MÁTÉSZALKAI TANKERÜLETI KÖZPONT

A Mátészalkai Tankerületi Központ

18/2017. (VIII. 21.) szabályzata

A Mátészalkai Tankerületi Központ informatikai rendszereinek biztonságos felhasználásáról szóló szabályzata

Készítette:

Mátészalka, 2017. augusztus „21".

.....

Pesti Béla László

tankerületi igazgató

Mátészalkai Tankerületi Központ

A Mátészalkai 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, 2017. ..October..... „24..."

.....

dr. Solti Péter

elnök

Klebelsberg Központ

TARTALOM

ELSŐ RÉSZ 4
I. Fejezet 4
Általános rendelkezések 4
1. A szabályzat hatálya 4
2. A szabályzat célja 5
3. A Szabályzat jogi háttere és kapcsolódó belső irányítási eszközök 5
II. Fejezet 6
4. Értelmező rendelkezések 6
MÁSODIK RÉSZ 11
III. Fejezet 11
Az információbiztonság szervezeti struktúrája, felelősségi körök 11
5. A tankerületi igazgató feladatai 11
7. Az informatikai vezető feladatai 13
8. Az informatikus 14
9. Az adatgazda 14
10. Az alkalmazásgazda 15
11. A felhasználók 15
IV. Fejezet 16
Az informatikai biztonságra vonatkozó főbb szabályok 16
12. A felhasználókra vonatkozó szabályok 16
13. Vezetőkre vonatkozó szabályok 17
14. Külső felhasználókra vonatkozó szabályok 18
V. Fejezet 19
Információbiztonsági követelmények teljesülése 19
15. Szervezeti biztonsági követelmények 19
16. Személyi biztonsági követelmények, oktatás, jogosultságkezelés 19
17. Fizikai biztonsági követelmények 21
18. Informatikai biztonsági követelmények 21
19. Adminisztratív biztonsági követelmények 21
VI. Fejezet 22
Az információbiztonság működtetése 22
20. Megfelelés az IBSZ-nek, fenyegetettségek 22
21. Az IBSZ felülvizsgálata, aktualizálása 22
22.Az informatikai biztonsági események felismerése, jelentése 22
23. Biztonsági események kivizsgálása 23

24. Biztonsági események nyilvántartása ... 23
25. A biztonsági szabályok megszegésének következményei ... 23
26. Adatok mérése, kiértékelése, mérési pontok meghatározása ... 23
27. Azonosítás és feljogosítás az informatikai rendszer használatára ... 25
28. Szoftverek telepítése, internethasználat ... 25
29. Elektronikus levelezőrendszer használata ... 26
30. Informatikai fejlesztések és beszerzések általános követelményei ... 27
31. Üzemeltetés-biztonság általános követelményei ... 29
32. Vírusvédelem ... 29
VII. Fejezet ... 30
Elektronikus információs rendszerek biztonsági osztályba sorolása ... 30
33. Biztonsági szint meghatározás és biztonsági osztályba sorolás ... 30
34. Az információvagyon felmérése és osztályozása ... 30
35. Elektronikus információs rendszerek nyilvántartása és kezelése ... 32
VIII. Fejezet ... 33
Információbiztonsági eljárások ... 33
36. Általános irányelvek ... 33
37. Munkaállomások hozzáférésére vonatkozó minimális előírások ... 34
38. Szoftvereszközök használatának szabályozása ... 34
39. Tűzfalakkal kapcsolatos szabályozások, betörésvédelem, betörés detektálás ... 34
40.Távoli hozzáférés szabályozása ... 34
41. Mobil IT tevékenység, hordozható informatikai eszközök használata ... 35
42. A rendszer dokumentációk védelme ... 35
43. Ellenőrzések, rendszeres felülvizsgálatok ... 36
44. Biztonsági rendszerek felülvizsgálata ... 37
HARMADIK RÉSZ ... 37
45. Záró hatályba léptető és átmeneti rendelkezések ... 37

A Mátészalkai 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

3. § (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

4. § 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.

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

5. § 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

6. § (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

7. § (1) Az Informatikai Csoport 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 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,

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

8. § (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

9. § (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 Informatikai Csoport 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

10. § 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

11. § (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

12. § (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

13. § (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

14. § (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

15. § (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 Informatikai Csoportja 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

16. § (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.

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. *Informatikai Csoport: (INCS):* 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

szervezeti egység vezetője egyedi elbírálás alapján postafiók beállítást igényelhet.

(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. szakaszban 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 email cím létrehozását 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 email cím karbantartásához szükséges információkat igény esetén biztosítja az üzemeltetés részére, illetve kezdeményezi a csoportos email cím alá történő felhasználói e-mail cím beállítását.

(9) A csoportos email címeket a felelősök félévente felülvizsgálják és szükség esetén gondoskodnak azok módosításáról vagy megszüntetéséről. A csoportos email 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.

30. Informatikai fejlesztések és beszerzések általános követelményei

30. § (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 szakában, szolgálati úton, az INCS 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 az INCS 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 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 – 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,

e) a mentési rendbe való illesztését,

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

(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 általános követelményei

31. § (1) Az informatikai rendszerek rendeltetésszerű működéséért, folyamatos rendelkezésre állásáért a NISZ az egyedi szolgáltatási szerződésében foglaltak szerint felel.

(2) 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.

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

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

(5) A mentésre, illetve az archiválásra vonatkozó szabályokat a rendszerelemek üzemeltetési kézikönyveinek mentésre és archiválásra vonatkozó leírásában kell szabályozni.

(6) 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

32. § (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 tájékoztatást kérhet a NISZ-től.

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

VII. FEJEZET

ELEKTRONIKUS INFORMÁCIÓS RENDSZEREK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

33. Biztonsági szint meghatározás és biztonsági osztályba sorolás

33. § (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 az IBSZ 2. számú 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

34. § (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

35. § (1) A Tankerületi Központ informatikai rendszereinek 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

36. § (1) A Tankerületi Központ épületeiben üzemeltetett eszközök logikai védelmét az 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 munkakör, 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 Tankerületi Központ informatikáért felelős szervezeti egysége 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 Tankerületi 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 személyügyekért felelős szervezeti egysége 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 Tankerületi Központ személyügyekért felelős szervezeti egysége útján kezdeményezi a NISZ kapcsolattartónál.

(13) Gyakornokok esetén a hozzáférési jogosultságok – hasonlóan a külső felhasználók számára létrehozott azonosítókhoz –, csak bizonyos, a munkavégzésükhöz feltétlenül szükséges területekhez való hozzáférést tehetnek lehetővé. A hozzáférési jogosultság megadását a gyakornokot alkalmazó szervezeti egység vezetője vagy a gyakornok közvetlen vezetője – a Tankerületi Központ személyügyekért felelős szervezeti egysége útján – igényelheti a NISZ kapcsolattartótól.

37. Munkaállomások hozzáférésére vonatkozó minimális előírások

37. § (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) Szenzitív adatbázisokat és programokat – amennyiben megoldható – hardveres azonosítást biztosító eszközzel kell védeni.

38. Szoftvereszközök használatának szabályozása

38. § (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 ellenőrizheti.

(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 - a telepítéshez a NISZ közreműködése szükséges,

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, ide értve az engedélyezett freeware és shareware szoftvereket is (5. számú 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

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

40.Távoli hozzáférés szabályozása

40. § (1) A távoli hozzáférések engedélyezésével, korlátozásával és felügyelet alatt tartásával 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

(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.

17. Fizikai biztonsági követelmények

17. § (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

18. § (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

19. § (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

20. § (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 teljes körűen 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

21. § (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

22. § (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.

23. Biztonsági események kivizsgálása

23. § (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).

24. Biztonsági események nyilvántartása

24. § (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 és a biztonsági vezető közösen 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.

25. A biztonsági szabályok megszegésének következményei

25. § (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 bűntető eljárás megindítását kezdeményezni.

26. Adatok mérése, kiértékelése, mérési pontok meghatározása

26. § (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 és feljogosítás az informatikai rendszer használatára

27. § (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 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 6 karakter hosszúságúak lehetnek,

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.

(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.

28. Szoftverek telepítése, internethasználat

28. § (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

29. § (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

való tartása. A Tankerületi Központ informatikai rendszerének távoli elérésére csak egyedileg azonosított felhasználók számára 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

41. § (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

42. § (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. Ellenőrzések, rendszeres felülvizsgálatok

43. § (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.

(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.

(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.

44. Biztonsági rendszerek felülvizsgálata

44. § 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

HARMADIK RÉSZ

ZÁRÓ HATÁLYBA LÉPTETŐ ÉS ÁTMENETI RENDELKEZÉSEK

45. § Jelen szabályzat a Klebelsberg Központ elnökének jóváhagyását követő 5. napon lép hatályba.