Iktatószám: KKK 027924002/
00019-1/2022.

Intézmény neve:

Lakitelki Eötvös Általános Iskola
Buzás János Tagintézménye
6032 Nyárlőrinc, Iskola utca 2-4.

OM azonosító:

027924

Szervezeti és Működési Szabályzat melléklete

Kecskeméti Tankerületi Központ

egységes Informatikai Biztonsági Szabályzata

Jóváhagyom:

Nyárlőrinc, 2022. 02. 22.

.....
Intézményvezető

Lakitelki Eötvös Általános Iskola Buzás János Tagintézménye
6032 Nyárlőrinc, Iskola utca 2-4.
Telefon: 76/589-020

Tartalomjegyzék

ÁLTALÁNOS RENDELKEZÉSEK

1. Az Informatikai Biztonsági Szabályzat célja

(1) Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az intézménynél az elektronikus biztonság, és adatvédelem alkotmányos elveinek, követelményeinek az érvényesülését, és megakadályozza a jogosulatlan hozzáférést, megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

(2) Az Informatikai Biztonsági Szabályzat célja továbbá:

a. a titok, munka, vagyon és tűzvédelemre vonatkozó védelmi intézkedések betartása,
b. az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
c. a biztonságot szolgáló karbantartás és fenntartás,
d. az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
e. az adatállományok tartalmi és formai épségének megőrzése,
f. az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
g. a munkaállomásokon lekérdezhető adatok körének meghatározása,
h. az adatállományok biztonságos mentése,
i. az informatikai rendszerek zavartalan üzemeltetése,
j. a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
k. az adatvédelem és adatbiztonság feltételeinek megteremtése.

(3) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

(4) A jelen Informatikai Biztonsági Szabályzat az elektronikus védelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

(1) Az IBSZ személyi hatálya az intézmény valamennyi fő és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

(2) Tárgyi hatálya:

a. kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
b. kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
c. kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
d. kiterjed a rendszer, és felhasználói programokra,
e. kiterjed az adatok felhasználására vonatkozó utasításokra,
f. kiterjed az adathordozók tárolására, felhasználására.

3. Értelmező fogalomtár

A 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.
4. *Adatbázis:* azonos minőségű, 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, DVD, floppy, merevlemez, USB-memória, felhőszolgáltatás, SPS.
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. KRÉTA, SPS napló, nyilvántartások vezetése, ellenőrzése, ennek rendje.)
10. *Archiválás:* adatok, adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése.
11. *Azonosítás (Identifikáció):* informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Ezen folyamat része a hitelesítés (autentikáció). Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi.
12. *Autorizáció (feljogosítás):* azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap.
13. *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.
14. *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.
15. *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.

16. *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.
17. *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.
18. *Biztonsági követelmények:* a kockázatelemzés eredményeként megállapított, elfogadhatatlan mértékű veszély mérséklésére, vagy megszüntetésére irányuló szükségletek együttese.
19. *Biztonsági megfelelőség:* az informatikai rendszer mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek.
20. *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.
21. *Felhőszolgáltatás (cloudclient), és Sharepoint:* A szolgáltatásokat nem egy meghatározott harvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, annak üzemeltetési részleteit a felhasználótól elrejtve. A szolgáltatásokat a felhasználók a hálózaton keresztül érhetik el, vagy az interneten.
22. *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.
23. *Folytonos védelem:* az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
24. *Hardver:* az informatikai rendszer vagy számítógép fizikai elemei
25. *Hálózat:* számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé.
26. *Helyreállítás:* valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen.
27. *Hitelesítés (autentikáció):* a rendszerbe kerülő, ott lévő és onnan kikerülő adatok forrásának (az adat közlőjének), megbízható azonosítása.
28. *Hitelesség:* annak biztosítása, hogy a rendszerbe kerülő adatok és információk eredetiek, a megadott forrásból az abban tárolttal azonos, változatlan tartalommal származnak.
29. *Hozzáférés:* az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása.
30. *Illetéktelen személy:* olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult.
31. *Informatikai alkalmazás:* számítógépen, illetve egyéb informatikai eszközön futó program.
32. *Informatikai biztonság:* az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított.

33. *Informatikai biztonsági incidens:* az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, amelynek célja a kezelésében lévő adatok, dokumentumok és egyéb információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása.

34. *Informatikai biztonsági követelmények:* az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság.

35. *Informatikai rendszer:* a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese.

36. *Informatikai vészhelyzet:* az információs infrastruktúra leállása, szolgáltatások megszakadása, elérhetetlensége, információs vagyonnak jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés.

37. *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.

38. *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.

39. *Információvédelem:* szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.

40. *Jogosultság:* az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához.

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

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

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

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

45. *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.

46. *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.

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

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

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

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

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

52. *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.

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

54. *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.

55. *Szoftver:* a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.

56. *Teljes körű védelem:* azon bármilyen típusú aktív, vagy passzív védelmi intézkedések, melyek a rendszer összes elemére kiterjednek.

57. *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.

58. *Veszély (fenyegetés):* természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett eszközökre.

59. *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.

60. *Visszaállítás:* az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása.

4. Kapcsolódó szabályozások

(1) Az Informatikai Biztonsági Szabályzatot az alábbi előírással összhangban kell alkalmazni:
   a. Szervezeti és Működési Szabályzat.

5. Védelmet igénylő, az informatikai rendszerre ható elemek

(1) Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

(2) Az informatikai rendszerre az alábbi tényezők hatnak:

a. a környezeti infrastruktúra,
b. a hardver elemek,
c. az adathordozók,
d. a dokumentumok,
e. a szoftver elemek,
f. az adatok,
g. a rendszerelemekkel kapcsolatba kerülő személyek.

(3) A védelem tárgya, a védelmi intézkedések kiterjednek:

a. a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
b. az alkalmazott hardver eszközökre és azok működési biztonságára,
c. az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
d. az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
e. az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,
f. a személyhez fűződő és vagyoni jogokra.

(4) A védelem eszközei a mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

6. A védelem felelőse

(1) A védelem felelőse a rendszergazda, vagy akadályoztatása esetén annak, rendszergazdai szerződésben meghatározott megbízottja, erre kijelölt személy.

(2) A jelen szabályzatban foglaltak szakszerű végrehajtásáról a védelmi felelősének kell gondoskodnia. Védelmi felelős feladatai:

a. ellenőrzi a védelmi előírások betartását,
b. felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
c. gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
d. feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
e. a védelmi rendszer érvényesülésének ellenőrzése,
f. felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
g. ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
h. a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
i. a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
j. folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,

(3) A védelmi felelős, ellenőri feladatai:

a. rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
b. előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

(1) Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

(2) A védelmet igénylő adatok, és információk osztályozása, minősítése, hozzáférési jogosultság.

(3) Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

a. közlésre szánt, bárki által megismerhető adatok,
b. minősített, titkos adatok.

(4) Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

(5) Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

(6) A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

(7) A kijelölt dolgozók előtt a titokvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

(8) Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

(9) Minősített adatok esetén, az információhoz való hozzáférést a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység adatbázisokhoz való hozzáférés, a fájlba történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet utólag visszakereshető.

(10) A naplófájlokat havonta át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.

(11) A naplófájlok áttekintéséért, értékeléséért a rendszergazda felelős.

(12) A titkot képező adatok védelmét, a feldolgozás az adattovábbítás, a tárolás során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

(13) Kiosztott jogosultságok az intézményben használt szoftverekhez, adatokhoz

a. Kréta rendszer
b. Érettségi jelentkeztető rendszer
c. KIRA - gazdasági részlegen dolgozó ügyviteli dolgozók
d. Központi mérés-értékelés adatbázis
e. Szakmai vizsga kezelő rendszer
f. Könyvtár adatbázis
g. Iskolai könyvek igénylésének adatbázisa

(14) A jogosultságok kiosztását megelőzően az érintett dolgozók adatbiztonsági nyilatkozatot írnak alá.

8. Az informatikai eszközbázist veszélyeztető helyzetek

(1) Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

(2) Környezeti infrastruktúra okozta ártalmak

a. Elemi csapás:
   a) földrengés, árvíz,
   b) tűz,
   c) villámcsapás, stb.

b. Környezeti kár:
   a) légszennyezettség,
   b) nagy teljesítményű elektromágneses térerő,
   c) elektrosztatikus feltöltődés,
   d) a levegő nedvességtartalmának felszökése vagy leesése,
   e) piszkolódás (pl. por).

c. Közüzemi szolgáltatásba bekövetkező zavarok:
   a) feszültség kimaradás,
   b) feszültségingadozás,
   c) elektromos zárlat,
   d) csőtörés

(3) Emberi tényezőre vissza vezethető veszélyek:

a) Szándékos károkozás:
   a)behatolás az informatikai rendszerek környezetébe,
   b) illetéktelen hozzáférés (adat, eszköz),
   c)adatok, eszközök eltulajdonítása,
   d) rongálás (gép, adathordozó),
   e)megtévesztő adatok bevitele és képzése,
   f) zavarás (feldolgozások, munkafolyamatok).

b) Nem szándékos, illetve gondatlan károkozás:
   a. figyelmetlenség (ellenőrzés hiánya),
   b. szakmai hozzá nem értés,
   c. a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
   d. a jelszó gyakori, havonta történő megváltoztatásának az elmulasztása,
   e. a megváltozott körülmények figyelmen kívül hagyása,
   f. illegális másolattal vírusfertőzött adathordozó behozatala,
   g. biztonsági követelmények és gyári előírások be nem tartása,
   h. adathordozók megrongálása (rossz tárolás, kezelés),
   i. a karbantartási műveletek elmulasztása.

(4) A szükséges biztonságjelző, és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

(5) Tervezés és előkészítés során előforduló veszélyforrások
   a. a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
   b. hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

(6) Rendszerek megvalósítása során előforduló veszélyforrások
   a. hibás adatállomány működése,
   b. helytelen adatkezelés,
   c. programtesztelés elhagyása.

(7) Működés és fejlesztés során előforduló veszélyforrások
   a. emberi gondatlanság,
   b. szervezetlenség,
   c. képzetlenség,
   d. szándékosan elkövetett illetéktelen beavatkozás,
   e. illetéktelen hozzáférés,
   f. üzemeltetési dokumentáció hiánya.

9. Az informatikai eszközök környezete, azok védelme

(1) Munkaállomások

A felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook). 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. 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. A számítógépes munkaállomások képernyőit úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa. Munkaállomásokra vonatkozó előírás csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.

(2) Adathordozók
   a. könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
   b. az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
   c. a használni kívánt adathordozót (CD, DVD, USB-memória , külső merevlemez, felhő) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
   d. a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
   e. adathordozót más szervezetnek átadni csak engedéllyel szabad,
   f. a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

(3) Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetés, karbantartás és szervizelés rendjét külön utasításban kell szabályozni. A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni. A munkák szervezésénél figyelembe kell venni:
   a. a gyártó előírásait, ajánlatait,
   b. a hardver tesztek által feltárt hibákat.
   c. billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell
   d. Alapgép szétbontását csak a rendszergazda végezheti el.

(4) Szoftver védelem

A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá a rögzített tételek visszakeresésének és javításának lehetőségét is.

(5) Vírus védelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

a. Minden munkaállomásra és szerverre vírusellenőrző szoftvert kötelező telepíteni.

b. A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetén meg kell vizsgálni az adathordozó tartalmát. Ha az adathordozón a vírusellenőrző program vírust talált, nem engedhet másolást, futtatást, amíg a vírusoktól nem mentesítik az adathordozót.

c. Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.

d. A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása.

(6) Szerverszoba

A gépterem és szerverszoba védelme elemi csapás (vagy más ok) esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

a. menteni a még használható anyagot,
b. biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
c. új adatfeldolgozás, helyiségek kialakítása,
d. archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

Fenttartási igénye:

a. a szerverszobát a legbiztonságosabb, legvédettebb területre kell telepíteni,
b. a lehető legkevesebb nyílászáróval kell rendelkeznie,
c. váratlan áramkimaradás esetén a szervereket szünetmentes tápegység kell ellátni, mellyel az áramkimaradás folyamatosságát biztosítani lehet.

(7) Egyéb vagyonvédelmi előírások

a. a gépterem és szerverszoba külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
b. a szerverszobába való be és kilépés rendjét szabályozni kell,
c. csak az illetékes dolgozók tartózkodhatnak a gépteremben,
d. a szerverszoba kulcsának felvétele illetve leadása csak aláírás ellenében történhet,
e. munkaidőn túl a szerverszobában csak engedéllyel lehet dolgozni,
f. a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
g. a szerverszobába történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
h. az informatikai eszközöket csak a kijelölt dolgozók használhatják,
e. az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

(8) Tűzvédelem

a. A gépterem (szerverszoba) illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
b. A tűzvédelem feladatait, sajátos előírásokat a gépteremre vonatkozóan az intézmény Tűzvédelmi szabályzata tartalmazza.
c. A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállománytároló helyiség között.
d. Az intézmény azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.
e. Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.
f. A gépteremben dohányozni tilos!
g. A géptermekben, valamint a munkaállomásoknál ételt, italt fogyasztani tilos!
h. A nagy fontosságú, pl. törzsadatállományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

10. Az informatikai feldolgozás folyamatának védelme

(1) Az adatrögzítés védelme

A szerverek rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell. Rögzítési folyamatok meghatározása:

a. adatbevitel hibátlan műszaki állapotú berendezésen történjen,
b. tesztelt adathordozóra lehet adatállományt rögzíteni,
c. az adatrögzítés szoftver védelme.
d. hozzáférési lehetőség:
    a. a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá).
    b. az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
e. adatrögzítési folyamat bizonylatolása.
f. másodlagos adathordozókat kísérő jeggyel kell ellátni melynek tartalma
    a. témaazonosító, bizonylat neve,
    b. rekord (tételszám),
    c. rögzítést ill. ellenőrzést végző személyek nevei.
g. adatrögzítés folyamatához kapcsolódó dokumentációk:
    a. adatrögzítési utasítások,
    b. ellenőrző rögzítési utasítások,
    c. tesztelő és törlő programok kezelési utasításai,
    d. megőrzési utasítások,
    e. gépkezelési leírások.

(2) Az adathordozók védelme és tárolása

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani. Az informatikai eszközök üzemeltetéséért a mindenkori rendszergazda felelős.

Köteles gondoskodni a feldolgozások igényeinek megfelelő mágneses adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.

Az operációs rendszer adta lehetőségek figyelembe vételével biztosítani kell a külső és belső címek azonosságát.

A belső címke felépítésével illetve használatánál figyelembe kell venni a megőrzési időpont ellenőrzésének szükségszerűségét.

Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

Az adathordozók tárolására a géptermen kívüli műszaki, és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

(3) Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni. A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását. A nyilvántartás vezetéséért: körzet leltárfelelőse a felelős.

(4) Az adathordozók megőrzése

Az adathordozók megőrzési idejét a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló többször módosított 1995. évi LXVI. törvényben foglaltak, továbbá intézményünk Bizonylati rendjében és Iratkezelési szabályzatában foglaltak alapján az adatkezelő határozza meg.

(5) Az adathordozók karbantartása

Az adathordozókat 3 évenként tisztítani kell és ellenőrizni a mágneses adathordozók állapotát, elöregedését.

(6) Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell: a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően felhasználásra alkalmatlan CD, DVD, merevlemez, USB-memória

Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezésről jegyzőkönyvet kell készíteni, melynek az alábbi adatokat kell tartalmaznia:

a. a selejtezendő adathordozók tulajdonosának megnevezését,
b. a selejtezés időpontját,
c. milyen adathordozók, és azok mely adatai kerülnek selejtezésre,
d. a selejtezést végzők aláírását.
e. A selejtezési jegyzőkönyvek nem selejtezhetőek.
f. Titkos adatokat tartalmazó adathordozókat selejtezni nem lehet.
g. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni.
h. Biztonsági illetve archív adatállomány előállítása másolásnak számít.

(7) Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

(8) Mentések, fájlokok védelme

Az informatikában a legnagyobb értéket a számítógépen tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése.

a. A mentett adatokhoz csak a mindenkori rendszergazda, illetve a tagintézmény vezető férhetnek hozzá.

Az egyéb mentéseket meghatározott időszakonként el kell végezni.

A munkák során létrehozott dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.

A személyi anyagok adatállományának mentését központi szoftver automatikusan végzi el.
Az egyéb analitikus nyilvántartások adatainak mentését heti gyakorisággal az iskolai titkár számítógépe, automatikusan végzi el.

A levelezések mentését vagy a felhasználó, vagy kérésre a rendszergazda végzi el.

Az adatállományok filevédelme során gondoskodni kell arról, hogy azok ne károsodjanak.

A fontosabb állományokat tartalmazó adathordozókról másolatot kell időnként készíteni. A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

(9) Rendszerszoftver védelme

Az üzemeltetésért felelős vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők

legyenek a felhasználók számára.
Teendők a következők:

a. az üzembiztonság érdekében tartalék operációs rendszerrel kell rendelkezni, amely szükség esetén azonnal betölthető legyen,
b. a rendszerszoftver módosításához az üzemeltetésért felelős vezető engedélye szükséges,
c. név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek,
d. a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni,
e. a változtatásokról nyilvántartást kell vezetni.

(10) Felhasználói programok védelme, Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Minden felhasználónak jelszóval kell védenie a programját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

A jelszavaknak az alábbi minimális követelménnyel kell rendelkeznie:

a. A hálózati jelszó legalább 8 karakterből álljon, kis és nagybetűk, valamint számok, egyéb írásjelek közül legalább 2 típusút tartalmazzon.

b. Az alkalmazáshoz szükséges jelszavaknak legalább 5 karakterből kell állni.

c. A jelszó nem lehet azonos a felhasználó névvel, annak becézett formájával, vagy könnyen visszafejthető kifejezéssel.

d. A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavakat havonta meg kell változtatniuk.

e. Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.

f. A jelszó megváltoztatásakor az új jelszó nem lehet azonos a korábban használt 5 jelszóval.

g. A jelszót nem szabad több személy között megosztani.

h. A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.

i. A jelszót soron kívül meg kell változtatni, ha az illetéktelen személy tudomására jutott, vagy juthatott.

j. A jelszavakat, valamint a munkaállomások BIOS jelszavát lezárt, aláírt és lepecsételt borítékban páncélszekrényben kell tárolni, lehetőleg a vezető irodájában.

Gondoskodni kell arról, hogy a tárolt programok, fileok ne károsodjanak, a követelményeknek megfelelően működjenek.

Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni.

A telepítést dokumentálni kell. A dokumentálásnak tartalmaznia kell azt, hogy milyen programot, mikor és ki telepített fel a számítógépre.

A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

a. a program azonosítója,
b. a program készítőjének neve,
c. a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része. Programok megőrzése, nyilvántartása, a programokról naprakész nyilvántartást kell vezetni, a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A programok nyilvántartásáért és működőképes állapotban való tartásáért a mindenkori rendszergazda felelős.

(11) Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezettségű dokumentálásnak. A dokumentációról nyilvántartást kell vezetni, s ennek az alábbiakat kell tartalmaznia:

a. rendszer megnevezése,
b. dokumentáció típusa,
c. a rendszer adatvédelmi minősítése,
d. a kidolgozók névsora,
e. példányszám és tárolás helye,
f. az átadás ideje,
g. módosítások megnevezése és ideje.

11. A központi eszközök, és a hálózat munkaállomásainak működésbiztonsága

(1) Központi gépek, szerver

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek merevlemezei RAID1 tükrözéssel vannak ellátva. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

(2) Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

Az informatikai eszközt és tartozékait helyéről elvinni a rendszergazda tudta és engedélye nélkül nem szabad.

A munkaállomások tekintetében az alábbi rendelkezéseket is be kell tartani:

a. A munkaállomások nincsenek jól védhető helyen, ezért védelmükről szoftver úton gondoskodni kell.
b. Ha a felhasználó napközben magára hagyja a gépet, zárolást, vagy jelszavas képernyővédőt kell alkalmaznia.
c. Ha a felhasználó munkaviszonya megszűnik, akkor felhasználói azonosítóját meg kell szüntetni.

(3) Hálózat védelme

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. A hálózathoz való hozzáférés korlátozott. A hálózat a csatlakoztatott eszközök fizikai címe alapján szegmensekre van osztva. A szegmensek határozzák meg a hálózati hozzáférés mélységét. A hálózati hozzáférést az iskolában üzemeltetett szerver (proxy szerver) garantálja. Az internet és a hálózat hibaelhárítása a mindenkori rendszergazda feladata. Hiba esetén az iskola vezetése azonnal értesíti a rendszergazdát.

12. Internet hozzáféréssel kapcsolatos intézkedések

(1) Az internet eléréseket biztosító számítógépekre a helyi hálózatra nem kapcsolódó munkaállomásokra vonatkozó szabályok érvényesek.

(2) Az internetes gépen minden esetben működtetni kell a vírusvédelmet.

(3) A vírusok és az illetéktelen hozzáférések miatt tűzfalat kell konfigurálni.

(4) A tűzfal működése közben keletkező állományokat az üzemeltetőnek rendszeresen ellenőrizni kell.

(5) A dolgozók részére történő internetes hozzáférhetőséget, azon való keresés kiterjesztését az intézményvezető felkérésére a rendszergazda szabályozza.

13. Elektronikus levelezéssel kapcsolatos rend

(1) Az elektronikus levelezést külső szolgáltató, külső szerver biztosítja. A szerveren alkalmazandó minimális biztonsági előírások:

a. rendelkezzen webes kliens alkalmazással

b. rendelkezzen az IBSZ-ben meghatározott jelszóházirenddel

c. rendelkezzen levelezési listák kezelésével

d. rendelkezzen olyan felülettel, mely segítségével különösebb szakértelem nélkül menedzselhetők az e-mail fiókok, listák

e. spam szűréssel rendelkezzen

f. rendelkezzen vírusvédelemmel

g. rendelkezzen rosszindulatú támadások elleni védelemmel

(2) Az alkalmazottak, munkavállalók esetleges munkahely váltása után az összes használt jelszót azonnal le kell cserélni!

14. Ellenőrzés

(1) Az intézmény éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

(2) Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszerben meglévő veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az ismétlődjen.

(3) Az informatikáért felelős ellenőrzi, és felel azért, hogy a felhasználók kizárólag a vezetőjük által igényelt és megjelölt informatikai jogosultsággal rendelkezzenek. Szükség esetén gondoskodnia kell a jogosultság törléséről, módosításáról.

(4) A felülvizsgálat során vizsgálni kell:

a. a hozzáférési jogosultságok naprakészségét, a kiadott jogosultságok szükségességét;

b. a felhasználók rendelkeznek-e a megfelelő informatikai-biztonsági ismeretekkel;

c. az informatikai biztonsági szabályok érvényesülnek-e a folyamatokban;

d. megfelel-e a követelményeknek, a jogosultság kezelésben előírt dokumentumok léteznek-e, illetve naprakészek-e;

(6) Jogosultságok hitelességét rendszeresen felül kell vizsgálni, a következő ütemezés szerint:

Felülvizsgálat tárgya	Felülvizsgálat ciklikussága
Megfelelőségi vizsgálat	12 hónap
Jogosultságok betartásának ellenőrzése	12 hónap
Dokumentációk felülvizsgálata	12 hónap

15. Záró rendelkezések

(1) Az Informatikai Biztonsági Szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.
(2) A jelen szabályzatban nem szabályozott kérdések tekintetében a Kecskeméti Tankerületi Központ egyéb belső szabályzatai, a GDPR és az Infótörvény rendelkezései alkalmazandók.