központban 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 (továbbiakban: vendég felhasználók), akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással az IBSZ tárgyi hatálya alá tartozó eszközöket, alkalmazásokat és szolgáltatásokat (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) pont a továbbiakban együtt: felhasználók.

(3) A (2) bekezdés hatálya alá tartozó felhasználókkal kötendő, jogviszony létrehozására irányuló dokumentumban rögzíteni szükséges e 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.

2. § Az IBSZ tárgyi hatálya kiterjed:

a) a Nemzeti Infokommunikációs Szolgáltató Zrt. (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 a Tankerületi Központ részére üzemeltetett eszközökön tárolt adatok teljes körére, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

2. A szabályzat célja

3. § (1) Az IBSZ célja a Tankerületi Központ által használt informatikai rendszer, 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.

(2) 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.

(3) Az IBSZ kiadásának célja továbbá a Tankerületi Központ által használt informatikai rendszer alkalmazásának és felhasználásának biztonsági szempontból történő szabályozása.

3. A Szabályzat jogi háttere és 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) a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet,

c) 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,

d) 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,

e) az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló 42/2015. (VII. 15.) BM rendelet,

f) 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,

g) a Tankerületi Központ Szervezeti és Működési Szabályzata;

h) a Tankerületi Központ Egyedi Iratkezelési Szabályzata,

i) a Tankerületi Központ Adatvédelmi és Adatbiztonsági Szabályzata.

(2) Az informatikai biztonság területén érvényesítendő védelmi célkitűzéseket a Tankerületi Központ Informatikai Biztonsági Stratégiája tartalmazza.

(3) Az informatikai biztonságra vonatkozó Tankerületi Központra vonatkozó rendelkezések előkészítése és összeállítása az MSZ ISO/IEC 27000 szabványcsaládra figyelemmel történt (lásd: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en).

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. figyelembe vételével:

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 (jellemzőjű), 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 (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:* az 1. § (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. *INFO:* A Tankerületi Központ informatikáért felelős szervezeti egysége-Gazdálkodási, Üzemeltetési és Pályázati Főosztály.
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. *Tankerületi Központ kapcsolattartója:* a Tankerületi Központ informatikáért felelős szervezeti egysége, amely a NISZ által üzemeltetett informatikai rendszerrel kapcsolatban felmerülő igényeket összesíti és a NISZ felé továbbítja. Ebbe az igénycsoportba nem tartoznak a folyamatban levő szolgáltatással kapcsolatos igények (alkalmazási teendők, hibaelhárítás, hibabejelentés, javítás, informatikai eszközök költöztetése).

55. *Kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

56. *Kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

57. *Kockázattal arányos védelem:* az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

58. *Következmény:* valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát.

59. *Külső felhasználó:* a Tankerületi Központtal szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai.

60. *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.

61. *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.

62. *Munkaállomás:* a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook).

63. *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.

64. *Naplózás:* az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében.

65. *NISZ:* a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendeletben meghatározott központi szolgáltató.

66. *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.

67. *Osztályozás:* adatok, információk, információs infrastruktúra elemek, információs infrastruktúrák biztonsági szempontból való osztályainak kialakítása és ez alapján osztályokba sorolása.

68. *Program:* számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.

69. *Rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

70. *Rendszerelem:* információs infrastruktúra elem.

71. *Sebezhetőség:* olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi.

72. *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.

73. *Szervezeti biztonság:* egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében.

74. *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.

75. *SLA:* szolgáltatási szint megállapodás (Service Level Agreement), amely a megrendelő

(Tankerületi 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.

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 Nemzeti Elektronikus Információbiztonsági Hatósággal (továbbiakban: NEIH) és részére tájékoztatást nyújt a jogszabályi követelményeknek megfelelően, illetve a biztonsági incidensek esetén, ha az szükséges.

6. Az elektronikus információs rendszer biztonságáért felelős személy feladatai

7. § (1) Az informatikai biztonsági szabályok betartásáról a tankerületi 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) elkészíti 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 NEIH-el és a kormányzati eseménykezelő központtal,

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 az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről szóló 42/2015. (VII. 15.) BM rendelet szerint az Ibtv.-ben 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.

7. Az informatikai vezető feladatai

8. § (1) A Gazdálkodási, Üzemeltetési és Pályázati Főosztály vezetője (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 beosztottaik részére igényelt számítógépes erőforráshoz való hozzáférési jogosultságok engedélyezéséért, 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 – különösen a számítóközpontokba, kommunikációs központokba – 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 Gazdálkodási, Üzemeltetési és Pályázati Főosztály 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,

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) A rendszergazdák 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 a 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. § Az alkalmazásgazda jelen Szabályzat szerinti, informatikai biztonságra vonatkozó elsődleges feladatai:

a) az adott alkalmazás bevezetése során történő közreműködés,

b) az informatikai alkalmazás életciklusának folyamatosan figyelemmel kísérése, az észlelt informatikai biztonságot érintő rendellenességről a Helpdesk tájékoztatása,

c) az informatikai rendszer módosítási igényről javaslatot tenni az általa menedzselt alkalmazás frissítésére, kezdeményezni a rendszermentések visszaállítását és

d) támogatni a felhasználókat az adott informatikai alkalmazás használatában, felkérés esetén – az érintett alkalmazás vonatkozásában – szervezett oktatások megtartása.

11. A felhasználók

12. § (1) Általános felhasználók a Tankerületi Központ foglalkoztatottjai (ideértve a gyakornokokat is), 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.

(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 Tankerületi Központ személyügyekért felelős szervezeti egysége 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 jogokra).

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 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 Tankerületi Központ informatikáért felelős szervezeti egysége felé.

(5) A vezető köteles gondoskodni az irányítása alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ és az IBSZ-el 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. 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.

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 a Tankerületi Központ informatikáért felelős szervezeti egysége 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 Főosztály 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.

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.

(4) Az oktatáson történt részvételt a megjelent személyek az IBSZ oktatásán való részvételről szóló nyilatkozat (3. számú melléklet) aláírásával igazolják. Az IBSZ oktatásán való részvételről szóló nyilatkozatban az oktatáson történt részvétel igazolása mellett kötelesek nyilatkozni arról, hogy az informatikai biztonsági előírásokat megismerték és azok betartását magukra nézve kötelezőnek fogadják el. Az IBSZ oktatásán 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 (továbbiakban: SZEAT)-ba történő felvételt követően, a Tankerületi Központ személyi ügyekért felelős szervezeti egysége közreműködésével történik.

(8) A jogosultságok kiosztása előtt, amennyiben az adott munkakör, tevékenység megköveteli a tipikus jogoktól – ide nem értve a munkavégzéshez szükséges adatbázisok elérését – történő eltérést a szervezeti egység vezetőjének az elektronikus információs rendszer biztonságáért felelős személy egyetértését kell kérnie.

(9) A hozzáférési jogosultság – a személyzeti ügyekért felelős szervezeti egység adatszolgáltatása alapján – 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 – a 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 személyügyekért felelős szervezeti egységénél,

b) a személyügyekért felelős szervezeti egység 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.