(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

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

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

18. Informatikai biztonsági követelmények

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

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

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

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

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

19. Adminisztratív biztonsági követelmények

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

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

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

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

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

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

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

VI. FEJEZET

AZ INFORMÁCIÓBIZTONSÁG MŰKÖDTETÉSE

20. Megfelelés az IBSZ-nek, fenyegetettségek

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

(2) Az IBSZ-nek megfelelő működést igény szerint, de legalább évente 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

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

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

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

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

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

22.Az informatikai biztonsági események felismerése, jelentése

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

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

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

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

ba) nem nyilvános adat illetéktelen személy általi megismerése,

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

bc) informatikai rendszer működésének, használatának jogosulatlan akadályozása,

bd) nem engedélyezett vagy licenccel nem rendelkező szoftver telepítése,

be) felhasználói jelszavak egymás közötti megosztása, hozzáférhetővé tétele,

bf) vírusfertőzés, kémprogramok, billentyűzetleütést figyelő alkalmazások megjelenése,

bg) mobil eszköz elvesztése, ellopása esetén,

bh) fentiek bármelyikére tett kísérlet

(a továbbiakban együtt: biztonsági események).

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

(4) A bejelentés során minimálisan megadandó információk:

a) az informatikai biztonsági esemény pontos leírása,

b) érintett informatikai szolgáltatás pontos megnevezése,

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

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

e) észlelő neve, elérhetősége (opcionális),

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

23. Biztonsági események kivizsgálása

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

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

24. Biztonsági események nyilvántartása

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

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

(2) Az információbiztonsággal kapcsolatos szabályok súlyos megszegése vagy annak gyanúja esetén az elektronikus információs rendszer biztonságáért felelős személy javaslatára – érintett foglalkoztatott közvetlen vezetője, illetve az utasítási joggal rendelkező vezető véleményének kikérésével – a tankerületi igazgató jogosult a megfelelő jogkövetkezmények érvényesítése érdekében fegyelmi eljárást indítani, illetőleg szabálysértési, vagy bűntető eljárás megindítását kezdeményezni.

26. Adatok mérése, kiértékelése, mérési pontok meghatározása

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

hozzáférhetővé kell tenni.

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

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

27. Azonosítás és feljogosítás az informatikai rendszer használatára

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

(2) Az informatikai rendszer használata során a felhasználók 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

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

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

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

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

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

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

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

a) bizonyos fájl-típusok letöltésének korlátozása,

b) az alapvető etikai normákat sértő oldalak látogatásának tiltása,

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

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

(7) Felhasználók internethasználatára vonatkozó általános szabályok:

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

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

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

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

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

29. Elektronikus levelezőrendszer használata

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

(2) A Tankerületi Központtal kormányzati szolgálati jogviszonyban vagy munkaviszonyban álló személy kaphat levelezési címet, személyes postafiókot. Külsős munkavállaló esetén a foglalkoztató szervezeti egység vezetője egyedi elbírálás alapján postafiók beállítást igényelhet.

(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

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

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

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

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

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

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

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

(8) A központi, valamint az európai uniós forrásból megvalósuló fejlesztési projektek informatikai biztonsági követelményeinek teljesítése érdekében a projekt vezetője a projekt tervezési szakában, szolgálati úton, az INFO 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 INFO 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 az informatikáért felelős szervezeti egység javaslata alapján, az elektronikus információs rendszer biztonságáért felelős személy felügyelete mellett a NISZ végzi.

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

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

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

32. § (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

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

a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,

b) támogassa a valós riasztások kiszűrését,

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

d) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,

e) biztosítsa az új fenyegetések időben történő felismerését.

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

(3) A hálózat esetében a vírusvédelem központilag biztosított.

(4) Az elektronikus információs rendszer biztonságáért felelős személy az általános vírusbiztonsági helyzet értékeléseként az előző naptári év vírusriasztásainak statisztikai jellemzőiről és a megtett intézkedésekről 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

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

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

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

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

(5) A biztonsági besorolást tartalmazó táblázat 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

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

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

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

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

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

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

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

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

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

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

Elhanyagolható	
jelentéktelen kár	közvetlen anyagi kár: 0-10.000,- Ft, közvetett anyagi kár 1 embernappal állítható helyre, nincs bizalomvesztés, a probléma a szervezeti egységen belül marad, nyilvános adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Alap	
csekély kár	közvetlen anyagi kár: 10.001-100.000,- Ft, közvetett anyagi kár 1 emberhónappal állítható helyre, társadalmi-politikai hatás: kínos helyzet a szervezeten belül, személyes adatok bizalmassága vagy hitelessége sérül, csekély jelentőségű hivatali információ, adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Fokozott	
közepes kár	közvetlen anyagi kár: 100.001-1.000.000,- Ft, közvetett anyagi kár 1 emberévvel állítható helyre, társadalmi-politikai hatás: bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel, személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, közepes jelentőségű hivatali információ vagy egyéb jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok, stb.) védett bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
Kiemelt	
nagy kár	közvetlen anyagi kár: 1.000.001-10.000.000,- Ft, közvetett anyagi kár 1-10 emberévvel állítható helyre, társadalmi-politikai hatás: bizalomvesztés a szervezet felső vezetésében, középvezetésen belül személyi konzekvenciák, különleges személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül, nagy jelentőségű hivatali információ bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.

Rendkívüli	
kiemelkedően nagy kár	közvetlen anyagi kár: 10.000.001-100.000.000,- Ft, közvetett anyagi kár 10-100 emberévvel állítható helyre, társadalmi-politikai hatás: súlyos bizalomvesztés, a szervezet felső vezetésén belül személyi konzekvenciák, nagy tömegű különleges személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, kiemelt jelentőségű hivatali információ bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.
4+Rendkívüli+	
különösen nagy kár	A „kiemelkedően nagy kár" értéket meghaladó, vagy visszafordíthatatlanul súlyos kár, amely közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását, az államháztartás működését, az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeit, külügyi és nemzetközi kapcsolatait, a szövetséges tagállamokkal közös biztonsági érdekeit.

35. Elektronikus információs rendszerek nyilvántartása és kezelése

36. § (1) A Tankerületi Központ informatikai 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

37. § (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

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

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

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

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

38. Szoftvereszközök használatának szabályozása

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

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

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

40.Távoli hozzáférés szabályozása

41. § (1) A távoli hozzáférések engedélyezésével, korlátozásával és felügyelet alatt tartásával a Tankerületi Központ és a NISZ közös célja a távoli hozzáférés jellegéből következő információbiztonsági és informatikai szolgáltatás biztonsági kockázatok csökkentése, valamint a távoli hozzáférések és az azok által elérhető funkcionalitások számosságának a lehető legalacsonyabb szinten

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

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

a) WebMail-szolgáltatás – OWA elérésen keresztül,

b) Távsegítség nyújtása (kizárólag NISZ alkalmazottakon keresztül).

41. Mobil IT tevékenység, hordozható informatikai eszközök használata

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

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

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

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

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

cb) nem hagyhatják őrizetlenül gépjárműben,

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

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

(3) Tilos a mobil eszközök:

a) engedély nélküli átruházása vagy adatainak közlése, lementése,

b) megfelelő védelem nélkül nem biztonságos hálózathoz csatlakoztatása,

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

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

a) amely adatokról központi biztonsági mentés készül,

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

42. A rendszer dokumentációk védelme

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

(2) Az illetéktelen hozzáférés megelőzése érdekében

a) gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról,

b) minimálisra kell csökkenteni a rendszerdokumentációkhoz hozzáférők számát,

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

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

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

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

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

a) a rendszerterv,

b) üzemeltetési kézikönyv,

c) a katasztrófa-elhárítási terv,

d) a mentési terv, és

e) az üzembehelyezési jegyzőkönyv.

43. Ellenőrzések, rendszeres felülvizsgálatok

44. § (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

45. § 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

46. § (1) A Szabályzat a vonatkozó jogszabályi előírások alapján készült, a Szabályzatban nem érintett kérdésekben a mindenkori hatályos jogszabályok előírásai alkalmazandók.

(2) A szabályzat a Klebelsberg Központ elnökének a jóváhagyását követő 5. napon lép hatályba, és a hatályba lépésekor a már előkészítés alatt álló közbeszerzésekre is alkalmazni kell.

(3) A Tankerületi Központ valamennyi szervezeti egységénél, illetve valamennyi általa fenntartott köznevelési intézménynél gondoskodni kell arról, hogy a szabályzatban foglalt előírásokat az érintett munkatársak megismerjék, aminek tényét a szabályzathoz csatolt megismerési nyilatkozaton aláírásukkal igazolják, a hatálybalépés napjával egyidejűleg.

(4) A Szabályzat hatálya alá tartozó személyek kötelesek a vonatkozó jogszabályok és e Szabályzat előírásait áttanulmányozni, értelmezni és az azokban foglaltak szerint a tőlük elvárható gondossággal eljárni.

(5) Jelen szabályzat hatályba lépésével egyidejűleg hatályát veszíti az e tárgykörben kiadott korábbi szabályozás.

MEGISMERÉSINYILATKOZAT

Mint az Esztergomi Tankerületi Központ munkavállalója az Esztergomi Tankerületi Központ 17/2018. (VII.30.) számú Az Esztergomi Tankerületi Központ Informatikai rendszereinek biztonságos felhasználásáról szóló szabályzatban foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat köteles vagyok betartani és betartatni.

Intézmény neve: _____

Név	Munkakör	Dátum	Aláírás