Iktatószám: 90701-A/574-35/2023

Az Aranyalma Integrált Szociális Intézmény Fejér Vármegye 33/2023. (12.14.) számú szabályzata az informatikai biztonságról

1. Általános rendelkezések

1. Az informatikai biztonságról szóló szabályzat (a továbbiakban: szabályzat) az Aranyalma Integrált Szociális Intézmény Fejér Vármegye (székhelye: 8082 Gánt, Bányatelep 1.), a továbbiakban: Intézmény) által használt, üzemeltetett vagy felügyelt informatikai rendszerekre vonatkozóan tartalmazza a legfontosabb információtechnológiai biztonsági feladatokat, továbbá meghatározza azokat az intézkedéseket, tevékenységeket, amelyekre a biztonságos működés érdekében szükség van.

2. Jelen szabályzat alapvető célja, hogy az Intézmény informatikai rendszerének működtetése, üzemeltetése során biztosítsa az adatvédelem elveinek, az információbiztonság követelményeinek érvényesülését, valamint, hogy az Intézmény az informatikai szolgáltatás területén biztosítsa:

a) az informatikára vonatkozó jogszabályi előírások érvényesítését;
b) a folyamatos informatikai üzembiztonság fenntartását;
c) az informatikai vagyon védelmét és megőrzését.

3. (1) Jelen szabályzat hatálya kiterjed az Intézmény tulajdonában, kezelésében lévő valamennyi informatikai rendszerre és azok elemeire, az ott használt alkalmazásokra és adatbázisokra, valamint az általuk keletkeztetett, feldolgozott, tárolt, továbbított valamennyi adatra és információra (függetlenül azok megjelenési formájától), minden eszköz műszaki-, valamint az informatikai folyamatok dokumentációjára.
(2) A szabályzat személyi hatálya az Intézmény Szervezeti és Működési Szabályzatában (a továbbiakban: Intézményi SZMSZ) rögzített személyi hatály szerinti személyekre (a továbbiakban: Munkatársak), valamint a 4. pont 27. alpontja szerinti felhasználókra terjed ki.

4. Jelen szabályzat alkalmazásában:
1. *Adat:* az információ hordozója, megjelenési formája, értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) jelsorozat; olyan jelsorozat, amelyből információ nyerhető ki.
2. *Adatállomány:* adathordozón tárolt, jelképes névvel ellátott adathalmaz.
3. *Adatbázis:* a megfelelő kezelőszoftverrel rendszerbe szervezett, egy vagy több adatállomány.
4. *Adatbázis-motor:* adatbázis-kezelő programok közös, szabvány szerint működő, az adatbázisok elemeit kezelő, hozzáférést, adatfeldolgozást, keresést és egyéb funkciókat kiszolgáló alapmodulja. Az adatbázis-motor az adatbázis kezelő programok vázaként működik, ezek moduljait is vezérli, működésüket alapszabályok szerint definiálja, kiegészítő funkciókat, illesztéseket szabályozza.
5. *Adathalmaz:* valamilyen feldolgozás részére rendelkezésre álló adatok összessége.
6. *Adatátvitel:* adatok szállítása összeköttetéseken, összekötő utakon, informatikai eszközök között.
7. *Adatbiztonság:* az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
8. *Adatbiztosítás:* szélesebb értelemben azon intézkedések összessége, amelyek célja az adatbiztonság szavatolása. Szűkebb értelemben az az intézkedés, amelynek megvalósítása során az adatok biztonsági okokból (rendelkezésre állás és sértetlenség) rendszeresen mentésre kerülnek.
9. *Adatkezelő:* az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.
10. *Adatkezelés:* az adatokon végzett tevékenység (az adatok gyűjtése, rendszerezése, feldolgozása, módosítása, archiválása, törlése, stb.).
11. *Adatvédelem:* az adatok jogosulatlan megszerzésének, illetve manipulálásának megakadályozására irányuló intézkedések összessége.

12. *Alkalmazói program (alkalmazói szoftver):* olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.
13. *Bejelentkezés:* az informatikai rendszer és egy felhasználó között olyan kapcsolat kezdeményezése az utóbbi által, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik, valamint a felhasználó egyértelműen azonosítható lesz.
14. *Bizalmas információ:* az információ létezését vagy tartalmát csak az erre feljogosított személyek, egy meghatározott biztonsági szinten érhetik el.
15. *Bizonyítható azonosítás:* a hozzáférési folyamat jogosultság ellenőrzése során, olyan azonosítási eljárás, amelynek segítségével kétséget kizáróan, utólag is bizonyítható a felhasználó, illetve a szolgáltatást igénybevevő kiléte.
16. *Biztonsági esemény (,,incidens):* olyan esemény, amely bármelyik biztonsági alapelvet (bizalmasság, sértetlenség, rendelkezésre állás) megsértette, és ez által az adatvédelem sérülése bizonyított, illetve nagy bizonyossággal vélelmezhető.
17. *Elektronikus levelező rendszer:* olyan informatikai rendszer, amely az elektronikus levelek (e-mail) küldésére és fogadására szolgál. Alapelemei: felhasználói postafiók, technikai fiók, terjesztési lista, nyilvános naptár, jogosultságok (betekintési, szerkesztési, meghatalmazotti levélküldési, tulajdonosi, adott email címről levélküldési jog). Saját üzemeltetésű, illetve külső szolgáltatótól átvett szolgáltatás keretében vehető igénybe.
18. *Elektronikus levelező rendszer – felhasználói postafiók:* az Intézmény által a munkatársak (felhasználó) munkavégzés céljából rendelkezésére bocsátott elektronikus postafiók, amelyhez a felhasználó hozzáféréssel rendelkezik és a munkakörében meghatározott feladatok elvégzéséhez használja kapcsolattartásra az Intézmény, illetve a Főigazgatóság és a kirendeltségek munkatársaival, valamint külső személyekkel. A felhasználói fiók meghatározottan egyetlen személyhez kötődik. A postafiók főbb elemei: Beérkezett üzenetek mappa és almappái, Elküldött üzenetek mappa és almappái, személyes naptár.
19. *Elektronikus levelező rendszer – technikai fiók:* olyan elektronikus postafiók, amely jellemzően több felhasználó által használt (a felhasználók előre definiált jogosultsági szinttel férnek hozzá). A technikai fiók egy megadott struktúrájú megnevezéssel rendelkezik.
20. *Elektronikus levelező rendszer – Nyilvános Naptár:* az elektronikus levelező rendszer speciális objektuma, amelyet a személyes naptárral megegyező feladatot lát el. A naptárhoz egy adott felhasználó előre definiált hozzáféréssel (betekintési joggal, szerkesztési joggal, nincs jogosultsága) láthatja az objektum tartalmát (naptárbejegyzéseket).
21. *Elektronikus levelező rendszer – betekintési jogosultság:* az elektronikus levelező rendszerhez tartozó alap jogosultságszint, amelyet felhasználói postafiók mappájához, technikai postafiókhoz valamint nyilvános naptárhoz rendelhetünk. Ezzel a jogosultsággal a felhasználó a mappák tartalmába betekintést nyer, elemein változtatni nem tud, az elemek áthelyezése, törlése, új almappa létrehozása nem megengedett.
22. *Elektronikus levelező rendszer – szerkesztési jogosultság:* az elektronikus levelező rendszernek az alapszintnél magasabb jogosultsági szintje, amelyet felhasználói postafiók mappájához, technikai postafiókhoz valamint nyilvános naptárhoz rendelhetnek. Ezzel a jogosultsággal a felhasználó a mappa elemeit módosíthatja, törölheti, almappákat hozhat létre.
23. *Elektronikus levelező rendszer – meghatalmazotti levélküldési jog:* az elektronikus levelező rendszer speciális jogosultsága, amelyet felhasználói postafiókhoz, illetve technikai fiókhoz rendelhetnek. A jogosultsággal az adott felhasználó egy másik felhasználó (vagy technikai fiók) nevében elektronikus levelet küldhet. Ekkor a levél címzettjében az „XY" Meghatalmazó: „Z felhasználó" vagy „a technikai fiók neve" szerepel. Az elküldött levél a meghatalmazott felhasználó elküldött üzenetek mappájába kerül tárolásra.
24. *Elektronikus levelező rendszer – tulajdonosi jog:* az elektronikus levelező rendszerben lévő legmagasabb jogosultsági szint. Egy felhasználó a személyes felhasználói postafiókján tulajdonosi jogosultsággal rendelkezik. E jogosultság birtokában képes a postafiók elemeihez más felhasználók részére jogosultságokat biztosítani.
25. *Elektronikus levelező rendszer – adott e-mail címről levélküldési jog:* az elektronikus levelező rendszer speciális jogosultsága, amelyet felhasználói postafiókokra illetve technikai fiókokra állíthatunk. Az a felhasználó, aki ezzel a jogosultsággal rendelkezik, úgy küldhet levelet egy

másik felhasználó illetve a technikai fiók nevében, hogy a levél címzettje nem látja azt, hogy ezt a levelet ténylegesen nem a levél feladója, hanem más felhasználó küldte. A jogosultság csak megfelelő indoklással és annak a felhasználónak a személyes beleegyezésével adható ki, akinek az e-mail címéről küldeni kívánnak. A jogosultság igénylése kizárólag írásban történhet.

26. *Elektronikus levelező rendszer – terjesztési lista:* az elektronikus levelező rendszer olyan objektuma, amely arra szolgál, hogy egy levél több felhasználó (címzett) részére is elküldésre kerülhessen anélkül, hogy a tényleges címzetteket egyesével kellene a levél címzettjei közé felvenni. A terjesztési lista alapesetekben felhasználókat, de igény szerint további terjesztési listákat tartalmazhat. Megkülönböztetünk központilag kezelt és helyi (a felhasználó saját célfeladatára létrehozott) terjesztési listát.

27. *Felhasználó:* az informatikai rendszeren kívüli személy, aki az informatikai rendszereit használja feladatai megoldásához. Az Intézmény munkatársa, valamint az Intézményvezető jelen szabályzat szerinti – külön, írásos – engedélyével rendelkező személy.

28. *Hardver:* az informatikai rendszer fizikai elemei.

29. *Hálózat:* két vagy több számítógép, illetőleg általánosságban informatikai rendszerek összekapcsolása, amely a komponensei közötti adatcserét teszi lehetővé.

30. *Helpdesk rendszer:* olyan információs rendszer, amely a felhasználók hibabejelentéseinek és egyéb informatikát érintő bejelentéseinek kezelését és az intézkedések dokumentálását és nyomon követését teszi lehetővé.

31. *Hozzáférés:* olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.

32. *Informatika:* olyan tudomány, amely elméletet, szemléletet és módszertant ad a számítógépes információfeldolgozás tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

33. *Informatikai biztonság:* az informatikai rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében képes hozzáférni. Az adatok egyéb (nem szabályozott) módon nem változnak és hitelességük megállapítható. A rendszer rendelkezésre állása kielégíti a megadott követelményeket.

34. *Informatikai eszközök:* minden olyan hardver és szoftver elem, mely az informatikai és számítástechnikai rendszerek működésében részt vesz.

35. *Informatikai rendszer:* a hardverek és szoftverek olyan kombinációjából álló rendszer, amelyet az adat- illetve információkezelés különböző feladatainak és folyamatainak teljesítésére alkalmaznak.

36. *Informatikai támadás:* minden olyan hardver vagy szoftver elem működését befolyásoló tényező, amely szándékosan akadályozza azok működését vagy kárt tesz azokban.

37. *LAN (Local Area Network):* helyi számítógépes hálózat.

38. *Működőképesség:* a rendszernek és elemeinek, az elvárt és igényelt üzemelési állapotban való fennmaradása.

39. *Pótlólagos szoftver:* olyan kiegészítő szoftver, amelyet a védelem erősítésének érdekében alkalmaznak.

40. *Program:* eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

41. *Rendelkezésre állás:* az a tényleges állapot, amikor információk vagy adatok elérhetősége és a rendszer működőképessége az arra jogosultak számára sem átmenetileg, sem pedig tartósan nincs akadályozva.

42. *Rendszerprogram (rendszerszoftver):* olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassák és az alkalmazói programokat működtessék. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

43. *Sértetlenség (integritás):* az információ sértetlensége alatt azt a fogalmat értjük, hogy az információkat, adatokat illetve a programokat csak az arra jogosultak változtathatják meg és azok, más módon nem módosulhatnak.

44. *SPAM:* kéretlen üzleti, politikai vagy vallási célú e-mail, fax vagy SMS, legtöbbször kereskedelmi célú és nagy mennyiségben kiküldött üzenet.

45. *Szoftver:* valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

46. *Tartomány:* a hálózaton lévő szerverek és más számítógépek logikai csoportja, amelyek egy közös biztonsági és bejelentkezési nyilvántartó rendszert használnak. A tartományba nem csak a helyi hálózaton, hanem távoli helyszíneken lévő számítógépek is beléptethetőek.
47. *Tűzfal (firewall):* a belső hálózatot a külső hálózattól védő szoftver és/vagy hardver eszköz. Szabályozza a két oldal közötti információáramlást, biztosítja, hogy az alkalmazások csak a számukra engedélyezett erőforrásokat érhessék el.
48. *Védelmi mechanizmusok:* olyan védelmi intézkedések, amelyeket biztonsági szabványok határoznak meg, a hardver- és szoftvergyártó cégek pedig termékeik előállítása során építik be és szolgáltatják a felhasználók részére.
49. *Vírus:* olyan programtörzs, amely önállóan vagy a felhasználói programba épülve annak normál működését akadályozza. A felhasználói program alkalmazása során *„trójai faló"*-ként működhet, azaz a felhasználó tudta nélkül hajt végre illegális feladatokat, közben „megfertőzhet" az informatikai rendszerben lévő más rendszer- vagy felhasználói programot is, esetleg megsokszorozva önmagát (lehet mutáns is). A *logikai bomba* a vírusnak olyan része, amelyik adott feltétel teljesüléséhez (pl. időhöz, esemény bekövetkezéséhez, logikai változó adott értékéhez) kötött módon aktivizálódik.
50. *WAN (Wide Area Network):* nagy távolságú számítógép-hálózat.
51. *Felhő-alapú informatikai rendszer:* olyan informatikai rendszer, amelynek a szolgáltatásai (szoftver, fejlesztői környezet/platform illetve teljes vagy részleges infrastruktúra biztosítása) egy felhasználói hitelesítés után hozzáférhető, azonban a rendszer mögötti tényleges, technikai megvalósítás részleteit a szolgáltató az igénybe vevő előtt nem fedi fel, így a rendszerben tárolt adatok pontos helyét sem. A szolgáltatás mögötti rendszer főbb jellemzői a redundáns megvalósítás és a terheléselosztás.
52. *Felhő-alapú tárhely-szolgáltatás:* a felhő-alapú informatikai rendszer infrastruktúra szolgáltatás keretében tárhelyet biztosít, amely tárhely felhasználói hitelesítés után az interneten keresztül elérhető. A rendszer a tárhelyen tárolt adatállományt a szolgáltató adatközpont hálózatában, többszörösen tárolja, de a felhasználó felé egy adatállományként, egy logikai egységként teszi elérhetővé. Fő jellemzője a redundáns, legtöbbször különböző földrajzi helyeken felállított adatközpontok közötti folyamatos szinkronizációval történő megvalósítás.
53. *Nyilvános felhő:* olyan rendszer, amelynek megvalósítója minden érdeklődő részére felkínálja az adott szolgáltatást. Ingyenesen elérhető, korlátozott erőforrásokat biztosító szolgáltatásait bárki igénybe veheti. Az elérhető erőforrások nagysága a térítési díj fejében növelhető. Az informatikai rendszer biztonsági intézkedései alapvetően minden igénybe vevő számára egységes és a szolgáltató által előre megalkotott. Az igénybe vevőt érintő jogszabályok előírásainak való megfelelést az igénybe vevőnek kell elbírálnia.

2. A Szabályzat kapcsolódásai, végrehajtása és felülvizsgálata

5. Jelen szabályzatot a mindenkor hatályos jogszabályokkal és az Intézmény belső szabályzataival összhangban kell alkalmazni. A szabályzatot az intézmény és a fenntartó között mindenkor hatályban lévő, a gazdálkodással kapcsolatos feladatok megosztásáról szóló megállapodásban rögzítettekkel összhangban kell alkalmazni. Amennyiben a megállapodás és a szabályzat között eltérés van, úgy a megállapodásban rögzítettek szerint kell eljárni és egyidejűleg intézkedni kell a szabályzat korrekciójáról.

6. A szabályzat kidolgozása, ellenőrzése, majd karbantartatása az Intézmény informatikai feladataiért felelős munkatársának / az informatikai feladatok ellátásáért felelős egység munkatársának / a rendszergazda feladatainak ellátását végző személy/vállalkozás - ahol kiszerződve vállalkozás végzi ezt - munkatársának feladata és hatásköre.

7. (1) Jelen szabályzat végrehajtásának ellenőrzése az intézményvezető/intézményvezető-helyettes feladata. A szabályzatban foglaltak végrehajtását az Intézmény belső ellenőrzésért felelős/a Belső ellenőrzésért felelős egység munkatársa is ellenőrizheti vizsgálatai során.
(2) Az Intézmény jelen szabályzatának hatálya alá vont informatikai eszközök és rendszerek kezelése, a szabályzatban foglaltak érvényesítése, betartatása az Intézmény informatikai

feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység kijelölt munkatársának feladata.

8. (1) A szabályzat hatálya alá tartozó valamennyi felhasználónak ismernie kell azokat a követelményeket és feladatokat, amelyeket a szabályzat számára meghatároz.
(2) A szervezeti egységek vezetői kötelesek gondoskodni arról, hogy az Intézmény alkalmazottai a megfelelő ismereteket megkapják.
(3) A külső fél a hivatali kapcsolattartón keresztül ismerheti meg a szabályzatban foglaltakat.
(4) A szabályzat hatálya alá tartozó valamennyi felhasználó köteles az Intézmény informatikai feladataiért felelős munkatársát, az informatikai feladatok ellátásáért felelős egység vezető munkatársának minden olyan tényről, eseményről közvetlenül vagy a szervezeti egységének vezetőjén keresztül közvetve értesíteni, amely jelen szabályzat rendelkezéseinek végrehajtását akadályozza, gátolja, vagy ilyen hatással lehet, illetve ellentétes jelen szabályzat rendelkezéseivel.

9. Jelen szabályzat végrehajtásának eszközei:
a) az egyes informatikai rendszerek oly módon történő kialakítása, beállítása, hogy az informatikai rendszer kikényszerítse jelen szabályzat rendelkezéseinek betartását;
b) jelen szabályzat kötelező betartatása;
c) jelen szabályzat betartását célzó rendszeres és időszaki ellenőrzések átfogó vagy cél-jelleggel (tételes vagy szúrópróbaszerű ellenőrzési módszerekkel);
d) a hálózat és a szerverek rendszeres monitorozása, a naplók és nyilvántartások pontos és napra kész vezetése, azok rendszeres ellenőrzése;
e) a szervezeti egység vezetőjének tájékoztatása a szervezeti egységet érintő ellenőrzési tapasztalatokról, a munkaviszonyból – ideértve a közalkalmazotti jogviszonyt is – fakadó, a jelen szabályzattal kapcsolatos kötelezettségek vétkes megszegéséről, vagy biztonsági eseményekről, az elkészített jegyzőkönyvek, jelentések, feljegyzések másolatának megküldése útján;
f) jelen szabályzat rendszeres megsértőivel szemben a szabályzatban foglalt ismeretek oktatásán való kötelező részvétel elrendelése és az ismeretek számonkérése évente (az informatikai biztonsági referens által összeállított és kiértékelt kérdőíven);
g) jelen szabályzat rendszeres megsértőivel szembeni – hátrányos jogkövetkezmény kiszabására vonatkozó – munkáltatói intézkedés alkalmazása.

10. A szabályzatot a 14. pont (1) bekezdésben meghatározott feladatot ellátó személy köteles és jogosult időközönként, de legalább évente felülvizsgálni, és szükség esetén a módosításokra javaslatot tenni.

11. A szabályzatot a 14. pont (1) bekezdésben meghatározott feladatot ellátó személy köteles felülvizsgálni és szükség esetén a módosításokra javaslatot tenni, az alábbi esetekben:
a) minden olyan szervezeti változás esetén, amely a szabályzatban hivatkozott szervezeti egységek bármelyikének megszűnésével vagy jelentős átalakulásával jár;
b) súlyos informatikai biztonsági események („incidensek") után, az esemény tanulságait figyelembe véve;
c) hatálybalépést követő évtől minden naptári év január 31. napjáig,
d) jogszabályváltozást követően – amennyiben a jogszabály másként nem rendelkezik – a jogszabályváltozás hatályba lépését követő 30 (harminc) napon belül.

12. Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység köteles legalább évente egy alkalommal megfelelőségi vizsgálatot végezni, és ha szükséges, a szabályzatot módosítani. A megfelelőségi vizsgálat során különösen az alábbiakat kell vizsgálni:
a) a szabályzat betartásával kapcsolatos ellenőrzések eredményét;
b) az időközben felmerülő informatikai és adatvédelmi eseményeket és az ezekkel összefüggő biztonsági vonzatokat.

3. Informatikai biztonsági feladat-, felelősségi és kompetencia körök

13. (1) Az intézményvezető:

a) gondoskodik az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: 2013. évi L. tv.) – illetve utóbb ennek helyébe lépő törvény, valamint a törvény végrehajtását szolgáló rendeletek – végrehajtásáról;

b) kinevezi az elektronikus információs rendszer biztonságáért felelős személyt;

c) jóváhagyja a rendszerek biztonsági osztályba sorolását és az ahhoz kapcsolódó szabályzatokat, stratégiákat;

d) hatáskörében részt vesz a fontosabb informatikai döntésekben, különösen informatikai beruházások, fejlesztések engedélyezésében, illetve az informatikai biztonságot meghatározó, befolyásoló területek, tevékenységek összehangolásában.

(2) Az Intézmény informatikai feladataiért felelős munkatársa, az informatikai feladatok ellátásáért felelős egység vezető munkatársa - illetve amennyiben e tevékenységet az intézmény kiszervezés keretében harmadik személy igénybe vételével látja el, úgy a harmadik személy -:

a) gondoskodik a 2013. évi L. tv. – illetve utóbb ennek helyébe lépő törvény, valamint a törvény végrehajtását szolgáló rendeletek – végrehajtásához szükséges feladatok ellátásáról;

b) meghozza az Intézmény informatikai rendszerével kapcsolatos szakmai döntéseket;

c) megteszi a külső szervezetek számára a szakmai nyilatkozatokat és tájékoztatásokat;

d) kijelöli az általános, illetve feladathoz kötött helyettesét;

e) irányítja az informatikai feladatok ellátásáért felelős egység dolgozóit;

f) kijelöli és meghatározza az informatikusok általános és speciális feladatait;

g) meghatározza az informatikai felelősségi köröket;

h) meghatározza az informatikai oktatási irányokat és gondoskodik megvalósításukról;

i) gondoskodik az Intézmény informatikai stratégiájának megalkotásáról;

j) gondoskodik az Intézmény informatikai eszköz- és adatvagyonának védelméről az eljárások és folyamatok szabályozása útján.

k) külső informatikai szolgáltatások, különösen a felhő-alapú informatikai szolgáltatások igénybevételének lehetőségéről a 14. pont (1) bekezdésben meghatározott feladatokat ellátó személy szakmai állásfoglalása mellett jár el a 2013. évi L. törvényben foglaltaknak megfelelően;

(3) Az Intézménynél alkalmazásban álló informatikus:

a) ellátja az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa által meghatározott informatikai munkaterületeket, feladatokat és célfeladatokat;

b) ellátja az Intézmény meghatározott telephelyeinek informatikai feladatait;

c) elvégezi az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa által a részére kijelölt egyéb feladatokat;

d) munkakapcsolatot tart az Intézmény szervezeti egységeinek dolgozóival, illetve vezetőivel, valamint az üzemeltetési feladatokat ellátó külső szervezetek munkatársaival;

e) az Intézmény érdekében érvényesíti az informatikai előírásokat;

f) eljár és intézkedik az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa vezetője részéről ráosztott feladat érdekében az előírások betartása mellett.

14. (1) Az Intézmény vezetőinek informatikai biztonsággal összefüggő tevékenységét az elektronikus információs rendszerek biztonságáért felelős személy (a továbbiakban: informatikai biztonsági referens) támogatja. Részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, kivizsgálja az informatikai rendkívüli eseményeket, elvégzi a rendszeres biztonsági ellenőrzéseket, és hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik az informatikai biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

(2) Az informatikai biztonsági referens feladatai és jogai:

a) feladata az Intézmény informatikai rendszerének olyan mértékű megismerése, hogy annak elemeit hatékonyan ellenőrizni tudja;

b) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
c) gondoskodik a jogszabályi előírásoknak megfelelő biztonsági osztályba sorolásról;
d) elvégzi vagy irányítja a fentiek szerinti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését;
e) előkészíti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot;
f) összehangolja a biztonságot meghatározó, befolyásoló területek tevékenységét az informatikai biztonság érdekében;
g) gondoskodik az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről, illetve jóváhagyásra előkészíti az éves informatikai biztonsági ellenőrzési tervet és jelen szabályzat javításait;
h) az Intézmény informatikai feladataiért felelős munkatársával/ az informatikai feladatok ellátásáért felelős egység vezető munkatársával együttműködve felügyeli a biztonsággal kapcsolatban készítendő tervek és szabályzatok elkészítését;
i) informatikai biztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét;
j) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit;
k) az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja, javaslatot tesz az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység vezető munkatársának a további intézkedésekre;
l) új informatikai helyiség tervezése és kialakítása során ellenőrzi a szabályzatban megfogalmazott, a helyiségek fizikai paramétereire vonatkozó követelmények kielégítését és a meglevő helyiségek paramétereinek értékét;
m) ellenőrzi az informatikai helyiségbe való beléptetési eljárást és a belépő személyek körének jogosságát;
n) ellenőrzi a beléptető rendszerek kódjának szükség szerinti cseréjét;
o) ellenőrzi az informatikai helyiségek helyiségeihez tartozó kulcsdobozok használatát;
p) ellenőrzi az informatikai biztonsági területeken működő riasztó- és jelzőrendszerek (pl. beléptető rendszer, tűzjelző rendszer, stb.) meglétét és megfelelő működését;
q) az Intézményi SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét;
r) ellenőrzi a fejlesztő rendszerek elkülönítésének megfelelőségét az éles rendszertől;
s) felügyeli az informatikai helyiségeket, eszközöket és infrastruktúrát érintő karbantartási terveket;
t) felügyeli a beruházásokat, a fejlesztéseket és az üzemvitelt informatikai biztonsági szempontból, illetve javaslatot tesz rájuk;
u) az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad;
v) szúrópróbaszerűen ellenőrzi:
va) az egyes felhasználói gépek hardverkonfigurációját és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverek listájával;
vb) hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott (a jogosultsági nyilvántartásban is szereplő) jogosultságokkal;
vc) hogy a javításra kiszállított eszközökön adat ne kerülhessen ki;
vd) az adathordozók selejtezését, illetve megsemmisítését;
w) értékeli a rendszer eseménynaplóit;
x) ellenőrzi a víruskereső programok használatát;
y) ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális);
z) ellenőrzi, hogy a vonatkozó informatikai biztonsági követelményeket a rendszerek fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e;

aa) amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését;
bb) az adott szakterületek vezetőivel egyeztetve meghatározza az egyes feladatkörökhöz tartozóan az informatikai biztonsággal kapcsolatosan elsajátítandó ismeretek körét, és ellenőrzi az elsajátítás tényét;
cc) javaslatot tesz informatikai biztonságot erősítő továbbképzésre;
dd) jelen szabályzatot évente felülvizsgálja, és javaslatot tesz a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások miatt szükségessé váló módosításokra;
ee) javaslattételi joga van a fokozott és kiemelt védelmi osztályba sorolt informatikai rendszerek hozzáférési jogosultságainak kiadásában;
ff) véleményezi a szervezetben felmerülő, vagy már igénybe vett felhő-alapú informatikai rendszerek szolgáltatásait, valamint a szolgáltató által biztosított tárolási helyeit, melyről szakmai véleményét továbbítja az Intézményvezetőnek;

15. (1) Jelen szabályzat vonatkozásában a felhasználó:
a) a munkavégzés során a rábízott eszközöket, szoftvereket felelősséggel, és az előírások, leírások, utasítások szerint használja és megőrzi;
b) az informatikai biztonsági szabályzatot megismeri és betartja;
c) tevékenyen részt vesz az informatikai oktatásokon, szükség esetén tudásáról számot ad;
d) a számítógépes munkavégzése során tiszteletben tartja a felhasználói csoportjára vonatkozó szabályokat és korlátozásokat, valamint a számítógépére megállapított házirendet;
e) a számítógépes rendszerekhez használt hozzáféréseit biztonságos módon megőrzi, a hozzáférésével elkövetett visszaélésekből és károkból származó következményekért a jogszabályokban rögzített mértékű felelősséggel tartozik;
f) jelzi az informatikai biztonsággal kapcsolatos észrevételeit;
g) informatikai segítséget kérhet, ha olyan jellegű feladatot kell ellátnia, amelyhez nincs meg a megfelelő informatikai tapasztalata;
h) a munkájához szükséges eszközöket, alkalmazásokat és szolgáltatásokat a szervezeti egysége vezetőjének engedélyével igényelheti;
i) bármilyen, külső informatikai szolgáltatás, különös tekintettel a felhő-alapú szolgáltatásokra igénybe vétele előtt tájékoztatja a szervezeti egységének vezetőjét, s a szolgáltatás használatát csak a szervezeti egység vezetőjének engedélyével kezdi meg;
(2) Jelen szabályzat vonatkozásában a szervezeti egység vezetője:
a) a szervezeti egység dolgozóinak felvétele, távozása, vagy munkakörváltozása esetén jelen szabályzatban meghatározott módon értesíti a változásról az Intézmény informatikai feladataiért felelős munkatársát/ az informatikai feladatok ellátásáért felelős egységet vagy az intézményvezető által erre megbízott személyt;
b) gondoskodik arról, hogy a szervezeti egységének dolgozói megismerjék, és munkavégzésük során alkalmazzák jelen szabályzatot;
c) ellenőrzi, hogy a szervezeti egységének dolgozói betartják-e jelen szabályzatot;
d) informatikai kérdésekben dönt jelen szabályzatban részére delegált területeken (igénylések, engedélyek).
e) javaslatot tehet felhő-alapú szolgáltatás igénybe vételére (illetve egyetértése esetén továbbítja a felhasználók igényét), amely engedélyezési folyamatába bevonja az informatikai biztonsági referenst, aki a 14. pont (2) bekezdés ff) pontja szerint jár el;

16. Jelen szabályzat tekintetében külső személynek (külső félnek) minősül azon természetes vagy jogi személy, aki az Intézménnyel kötött szerződéses kapcsolat keretében, az Intézmény által kezelt vagy felügyelt területen, az Intézmény megrendelésére informatikával kapcsolatos munkát vagy tevékenységet végez. A külső személy munkája során az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa, illetve az intézményvezető által erre megbízott személy gondoskodik a támogatásáról és felügyeletéről.

17. A külső személy (fél) munkavégzése során az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység, illetve az intézményvezető által erre megbízott személy a külső személy szerződéses kötelezettsége körében és személyes ellenőrzésen keresztül (kapcsolattartó) gondoskodik az alábbi követelmények teljesüléséről:

a) az informatikai rendszer integritása és az adatvédelem elvei nem sérülhetnek;

b) a hozzáférési jogot kapott partnerek (szervezetek, személyek) ezt a jogot tovább nem adhatják;

c) a hozzáférési azonosítókat (behívószám, login név, jelszó stb.) a külső személynek (félnek) titkosan kell kezelnie, biztosítania kell, hogy azokhoz illetéktelenek ne férhessenek hozzá;

d) a külső személynek (félnek) garantálnia kell, hogy azokon a gépeken, amelyeken keresztül a rendszerhez hozzáférnek, nincsenek backdoor programok, illetve ha ezek a gépek hálózatba vannak kötve, akkor a hálózat valamennyi gépére ki kell terjeszteni előbbiekben hivatkozott garanciát;

e) rögzíteni kell, hogy a hozzáférés bármely, a rendszer integritását sértő célból történő felhasználási kísérlete a hatályos jogszabályok szerint bűncselekménynek minősül;

f) ha külső személy (fél) távolról éri el az Intézmény informatikai hálózatát, illetve valamely informatikai rendszerét, akkor a biztonságos elektronikus adatcsere kapcsolat érdekében a külső fél köteles az Intézmény által előírt biztonsági megoldásokat (pl. VPN kapcsolatot) megvalósítani mindazon saját eszközein, amelyekről a távoli elérés lehetséges.

18. Amennyiben a külső személy (fél) a jelen szabályzat hatálya alá tartozó rendszerek, vagy rendszerelemek vonatkozásában szolgáltatást nyújt, akkor

a) első lépésben részletesen meg kell határozni az érintett rendszerelemeket és az érintett folyamatokat;

b) ezt követően meg kell határozni azokat a paramétereket (pl. a normál üzemmódban minimálisan rendelkezésre álló eszközök számát, egyidejűleg működőképes eszközöket és operációs rendszer szoftvereket – típusonként –, alkalmazások használóinak – típusonként – minimális számát, a maximális egyedi és átlagos kiesési időket, az üzemszerű módosítások átvezetésének maximális idejét, upgrade-ek követési idejét stb.), amelyeket a külső személyeknek el kell érnie ahhoz, hogy igazolható legyen a teljesítés.

19. Az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység vezető munkatársának mérlegelnie kell a külső személlyel (féllel) kapcsolatos rendelkezésre állási kockázatokat is. Amennyiben ez a Főigazgatóság által nyújtott szolgáltatások folyamatosságához szükséges, a külső személlyel (féllel) olyan szerződést kell kötni, amely a megfelelő rendelkezésre állási kötelezettségeket tartalmazza.

20. A külső személyek (felek) által nyújtott szolgáltatások ellenőrzését rendszeresen kell végezni, és bármely felmerülő együttműködési probléma esetén ki kell deríteni annak okát. A hiba okának gyors és hatékony kiküszöbölése érdekében meg kell tenni a szükséges lépéseket. A külső személlyel (féllel) kötött szerződésben meg kell határozni, hogy a szolgáltatást nyújtó külső személy nem-teljesítése, hibája, vétkessége esetén az Intézmény milyen kompenzációra (pl. kötbér), illetve kártérítésre tarthat igényt, és azt milyen módon érvényesítheti. Előbbi rendelkezéseknek ki kell terjedniük a szerződés megszüntetésének, felmondásának eseteire is, és külön meg kell határozni a biztonsági előírások megsértése esetére vonatkozó szabályokat.

4. Az információ vagyon védelmének szabályai

21. (1) Az Intézmény informatikai rendszeréről és eszközeiről csak az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység szolgáltathat adatokat.

(2) Az Intézmény által bevezetett alkalmazói rendszerek bevezetésében és felhasználásában közreműködő külső személy (fél) titoktartási nyilatkozat tételére köteles. A titoktartási kötelezettség kiterjed az alkalmazói rendszerekkel kapcsolatos, illetve ezek bevezetése során tudomásra jutó információkra.

(3) Az alkalmazói rendszerek bevezetése és működtetése kapcsán a rendszerekkel kapcsolatba kerülő külső személyeknek (feleknek) kötelezettséget kell vállalniuk azért, hogy

a) a tudomásukra jutott információkat kizárólag az Intézmény által meghatározott célokra használják fel;

b) azokat harmadik személy részére az intézményvezető előzetes, írásos engedélye nélkül nem adják át;

c) az Intézmény tevékenységére vonatkozó információk rögzítésére semmiféle technikai eszközt vagy más eszközt nem alkalmazhatnak.

22. (1) Minden felhasználó az általa végzett elektronikus adatfeldolgozás során személyesen felelős az adatvédelmi szabályok és az információbiztonsági előírások betartásáért.

(2) Külső személy (fél) munkavégzése során törekedni kell arra, hogy:

a) a feladatához szükségtelen hivatali adat, információ ne kerüljön tudomására;

b) a feltétlenül szükséges adat birtoklásáról és az információ megismeréséről nyilatkozzon, és ha szükséges titoktartási nyilatkozatot tegyen.

23. (1) Az Intézmény számítógépeiről, szervereiről – a munkahelyi célú felhasználás kivételével – nem engedélyezett a programok, a minősített adatot tartalmazó adatállományok, illetve a munkavégzés során szerzett egyéb adatok, információk másolása, azok más, illetéktelen személyekkel történő megismertetése.

(2) Nyomatképző berendezések (fénymásoló, nyomtató, stb.) használata során törekedni kell a felesleges vagy rontott iratpéldányok megsemmisítésére. Az előbbiekhez szükséges iratmegsemmisítő berendezések biztosítása és üzemeltetése, illetve a központi zúzásra szánt iratpéldányok gyűjtőedényeinek óránkénti ürítése Intézmény gazdálkodási feladatait ellátó szervezeti egységének feladata.

(3) Az információvédelem keretében törekedni kell a nyomatképző berendezések, biztonsági (szenzitív) nyomtatások, továbbá a fénymásoló berendezések, szkennelések használatára, üzemeltetésére és a lehetséges központosított kezelésére, ezzel csökkentve a felesleges és rontott iratpéldányok számát, valamint növelve az adatbiztonságot. A megoldások tesztelése, kiválasztása és üzemeltetése az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység feladata.

(4) A nyomatképző berendezések naplóját az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) a belső hálózaton tárolja legalább 30 (harminc) napra visszamenőleg.

(5) A műszaki eszközök (monitorok, nyomtatók, fénymásolók) elhelyezése során biztosítani kell, hogy bizalmas információ illetéktelen személy tudomására ne juthasson, illetve törekedni kell a monitorok esetében az épület ellenőrizetlen közlekedő folyosóiról való teljes rálátás megakadályozására, hatékony megnehezítésére.

(6) A (3) bekezdésben előírt biztonsági nyomatképző funkciók használatával a felhasználó kizárólagos felelőssége az iratpéldányok biztonságos kezelése, elhelyezése.

(7) Amennyiben a felhasználó gondatlanságból vagy szándékosan a (2) bekezdésben leírtaknak megfelelően nem gondoskodik a felesleges vagy rontott iratpéldányok megsemmisítéséről és így az iratpéldány illetéktelen kezekbe kerül, illetve az iratokban lévő információkat illetéktelen célra felhasználták, a felhasználó ezért teljes felelősséggel tartozik.

(8) Az adathordozók és nyomtatványok tárolása során gondoskodni kell az illetéktelen személyek hozzáférésének megakadályozásáról.

24. (1) Az IT biztonsággal szemben támasztott követelmények:

a) *Rendelkezésre állás:* a szolgáltatások és adatok elérhetősége biztosított legyen az arra jogosult felhasználók számára. Biztosított a védelem a jogosulatlan hozzáféréstől és adatmódosítástól, törléstől, illetve a szolgáltatás elérhetőségének megakadályozásától.

b) *Sértetlenség:* adat- és rendszerintegritás. Adatintegritással került biztosításra, hogy adat nem módosulhat nem engedélyezett (nem tervezett) módon a tárolás, feldolgozás, adatátvitel

során. Rendszerintegritás alapján a rendszer a megvalósított funkciót nem engedélyezett manipulációtól mentesen hajtja végre.
c) *Bizalmasság:* az a követelmény, hogy a bizalmas, vagy magántermészetű információ nem jut jogosulatlan személy kezekbe. Ez vonatkozik az adat tárolására, feldolgozására, átvitelére egyaránt.
d) *Felelősség:* bármely entitás cselekvései követhetőek legyenek, és egyértelműen visszavezethetőek legyenek rá.
e) *Megbízhatóság:* a különböző biztonsági intézkedések az irányítási, technológiai, működési vezérlés területén megfelelően működnek, és védik a rendszert és az általa feldolgozott adatot. Előbbi célok megvalósítottnak tekinthetők, ha:
ea) a kívánt funkció jelen van és pontosan megvalósított;
eb) megfelelő védelem van a nem szándékos hibák ellen;
ec) megfelelő védelem van a szándékos hibák (behatolás, stb.) ellen;
(2) Az Intézmény területén végzett minden tevékenység (építési és karbantartási munka, ügyfélforgalom bonyolítása, üzemeltetési feladatok ellátása, postaszolgálat, futárszolgálat) során figyelemmel kell lenni jelen szabályzat betartására és betartatására az IT biztonság követelményeinek maximális fenntartására.

25. Az Intézményben végzett minden tevékenység során szem előtt kell tartani
a) az ellátottak adatainak és információinak,
b) az ügyek elemeinek – mint külön ágazati törvényben is védett adatnak, információnak minősülő kifejezetten érzékeny információk – bizalmas jellegét és ezért az informatikai struktúrát és környezetet ennek megfelelően kell kialakítani.

26. (1) A számítógép- vagy programhibából eredő adatvesztés gyanúja esetén az – adatfeldolgozás szüneteltetése mellett – a kijelölt informatikust haladéktalanul értesíteni kell. Az értesítés módja személyes, vagy telefonos értesítés, vagy elektronikus úton tett bejelentés. A probléma tisztázása után az informatikus útmutatása szerint kell lefolytatni az adatrögzítést, illetve adatfeldolgozást.
(2) Az alkalmazásokhoz és a hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése útján gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, illetve ne törölhesse.
(3) A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sértetlenségét.

27. Az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység, vagy az intézményvezető által erre megbízott személy feladata biztosítani – illetve külső szolgáltató által szolgáltatott rendszer esetében biztosíttatni – az informatikai rendszerek folyamatos rendelkezésre állását az alábbi eszközök felhasználásával:
a) rendszeres adatmentésekkel, illetve szoftvertelepítő készletek megfelelő biztosításával és megfelelő tárolásával;
b) tartalék eszközök és alkatrészek biztosításával;
c) helyreállítási módszerleírások, vészforgatókönyvek naprakész biztosításával.

28. A rendszerek információvagyonának biztonsági szempontú osztályozása az adatok bizalmassága, megőrzési követelményei és hitelessége szempontjából történik.

29. Az adatokat az alábbi szempontok szerint kell osztályozni:
a) a közérdekű, illetve a közérdekből nyilvános adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.) határozza meg;
b) amennyiben ágazati törvény bizonyos adatkört védeni rendel, úgy az adott ágazati törvényben rögzítettek;
c) a közérdekű adat nyilvánosságához fűződő jogok minősítéssel történő korlátozását a minősített adat védelméről szóló 2009. évi CLV. törvény szabályozza;
d) az üzleti titok körébe tartozó adatokat a 2018. évi LIV. törvény határozza meg;
e) az adatok osztályozója, amennyiben azt jogszabály nem szabályozza, annak a szervezeti egységnek a vezetője, amelynek érdekkörébe az adat tartozik;

f) a rendszerekben nyilvánosnak csak az intézményvezető által egyértelműen annak minősített információ tekinthető;
g) a nyilvános adatok kivételével, valamennyi adatot bizalmasként (védendő nem titkos adat) kell kezelni.

30. (1) Az adatkezelésre vonatkozó szabályokat az Info tv. tartalmazza.
(2) Az informatikai adatkezelés és adatfeldolgozási munka során az adatvédelemre vonatkozó szabályok szerint kell eljárni.

31. (1) Az Intézmény informatikai hálózatára kizárólag az Intézmény által biztosított eszközöket (számítógépeket, laptopokat, mobil eszközöket) lehet rácsatlakoztatni.
(2) Az (1) bekezdésben foglaltak mellett külön engedéllyel, szakmailag indokolt esetben csatlakoztatható a felhasználó saját tulajdonában lévő eszköz az Intézmény informatikai hálózatára. A szakmai indok ellenőrzése az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység hatásköre.
(3) Saját tulajdonú eszköz felcsatlakoztatására kizárólag időszakos engedély adható ki, legfeljebb 1 (egy) hónapra. Az engedély megújítása csak a szakmai indokok fennállása esetén megengedett. Az engedély csak egyszer hosszabbítható meg.
(4) Amennyiben a külön engedélyt 2 (kettő) hónapnál hosszabb időre kellene kiadni, úgy mérlegelni kell informatikai eszköz biztosítását az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység rendelkezésére álló raktárkészletéből.
(5) Amennyiben a (4) bekezdésben foglaltak nem teljesíthetők, úgy a (3) bekezdésben kiállított engedély meghosszabbítható, ameddig az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység nem tud biztosítani megfelelő eszközt.
(6) Az (5) bekezdés alapján meghosszabbított engedély meghosszabbításának szakmai indokoltságát az Intézmény gazdálkodási feladatait ellátó szervezeti egysége bármikor megvizsgálhatja, és megalapozottság hiányában megvétózhatja.
(7) Az Intézmény informatikai hálózatára csatlakoztatott minden eszközön alkalmazni kell a kötelező jelszóhasználatot (amennyiben az Intézmény informatikai rendszere nincs ellátva központi címtárral, úgy a számítógépeken ki kell alakítani a kötelezően jelszóval védett lokálisan kialakított felhasználói környezetet), mobil eszközökön, a PIN kód használatát.
(8) Minden informatikai eszközön alkalmazni kell az időzáras [maximum 10 (tíz) perc inaktivitás után automatikusan érvénybe lépő] és kizárólag jelszóval (mobil eszközön, PIN kóddal vagy mintával) feloldható képernyőzárat.
(9) Minden olyan eszköznek, amelyről az Intézmény informatikai hálózata felhasználói authentikáció birtokában elérhető, megfelelő, naprakész vírusvédelemmel ellátottnak és ellenőrzöttnek (a vírusvédelmi program naplójában megtalálható, sikeres lefutás) kell lennie.
(10) Amennyiben a vírusvédelmi program folyamatos ellenőrzései aktívak, akkor nincs szükség igazolható ellenőrzésre, kivéve, ha a vírusvédelmi program telepítése a csatlakozás előtt 2 (kettő), vagy annál kevesebb nappal történt. Ebben az esetben kizárólag a naplóval bizonyítható ellenőrzés esetén engedélyezhető az eszköz felcsatlakoztatása.
(11) Amennyiben az Intézmény informatikai hálózatára a felhasználó tulajdonában lévő informatikai eszközt kíván felcsatlakoztatni, az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység köteles a jelszóra, a képernyőzárra, illetve a vírusirtó megoldásra vonatkozó ellenőrzést elvégezni. Az ellenőrzés lehet manuális ellenőrzés, illetve központi szoftveres ellenőrzés.
(12) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység a (11) bekezdésben meghatározott elemek bármelyikének hiányában megtagadhatja az eszköz felcsatlakozásának engedélyét az Intézmény informatikai hálózatára. A vírusvédelem hiányában a felcsatlakozás engedélyezése mérlegelés nélkül elutasítandó.
(13) A (7)-(8) bekezdésben foglaltakat az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) véletlenszerű kiválasztással, szúrópróbaszerűen ellenőrzi, és erről nyilvántartást vezet.

(14) Amennyiben a (13) bekezdésben leírt ellenőrzésen egy felhasználó többször fennakad, azaz a kötelező védelmi elem használatát mellőzi, úgy az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység javaslatot tehet az intézményvezetőnek a jelen szabályzat megsértésének szankciójára, amely javasolt szankció lehet:

a) szóbeli figyelmeztetés;

b) írásbeli figyelmeztetés, illetve kötelező részvétel biztonságtudatosság képzésen,

c) mobil eszköz használatának korlátozása (a felhasználható keret ideiglenes csökkentése, az adatforgalmi szolgáltatás ideiglenes felfüggesztése);

d) a mobil eszköz használatának teljes korlátozása (a használati engedély visszavonása);

e) ismételt és súlyos szerződésszegés esetén a szerződésszegésre vonatkozó jogkövetkezmények alkalmazása.

(15) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) által alkalmazott ellenőrzési eljárás elemei:

a) személyek kiválasztása:

aa) alapelv, hogy egy teljes ellenőrzési periódus alatt az ellenőrzésben az Intézmény minden felhasználója érintett legyen;

ab) azon felhasználó, aki fennakadt egy ellenőrzésen, legközelebb 2 (kettő) hónap múlva kerülhet újra sorra;

ac) azon felhasználó, aki az előző ellenőrzésén átment, legközelebb 6 (hat) hónap múlva kerülhet újra sorra;

b) kötelező ellenőrzési elemek:

ba) felhasználói fiók jelszóvédelmének az állapota;

bb) időzített jelszavas képernyőzár állapota;

bc) saját használatú eszköz esetén a vírusvédelem állapota (aktív-e a védelem, megfelelően működik-e, ellenőrzi-e az eszközre csatlakoztatott eszközöket);

bd) a személyes használatra kiadott mobil telefon PIN kód használatának ellenőrzése;

be) telepített programok használata (engedélyezettek-e);

c) egyéb ellenőrzési elemek:

ca) csatlakoztatott eszközök jogosultsága;

cb) mobil adathordozókon (pendrive, mobiltelefon, fényképezőgép adatkártyája) tárolt munkahelyi adatok kötelező jelszóvédelme.

(16) Az alkalmazott eljárás menete a (15) bekezdésben meghatározottakra elemeire vonatkozóan:

a) Az eljárás a felhasználó eszközein kizárólag a felhasználó jelenlétében végezhető.

b) Az ellenőrzés során a vizsgálat elemekről olyan jegyzőkönyv készül, amely alapján bizonyíthatóan és egyértelműen eldönthető a vizsgált elem működése (pl. képernyőkép készítése).

c) Minden vizsgálat során a kötelező elemek mellett a felhasználó eszközhasználati szokásai (pl. pendrive használat, illetve engedély) alapján egyéb ellenőrzési elemek is ellenőrzésre kerülnek.

d) A jegyzőkönyvet a vizsgálatot végző személynek és a felhasználónak is aláírásával el kell látnia. A felhasználó aláírásával a jegyzőkönyv tartalmát és annak következtetéseit elfogadja.

e) A felhasználó a jegyzőkönyv tartalmával, következtetésével, illetve az eljárás menetével kapcsolatos kifogásait a jegyzőkönyv felvételekor, illetve utólag az Intézmény informatikai feladataiért felelős munkatársánál/ az informatikai feladatok ellátásáért felelős egység vezető munkatársánál jelezheti.

f) A vizsgálat eredményét a vizsgálatot végző szervezeti egység saját nyilvántartásában vezeti, amely tartalmazza a vizsgálat eredményét és a következő legkorábbi lehetséges ellenőrzés időpontját.

g) A vizsgálat eredményéről a vizsgálatot végző szervezeti egység vezetője értesíti a

ga) felhasználót;

gb) az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egységet, amely a teljes nyilvántartásért (résznyilvántartások összesítéséért) felel.

h) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa értesíti az intézményvezetőt a vizsgálat eredményéről, amennyiben a vizsgálat szabálytalanságot talál és a felhasználó legalább a második alkalommal akad fenn az ellenőrzésen.

(17) Az Intézmény informatikai hálózatában az internet kijárat védelme érdekében biztonsági és védelmi megoldásokat kell alkalmazni.

(18) A biztonsági megoldások során gondoskodni kell a hálózat fizikai elemeinek védelméről:

a) a vezetékek és végpontok illetéktelenek általi hozzáférésének megakadályozásáról;

b) vezeték nélküli kapcsolatok megfelelő titkosításáról;

c) vezeték nélküli kapcsolódások megfelelő felügyeletéről és kezeléséről (pl. a kapcsolódó eszközök fizikai címének ellenőrzéséről és azok engedélyezéséről vagy tiltásáról);

d) eszközhöz való illetéktelen hozzáférés megakadályozásáról.

Az a)-d) pontokban leírt védelem megvalósítása az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatársnak) feladata.

(19) Tilos a számítógépekre olyan alkalmazásokat telepíteni és futtatni, amelyek a felhasználó billentyűleütéseit naplózza. Ennek szúrópróbaszerű ellenőrzése az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatársnak) feladata.

(20) A (19) bekezdésben megjelölt program telepítése és futtatása, illetve ezen információk bármilyen felhasználása jog- és szabályellenes.

32. (1) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység gondoskodik az Intézmény informatikai rendszereinek behatolás elleni védeleméről (tűzfal), az erre vonatkozó szakmai előírások és a biztonsági szabályok betartása mellett.

(2) A központi informatikai rendszereket automatikus vírusvédelmi rendszerrel kell ellátni, amelyek üzemeltetését és felügyeletét külső partnerekkel együttműködve az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység látja el.

(3) Szerverek esetén alkalmazandó vírusvédelmi eljárások:

a) Minden szerverhez, amelyhez kereskedelmi forgalomban beszerezhető vírusvédelmi szoftver kell beszerezni, és telepíteni. Biztosítani kell, hogy a szerveroldali vírusvédelmi szoftver, víruskereső motor és vírusminta adatbázisa automatikusan frissüljön.

b) A levelező szerver esetében a levelezésért felelős alkalmazásba beépülő, a levélforgalom vizsgálatát végző vírusvédelmi szoftvert kell alkalmazni.

(4) Az elektronikus levelezés biztonsági irányelveinek érvényesítéséről a levelező rendszer üzemeltetője felelős. Az irányelvek a következők:

a) a folyamatos üzembiztonság megvalósítása;

b) az elektronikus küldemények adatintegritásának megtartása;

c) a levelezőrendszer vírusvédelmének biztosítása és folyamatos frissítése;

d) az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelme (szoftverfrissítések, service packok – javító csomagok – és security-patch –biztonsági javítás – fájlok telepítése).

33. (1) Az Intézményben informatikai hálózatot, illetve vezetékes vagy mobil internet kapcsolatot csak az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység engedélyezhet, hagyhat jóvá és hozhat létre.

(2) A használatra kapott számítógép rendszerszintű beállításainak – ideértve az irodai programok felhasználói beállításait is – módosítása nem engedélyezett. (3) A felhasználónak tilos a vírusvédelmi programot inaktívvá tenni, a beállításokat megváltoztatni, a vírusvédelmet eltávolítani.

(4) A vírussal fertőzött fájlt vagy elektronikus adathordozót bármilyen formában továbbítani, továbbadni, illetve fertőzött állománnyal munkát végezni szigorúan tilos.
(5) Az Intézmény informatikai rendszerébe és informatikai eszközén csak azt a szoftvert szabad telepíteni és használni, amelyik:
a) az Intézmény által jóváhagyott, telepítésre kiadott és engedélyezett nyílt forráskódú szoftver, vagy
b) szerzői jog szerint biztosított licencigazolással, illetve más jogi igazolással rendelkező, illetve tulajdonosi vagy felhasználási szerződéssel biztosított hivatalos forrásból származó jogtiszta szoftver.

5. A HR erőforrásokra vonatkozó biztonsági szabályok

34. Jelen szabályzat hatálya alá eső személyekre a következő, általános kötelezettségek érvényesek:
a) az informatikai rendszerek használata csak hivatalos célokra engedélyezett;
b) a használt informatikai eszközpark kezelésével kapcsolatos kezelési és biztonsági ismereteket el kell sajátítani, és készség szintjére kell fejleszteni;
c) a rendszerekbe csak szabályszerűen, a személyes felhasználó-azonosító kóddal szabad bejelentkezni;
d) az informatikai rendszerekben csak azokat a feladatokat szabad elvégezni, amelyek a felhasználó vagy üzemeltető munkájának ellátásához szükségesek, függetlenül attól, hogy a rendszer esetleg ennél szélesebb körű tevékenységet enged meg;
e) minden személynek biztosítania kell, hogy felhasználó-azonosítóját más felhasználók ne tudják használni;
f) a képernyőket, nyomtatókat úgy kell elhelyezni, hogy azok minél kevesebb lehetőséget biztosítsanak illetéktelen betekintésre;
g) az Intézmény által rendszeresített biztonsági funkciókat (pl. az automatikus képernyővédő-aktiválás) kikapcsolni, megkerülni tilos;
h) az Intézmény eszközein csak a Főigazgatóság által engedélyezett eszközöket és programokat szabad használni;
i) tartózkodni kell minden olyan tevékenységtől, amely az informatikai rendszerben kárt okoz a biztonság, a sértetlenség és teljesítmény terén;
j) az információtechnológiai biztonságra és az adatvédelemre vonatkozó minden egyéb utasítást és jogszabályt maradéktalanul be kell tartani;
k) esetleges meghibásodás esetén törekedni kell a további károsodás megelőzésére (a hiba jelentésével, a további használat mellőzésével, stb.);
l) a felhasználónak vagy üzemeltetőnek ismernie kell a segítségkérés és hibajelentés módját, amennyiben ez az ismeret nem áll rendelkezésére, hiba esetén értesítenie kell a munkahelyi vezetőjét, külső személyek esetén az Intézmény kijelölt kapcsolattartóját;
m) az informatikai biztonságot veszélyeztető eseményről vagy ennek gyanújáról értesíteni kell az informatikai biztonsági referenst, informatikust és a munkahelyi vezetőt, külső személyek esetén az Intézmény kijelölt kapcsolattartóját;
n) a közvetlen munkahelyi vezető (külső személyek esetén az Intézmény kijelölt kapcsolattartója) a felelős azért, hogy a fenti szabályokat az érintettekkel ismertesse.

35. (1) A felhasználó, illetve informatikus a számítógépre csak saját nevében és jelszavával léphet be, illetve az alkalmazásokat csak saját nevében használhatja. Amennyiben az Intézmény informatikai rendszere nincs ellátva központi címtárral, úgy a számítógépeken ki kell alakítani a kötelezően jelszóval védett lokálisan kialakított felhasználói környezetet. Előbbiektől eltérően csak indokolt esetben, az illetékes szervezeti egység vezetőjének kérésére és az intézményvezető egyedi írásos engedélyének birtokában lehet eljárni.
(2) A jelszó érvényességi idejét, ezzel együtt a jelszócsere gyakoriságát az informatikai rendszer központi szabályozása vagy a használt rendszer működése határozza meg. A jelszó cseréjét ezen értesítés hiányában legalább 90 (kilencven) naponta kötelező elvégezni. Ha az informatikai

rendszer lehetővé teszi, törekedni kell arra, hogy a jelszócsere kikényszerítésre kerüljön, illetve a felhasználó e-mailes értesítést kapjon a jelszócsere szükségességéről.
(3) A felhasználó jelszókezelési szabályai:
a) jelszavak nem hozhatók nyilvánosságra;
b) a jelszavak biztonságának megőrzéséért a felhasználó személyesen felel;
c) a felhasználó a jelszavát nem oszthatja meg senkivel;
d) ha a felhasználónak a legkisebb gyanúja is felmerül, a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az informatikai biztonsági referenst, valamint az Intézmény informatikai feladataiért felelős munkatársát/ az informatikai feladatok ellátásáért felelős egységet értesíteni;
e) más felhasználó azonosítóját átmeneti jelleggel sem szabad használni;
f) a felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.

36. (1) A szakmai feladatok hatékony ellátásához szükséges információkhoz, szolgáltatásokhoz való hozzáférés érdekében az Intézmény valamennyi felhasználója jogosult a munkahelyi internet és elektronikus levelezés használatára.
(2) Az internet szolgáltatásait a munkahelyi eszközökön (azaz Intézmény által biztosított eszközökön) alapvetően a munkaköri feladatok ellátására lehet igénybe venni, a személyes célú használat kizárólag munkaközi szünetben megengedett.
(3) Minden weblap illetve internetes szolgáltatás elérése engedélyezett, amíg annak tartalma nem ütközik semmilyen jogszabályi előírásba. Ez alól kivételt jelentenek a különböző felhő-alapú informatikai szolgáltatások, amelyek kizárólag az informatikai biztonsági referens által, a 2013. évi L. törvényben foglaltak alapján véleményezettek és engedélyezésre javasoltak, s az intézményvezető által, külföldi felhő-alapú szolgáltatás esetén a Nemzeti Elektronikus Információbiztonsági Hatóság (továbbiakban: NEIH) által engedélyezett.
(4) Tekintettel arra, hogy az internethasználat az Intézmény által biztosított infrastruktúrán, illetve szolgáltatási költségen valósul meg, az Intézmény jogosult bármikor bármilyen weblap, internetes szolgáltatás elérésének ideiglenes vagy teljes korlátozására. Ezen weboldalak nem ütköznek semmilyen jogszabályi előírásba, letiltásuk a hálózat leterheltségének kezelhetőségére, a munkaidő hatékony kihasználására irányul. A külföldi felhő-alapú informatikai szolgáltatásokat a NEIH engedély kiadásáig az internet elérését biztosító informatikai berendezéseknek fő szabály szerint tiltani kell.
(5) A hálózat számára nagy terhelést jelentő kép- (pl. grafikus fájl, video) és hang- (pl. *.mov, *.mp3, *.avi, *.wav. stb.) információkat tartalmazó anyagok letöltése, továbbítása csak az intézményvezetővel előzetesen egyeztetve engedélyezett.
(6) A felhasználók az Intézmény nevében nem tölthetnek fel engedély nélkül az internetre adatot és anyagot (pl. honlap, hirdetmények).
(7) Az Intézmény tulajdonát képező szoftverek interneten vagy e-mailen keresztül történő továbbítása, mások részére való hozzáférhetővé tétele – előzetes külön engedély hiányában – nem engedélyezett.
(8) Az Intézmény felhasználóira az interneten történő viselkedésre, megnyilvánulásokra – tekintet nélkül az intézménnyel megkötött munkavégzésre irányuló jogviszony típusára – a Zöld Könyvben[1] – Az állami szerveknél érvényesítendő etikai követelményekről – megfogalmazott alapelvek érvényesek.
(9) Tiltott tartalmú oldalak:
a) szexuális tartalmú oldalak, különösen az alábbi tartalmakkal:
aa) kiskorúak veszélyeztetése;
ab) erőszak;
ac) pornográfia;
ad) marketing molesztáló jellegű formái (felhívás ilyen jellegű oldalak látogatására).
b) az emberi méltóság megsértése;
c) rasszizmus;

[1] http://korrupciomegelozes.kormany.hu/download/e/0b/60000/Z%C3%B6ld.pdf

d) szexuális beállítódás, vallás, nemzetiség vagy etnikai származás miatti megkülönböztetés;
e) gazdasági bűnözés fogalma alá eső cselekmények. veszélyeztetése;
f) csalás;
g) tiltott kereskedelmi tevékenység;
h) hitelkártyával való visszaélésben való közreműködés;
i) rémhírterjesztés;
j) információbiztonság veszélyeztetése;
k) rossz szándékú hackertámadás;
l) hacker, cracker technológiák és leírásuk, eszközök terjesztése, használata;
m) vírusprogramok terjesztése, írása;
n) a magánszféra megsértése;
o) személyes adatokkal való visszaélés;
p) elektronikus zaklatás;
q) a személyiségi jogok megsértése;
r) rágalmazás;
s) meg nem engedett összehasonlító reklám;
t) a szellemi tulajdon megsértése;
u) tiltott szerencsejáték;
v) a szerzői jog által védett digitális anyagok (művek, szoftverek, zenék stb.) jogosulatlan terjesztése;
w) bombák készítéséhez adott segítségnyújtás;
x) illegális kábítószer használat, előállítás és terjesztés;
y) nemzetbiztonsági kérdések;
z) terrorista tevékenység.

(10) A tiltott tartalmú oldalak tiltása tartalomszűrő megoldással történik. A tartalomszűrő működésének biztosítása és a szűrő szükség szerinti bővítése az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) feladata.

(11) Amennyiben a felhasználó az internetes portálok használata közben véleménye szerint olyan oldalt ér el, amely a (9) bekezdésben felsorolt tartalmú oldal valamely kritériumának megfelel, a szervezeti egység vezetőjének javasolhatja, hogy az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) együttműködését kérve módosítsa a tiltott tartalmú weboldalak listáját, így biztosítva a sértő tartalom elérhetetlenségét.

(12) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység, vagy az informatikai referens munkakörben foglalkoztatott munkatársa köteles meghatározott időközönként – de legalább 3 (három) havonta – a tiltólistákat felülvizsgálni az internetes forgalmi adatok birtokában. Ezeket az adatokat nem lehet személyhez kötni. Amennyiben nincs birtokában, úgy jogosult a szolgáltatótól az internetes forgalmi adatok lekérdezésére. A vizsgálat eredményéről és a javasolt intézkedések megtételéről az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa tájékoztatja az intézményvezetőt, aki dönt a szükséges intézkedésekről.

(13) A tiltott weboldalak listáján szereplő internetes oldal megnyitásának kísérlete nem minősül szabálysértésnek, mivel az nem ütközik semmilyen morális, erkölcsi illetve törvényi szabályba.

37. (1) Az Intézmény elektronikus levelezőrendszert biztosít a szervezete, illetve az Intézménnyel munkaviszonyban álló felhasználók részére, amelyet alapvetően a hivatalos munkavégzéshez biztosít. Az elektronikus levelezőrendszer lehet saját üzemeltetésű, illetve külső szolgáltató általi szolgáltatásként biztosított.

(2) Az elektronikus levelező rendszerben megjelenő információk, dokumentumok, elektronikus levelek az Intézmény tulajdonát képezik, figyelembe véve a személyes adatok kezelésére vonatkozó hatályos adatvédelmi szabályokat, eljárásokat.

(3) Az Intézmény által a felhasználó részére biztosított, a munkavégzését segítő elektronikus levelező postafiókot magáncélra használni bizonyos feltételekkel, formai követelményekkel engedélyezett.
(4) A magáncélú leveleket a postafiók könyvtárstruktúrájában láthatóan el kell különíteni a felhasználó által folytatott hivatalos levelezéstől (Magánlevelezés nevű könyvtárba a Beérkezett Üzenetek, illetve az Elküldött Üzenetek könyvtáraktól elkülönítve), a küldött és fogadott levelek fejlécét el kell látni a „[PRIVATE]" (azaz magáncélú) megjelöléssel. A megjelölés alapján az elektronikus levelet megilleti a levéltitok védelme.
(5) A magáncélú levél nem tartalmazhatja az Intézmény hivatalos elektronikus levélhez kötött aláírását.
(6) Az adatbiztonság, illetve az információs rendszer védelme okán az Intézmény informatikai hálózatát üzemeltető Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) munkatársai – például abból a célból, hogy a védett rendszerbe ne kerülhessen be vírus – jogosultak a magáncélú levél tartalmába betekinteni, azonban a megismert adatokat harmadik fél számára – így a munkáltató részére – nem jogosultak továbbítani. Amennyiben az ellenőrzést végző a magáncélú levelezésben veszélyes tartalmat talál, úgy a működtetett informatikai rendszerrel kiszűrt tartamú elektronikus levelet karanténba helyezi és erről a felhasználót értesíti.
(7) A (4) bekezdésben megjelölt könyvtárban található elektronikus levelek fejlécét tartalmazó listát az Intézmény gazdálkodási feladatait ellátó szervezeti egysége és a Belső Ellenőrzésért felelős szervezeti egysége által indított vizsgálat keretében bármikor lekérhetik, annak tartalmát az Intézmény adatvédelmi és adatkezelési szabályzatának alapján tárolja.
(8) Az Intézménytől távozó felhasználó postafiókjának archiválásáról, megszüntetéséről, valamint a megszüntetéséig a betekintési jogosultak köréről a távozó felhasználó szervezeti egység vezetője jogosult dönteni, ez alól kivétel a felhasználó által elkülönített, magáncélú levelezését tároló könyvtár.
(9) A felhasználó távozásakor az Intézmény adatvédelmi felelőse jogosult a felhasználó magáncélú leveleit tartalmazó könyvtár leveleinek fejlécét tartalmazó lista megtekintésére, ellenőrizve hogy azok megfelelnek-e a magáncélú felhasználásra jelölésnek és így a levelek kezelhetőek-e magáncélúnak. Az ellenőrzés eredményéről a távozó felhasználó szervezeti egység vezetőjét tájékoztatja, aki a (8) bekezdés alapján dönt a távozó felhasználó postafiókjának kezeléséről.
(10) A felhasználó postafiókjának teljes vagy részleges tartalma a felhasználótól elkérhető, illetve szükség esetén az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység bevonásával lekérhető az alábbi körülmények fennállásakor:
a) a Belső Ellenőrzésért felelős szervezeti egység, valamint
az Intézmény gazdálkodási feladatait ellátó szervezeti egysége által folytatott eljárások esetén az eljárás lebonyolításához szükséges információk megszerzésére vonatkozóan:
aa) a vizsgálat célzott, így az adatok bekérése is (vizsgált időperiódus vagy egyéb konkrét feltétel);
ab) első lépésben a postafiók leveleinek fejlécét, a fejléci információk alapján pedig a vizsgálatot végző szervezeti egység a vizsgálat céljának megfelelően kiválasztott levelek nyomtatott verzióját, beleértve a levél mellékleteit is;
ac) a levelezésből kinyert információk kezelésére, tárolására és megsemmisítésére a szervezeti egységek belső szabályai, valamint a Főigazgatóság adatvédelmi és adatkezelési szabályai az irányadóak;
b) külső nyomozati szerv által történt nyomozati cselekménybe való részvétel, hivatalos megkeresése esetén a nyomozati szerv által kért részletességgel – csak fejléc, nyomtatott forma (mellékletekkel), elektronikus másolat– .
(11) Az Intézmény levelezőrendszeréből küldött magánlevelezéshez kapcsolódó viselkedésre, megnyilvánulásokra a 36. pont (8),(11) és (12) bekezdéseiben foglaltak az irányadók. A hivatkozott szabályok megszegésének gyanúja esetén a magáncélú levelezések a Belső

Ellenőrzésért felelős szervezeti egység, illetve az Intézmény gazdálkodási feladatait ellátó szervezeti egysége által indított vizsgálatra korlátozások nélkül, teljes tartalommal átadhatóak.
(12) Az elektronikus levelezés során a postafiókokat vírusvédelmi rendszer védi. Az elektronikus postafiókba érkező, ismeretlen feladótól (gyanús, értelmezhetetlen vagy külföldi) származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldeményekkel – a fennálló vírusveszély miatt – fokozott óvatossággal kell eljárni. A gyanús küldemény érkezésekor, illetve a vírusvédelmi rendszer riasztása esetén haladéktalanul értesíteni kell az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység munkatársait vagy az intézményvezető által erre megbízott személyt. A csatolmányt ilyen esetben tilos megnyitni.
(13) A felhasználó elektronikus levelezési címével beregisztrálni bármely, az interneten lévő webes rendszerbe, illetve külső szervezet rendszerébe csak szakmailag indokolt esetben és a közvetlen vezetője hozzájárulásával engedélyezett.
(14) Tilos lánclevelek indítása vagy továbbítása.

38. (1) Az Intézmény a mobiltelefon használatának rendjéről szóló szabályzatában elfogadott elvek szerint az Intézmény munkatársai számára mobiltelefon elérhetőséget biztosíthat.
(2) A mobil szabályzatban előírt felhasználási keretösszeget a felhasználó hivatalos és személyes célra használhatja. A hívások listáját nem kérhető le.
(3) A mobiltelefonról indított internetezési szabályokra a jelen szabályzat 36. pontja megfelelően irányadó, azzal a kiegészítéssel, hogy a mobiltelefonon alapesetben nincsenek korlátozott weboldalak. A weboldalak korlátozását az intézményvezető utasítására az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység a mobiltelefon szolgáltatónál igényelheti, akár telefonszámra, akár időszakra vonatkozóan. A weboldalak elérése csak a munkaidő tartamára korlátozható, azzal, hogy a munkaidő tartamára sem korlátozhatóak jelen szabályzat 36. pont (4) és (5) bekezdésében meghatározott weboldalak, illetve tartalmak.
(4) A mobiltelefonról indított internetes forgalom listája nem kérhető le.
(5) A mobiltelefon tárolókapacitása mind hivatalos, mind személyes célra felhasználható, azzal a megkötéssel, hogy hivatalos dokumentumot kizárólag jelszavas védelemmel ellátva (megnyitási, illetve szerkesztési jelszóval védve) lehet tárolni. A jelszavas védelem használatáért a felhasználó teljes felelősséggel tartozik.
(6) Azok a mobiltelefonok, amelyek bármilyen, az Intézményhez köthető adatot, információt tartalmaznak (hivatali végleges, illetve munkadokumentum, fénykép, hivatali elektronikus levelezés), kizárólag a 31. pont (6) és (7) bekezdésében leírt jelszavas, illetve időzáras billentyű- vagy képernyőzárral használhatóak.
(7) A (6) bekezdésben leírt biztonsági elemek meglétének ellenőrzése jelen szabályzat 31. pont (12) bekezdésében foglaltakkal megegyezően történik és annak megszegése a 31. pont (14) bekezdésében leírtak szerint szankcionálható.

39. (1) Az új belépő dolgozót az illetékes szervezeti egység vezetője utasítja a szükséges informatikai biztonsági szabályok megismerésére, illetve tájékoztatja az informatikai szabályzatok elérhetőségéről. Az informatikai szabályzatok megismerésének tényét a dolgozó aláírásával igazolja.
(2) Minden felhasználó köteles a vonatkozó informatikai-szakmai szabályzatokat megismerni és betartani, illetve köteles ezek betartása során az informatikai rendszer használatát irányító személyekkel együttműködni.

6. Az informatikai biztonsági incidensek kezelése

40. (1) Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható), bármilyen bekövetkezett, vagy előre látható biztonsági eseményt (betörés, lopás, tűz, víz, villámcsapás, balesetveszélyes eszköz, eszköz elvesztése vagy eltűnése stb.) az intézményvezető (vagy az általa ezzel megbízott munkatárs) felé az eseményt észlelőnek azonnal jelezni kell.

(2) A felhasználó köteles jelezni az intézményvezetőnek (vagy az általa ezzel megbízott munkatársnak) bármely, az informatikai biztonságot érintő gyanús eseményt (például az előző nap lekapcsolt, de reggel bekapcsolva talált gépet), vagy ezzel kapcsolatos gyanúját.

41. Az informatikai rendszereket érintő (vagy vele összefüggésbe hozható) biztonsági eseményeket az alábbi módon kell bejelenteni:
a) felhasználói hiba észlelés esetén haladéktalanul értesíteni kell telefonon vagy személyesen az intézményvezetőt (vagy az általa ezzel megbízott munkatársat);
b) biztonsági esemény esetén haladéktalanul telefonon értesíteni kell az intézményvezetőt, aki az esemény jellegétől függően intézkedik.
Az eseményt követően az eseményről jegyzőkönyvet kell készíteni, és azt az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység részére írásban elküldeni (e-mail, levél). A jegyzőkönyvben rögzíteni kell az esemény részleteit, körülményeit.

42. Az informatikai rendszer bármely felhasználói pontján jelentkező, a hálózattal, eszközzel, illetve adott alkalmazással kapcsolatban felmerülő rendellenes működés, jelenség, vírusjelzés, futtatási hiba esetén a felhasználó köteles a tapasztalt jelenséget, és ha van, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul bejelenteni az informatikai biztonsági referensnek.

43. Az informatikai biztonsági referens a biztonsági incidenst kivizsgálja és az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység, illetve a kijelölt informatikus bevonásával intézkedést, illetve ezzel párhuzamosan szükség szerint változtatást javasol jelen szabályzat vonatkozásában. Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa, illetve az intézményvezető által kijelölt informatikus a hiba elhárítása érdekében intézkedik, illetve a probléma elhárítását elvégzi, a hiba megszüntetéséről és a további teendőkről a felhasználót pedig folyamatosan tájékoztatja, valamint helyettesítő eszköz biztosításával gondoskodik a felhasználó munkavégzési lehetőségéről.

44. (1) Az informatikai rendszer rendellenes működése vagy a biztonságot veszélyeztető esemény elhárítása érdekében az informatikai eszközök használatát, a hálózat működését, az internet és levelezés használatát az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység kezdeményezése esetén az intézményvezető részben vagy egészében korlátozhatja vagy leállíthatja.
(2) Jelen szabályzat 37. és 38. pontjában leírt internethasználat és elektronikus levelezés szabályainak a felhasználó általi megszegése esetén a jelen szabályzat 31.pont (14) bekezdésében megfogalmazott szankciók alkalmazhatók.
(3) A szabályzat szándékos, vagy gondatlan megszegését az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa a vizsgálatok eredményével és a javasolt szankcióval együtt tájékoztatja az intézményvezetőt.

7. A fizikai és környezeti infrastruktúra biztonsága

45. (1) Az informatikai infrastruktúra elemeinek és a helyiségeknek a kockázatokkal és a tágabb értelemben vett értékükkel arányos fizikai védelmet kell biztosítani.
(2) Informatikai helyiségeknek minősülnek azon helyiségek, amelyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak, kivételt képeznek azon egyéb helyiségek, amelyekben zárt, kulccsal biztosított rack szekrény található.
(3) Az informatikai helyiségekbe való belépési jogosultságot személyre szólóan, az adott személy feladata alapján kell meghatározni. Állandó vagy egyedi belépési jogosultságot az informatikai helyiségbe az intézményvezető adhat.

46. (1) A belépési jogosultsággal nem rendelkezők az informatikai helyiségben csak az arra jogosultak felügyelete mellett tartozódhatnak.

(2) Abban az esetben, ha az informatikai helyiségbe (pl. szerverszoba) valamilyen okból (szemle, ellenőrzés, szerelés, stb.) belépési jogosultsággal nem rendelkező személynek be kell jutni, arról előzetes egyeztetés mellett a kijelölt informatikus gondoskodik.
(3) Tilos az informatikai helyiségben a helyiség funkciójától eltérő anyag vagy eszköz tárolása.
(4) Az informatikai helyiségek számítógépeire telepített szoftverek karbantartását a kijelölt informatikusok végzik.

47. (1) Az informatikai eszközök nyilvántartásáért Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) tartozik felelősséggel. A kijelölt informatikus az eszközöket az informatikai eszköznyilvántartásban tartja nyilván és a változásokat lehetőség szerint azonnal, de legkésőbb 3 (három) napon belül aktualizálja.
(2) Az eszközökön (a számítógépeken, laptopokon és a mobil eszközökön) a kötelező biztonsági elemek (jelszó, időzáras képernyőzár, stb.) beállítása (központi- vagy helyi szabályozással) az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) feladata.
(3) Az eszközök átadásának-átvételének megtörténte feltételezi a biztonsági elemek meglétét és a felhasználó tudomását ezen biztonsági elemek kötelező használatáról, így a felhasználó az eszközért és annak biztonságos használatáért objektív felelősséggel tartozik.

48. (1) Az eszközök teljes életciklusa alatt kötelező azok nyilvántartása, és mozgásuk dokumentálása (üzembe helyezési dokumentum, átadás-átvétel nyomtatvány, szállítók, selejtezési bizonylat). Az informatikai berendezéseket, eszközöket fizikai valójukban is védeni kell a biztonságot fenyegető veszélyektől és a káros környezeti hatásoktól.
(2) A környezeti veszélyek és kockázatok mérséklése érdekében:
a) a berendezéseket úgy kell elhelyezni, hogy lehetőleg megakadályozzák az illetéktelen hozzáférést;
b) a különleges védelmet igénylő, fokozott és kiemelt biztonsági osztályba tartozó eszközöket elkülönítetten kell elhelyezni és használni;
c) a környezeti hatások és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével törekedni kell a szükséges működési feltételek biztosítására.
(3) Az informatikai eszközök rendeltetésszerű használatáért a számviteli leltárban az eszköz használójaként kijelölt alkalmazott a felelős, vagy az a személy, aki vezetői utasításra és engedéllyel azt használta. Közös használatú eszköz esetén az eszközök rendeltetésszerű használatáért, az a személy a felelős, akit a vezető adott esetben kijelölt az eszköz felügyeletére (csoportvezető, ügyeletes, munkafelelős stb.).
(4) A munkája során számítógépet használó felhasználó köteles az általa működtetett számítógépet és az ahhoz csatlakoztatott eszközöket:
a) a rendeltetésnek megfelelően, munkavégzés céljából, szakszerűen, az Intézmény érdekeit szem előtt tartva jelen szabályzatban meghatározott módon használni;
b) kikapcsolni, ha előre láthatóan hosszabb – 4 (négy) órát meghaladó – ideig nem használja (pl. értekezlet, megbeszélés, tárgyalás).
(5) Az informatikai eszközök használata során tilos:
a) az eszközt illetéktelen személynek átengedni;
b) az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni;
c) az eszközt a telepítési helyéről elmozdítani és elvinni a kijelölt informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök).
(6) Az informatikai eszközökhöz bármilyen külső eszközt, illetve kábelt csatlakoztatni csak a kijelölt informatikus engedélyével vagy közreműködésével lehet. Az informatikus által már csatlakoztatott és beüzemelt eszköz további használata visszavonásig engedélyezett (pl. pendrive, fényképezőgép).
(7) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) az engedélyezett, illetve tiltott informatikai eszközök szabályozását központilag illetve

manuálisan, az operációs rendszerbe beépített házirendekkel szabályozza, így biztosítva a (6) bekezdésben foglaltakat.
(8) Címkét, jelölést, feliratot csak a kijelölt informatikus helyezhet el az informatikai eszközökre, illetve távolíthat el onnan. Az eszközök burkolatát megbontatni tilos. Alkatrészt csak a kijelölt informatikus helyezhet be az eszközbe, illetve szerelhet ki az eszközből.

49. (1) Az informatikai eszközök a vonatkozó szabványnak megfelelően kizárólag védőföldeléssel ellátott 230 V feszültségű elektromos hálózati dugaszoló aljzatba csatlakoztathatók.
(2) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) feladata törekedni arra, hogy a szervezeti szintű alkalmazások működését befolyásoló informatikai és távközlési eszközök (pl. szerverek, rack szekrény stb.) szünetmentes tápegységekkel legyenek ellátva.

50. Az Intézmény területén az informatikai rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatárs) tájékoztatása után, annak jóváhagyásával, és felügyeletével lehet végezni.

51. Az informatikai eszközök és berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében:
a) a specifikációban javasolt időközönként el kell végezni a berendezések karbantartását;
b) a berendezések kezelését, illetve javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik;
c) az informatikai eszközök külső helyszínen történő javítása, karbantartása esetén gondoskodni kell az eszközön tárolt adatok végleges (visszaállíthatatlan) törléséről, vagy az adathordozó eltávolításáról.

52. (1) A mobil informatikai eszközről az arra felhatalmazott személy részére történő átadásakor az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység kijelölt informatikusa, vagy az intézményvezető által kijelölt felelős tárolási nyilatkozatot készít, amely tartalmazza az eszköz műszaki adatait, az átadás-átvétel adatait és az eszközön telepített szoftverek adatait.
(2) A felhasználó köteles a mobil informatikai eszközt lehetőleg hetente (, de hosszabb távollét esetén lehetőleg havonta) az Intézmény hálózatához csatlakoztatni abból a célból, hogy a biztonsági és vírusvédelmi frissítések települhessenek, megőrizve ezzel a biztonság integritását.
(3) A mobil eszközöket használó személyeknek:
a) kötelező a SIM kártya PIN kódos védelem, illetve az időzáras és kizárólag jelszóval, PIN kóddal vagy mintával feloldható képernyőzár használata, amennyiben a telefonon működő operációs rendszer rendelkezik erre alkalmas funkcióval (általános védelem);
aa) a felhasználó jelen szabályzat 47. (3) bekezdésében foglaltaknak megfelelően a biztonsági elemek kötelező használatát tudomásul vette és teljes felelőssége mellett használni is köteles azokat.
ab) az a) pontban meghatározott kötelező biztonsági elemek ellenőrzése a jelen szabályzat 36. pont (5) és (6) bekezdésében foglaltaknak megfelelően történik;
ac) a biztonsági elemek használata alól nem mentesül az, aki nem esett még jelen szabályzatban meghatározott ellenőrzés alá;
b) nem engedélyezett az eszközt gépjárműben, idegen helyen felügyelet nélkül hagyni;
c) a repülés, vagy vonatút alatt a mobil informatikai eszközt kézipoggyászként kell szállítani;
d) az Intézmény területén kívül, idegen helyen történő tárolás esetén (szálloda, lakás) fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemre;
e) nem engedélyezett az eszköz engedély nélküli átruházása vagy adatainak közlése;

f) nem engedélyezett megfelelő védelem nélkül idegen hálózathoz csatlakoztatni az eszközt, pl. jelszó nélkül elérhető vezeték nélküli (Wi-Fi) hálózatok;
g) a mobil eszköz átadása más felhasználó (vagy illetéktelen személy) részére szándékos gondatlanságnak minősül és a felhasználó teljes felelősségét vonja maga után (a mobil eszköz átvételével objektív felelőssége keletkezett a felhasználónak az Intézménnyel szemben);
h) nem engedélyezett a gépet bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.
(4) A kódolatlan mobil adathordozó eszközök rendkívül nagy kockázati veszélyforrást jelentenek, ezért a felhasználók ezeket csak informatikai ellenőrzés mellett használhatják.
(5) A kódolatlan mobil adattárolókon hivatali adatokat, információkat tartalmazó dokumentumok kizárólag olvasási, illetve módosítási jelszóvédelemmel ellátva kerülhetnek tárolásra. A dokumentumok kódolásáért a felhasználó kizárólagosan felelős.
(6) Amennyiben az Intézmény hivatali használatra átadott adathordozót a felhasználó számára, úgy azon magánjellegű adatot tárolni nem engedélyezett. A hivatali adathordozón tárolt adatokért a felhasználó kizárólagos felelősséggel tartozik.
(7) Magánjellegű adathordozót hivatali célra használni engedélyezett, azonban hivatali adatot, dokumentumot kizárólag jelszóval védve lehet tárolni. Ebben az esetben kötelező a megnyitáshoz, illetve a szerkesztéshez jelszót rendelni. Az adatok, dokumentumok jelszóval való védettségéért a felhasználó kizárólagos felelősséggel tartozik.
(8) Az Intézmény informatikai rendszerébe kapcsolt munkaállomásokon csak olyan adathordozót lehet használni, arról adatokat beolvasni, amelyen előtte a rendszeresített és telepített víruskereső programmal vírusellenőrzést végeztek.
(9) A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért. A mobil infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét haladéktalanul jelentenie kell a szükséges intézkedések megtétele érdekében.
(10) A felhasználók egyes feladatok elvégzése érdekében, a részükre biztosított, nyilvántartott és egyedi azonosítóval ellátott, hivatali tulajdonú mobil adathordozóra kimenthetik a feladatukhoz kapcsolódó állományaikat.

53. (1) A megsemmisítésre kijelölt eszközöket és kellékanyagokat megsemmisítésig a használatban lévő eszközöktől elkülönítetten kell tárolni és kezelni figyelembe véve:
a) a veszélyes anyagok tárolására és a megsemmisítésre vonatkozó szabályokat (fizikai védelem, szállítás);
b) a leltározási és selejtezési szabályzat előírásait;
c) az adatvédelem biztonsági követelményeit (hozzáférés elleni védelem).
(2) Az olyan hivatali helyiségeket, ahol informatikai eszközökkel történik a munkavégzés vagy informatikai eszközt tárolnak, zárral kell ellátni és a helyiséget távollét esetén vagyonvédelmi és biztonsági okokból zárva kell tartani.
(3) Az informatikai berendezések végleges használaton kívül helyezése előtt gondoskodni kell az összes adat, szoftver visszaállíthatatlan eltávolításáról és felülírásáról, vagy a beépített adathordozó eltávolításáról (roncsolásáról) és megfelelő tárolásáról.
(4) A külső személy által javításra, megsemmisítésre elszállított informatikai eszközökből el kell távolítani a beépített adathordozót, ha ez nem megoldott, a külső személy arra felhatalmazott képviselője a külső személy nevében érvényes és joghatályos nyilatkozatot köteles tenni az adatvédelmi és titoktartási szabályok betartására vonatkozóan.

54. (1) Az intézményvezető gondoskodik:
a) a szerverek működéséhez szükséges megfelelő fizikai környezet biztosításáról;
b) a megfelelő elektromos hálózat, villám és túlfeszültség, valamint érintésvédelmi berendezések meglétéről és működésének biztosításáról;
c) a behatolás elleni védelem és riasztórendszer kialakításáról (pl: beléptető rendszer, elektromos behatolás jelző, mozgásérzékelő, belső térvédelem);
d) a megfelelő tűzvédelmi rendszerről:
e) füstjelző és riasztó rendszer kialakításáról,

f) automata tűzoltó rendszer kialakításáról, vagy kézi tűzoltó készülékek (elektromos berendezések tűzének oltására alkalmas gázzal oltó készülék) elhelyezéséről;
(2) Az informatikai objektumok közüzemi ellátását (áramellátás, fűtés, szellőzés, vízszolgáltatás stb.) a vonatkozó szabályzatok és hatósági előírások szerint kell biztosítani.
(3) A szerverszobában vizesblokk kialakítása nem engedélyezett. A szerverszobát védeni kell szennyvíz, illetve esővíz bejutása ellen. A kialakítás során törekedni kell arra, hogy a szerverszoba felett vizesblokk ne helyezkedjen el.

8. A hálózat- és rendszerüzemeltetés biztonsága

55. (1) A rendszer napi üzemeltetéséhez tartozik a működés felügyelete, a mentések elvégzése és hiba esetén az eszközök javítása.
(2) A rendszer üzemeltetését ellátó informatikusoknak ismerniük kell az Intézmény rendszereszközeinek, operációs rendszereinek, adatbázisainak működését, az operációs és alkalmazói rendszerek hibaüzeneteit és a behatolás detektáló rendszerfigyelmeztető üzeneteit, illetve tudniuk kell alkalmazni a szükséges reagálásokat tartalmazó leírást.
(3) A rendszer felügyelete a felhasználói programok és adatbázisok, a szerverek és alapszoftverek, valamint a hálózat működésének folyamatos figyelemmel kísérését kívánja meg. A felelős informatikai munkatársaknak rendszeresen el kell végezniük azokat a tevékenységeket, amelyek alapján meggyőződhetnek arról, hogy a rendszer üzemszerűen, normálisan működik.
(4) A rendszer valamennyi hardver, illetve szoftver eleméről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a szerverek, munkaállomások pontos és naprakész hardver konfigurációját, a működtető szoftverek egyedi beállításait és elhelyezkedését, illetve az értük felelős személy nevét.
(5) Az alábbi naprakészen vezetendő nyilvántartásokat szükséges elkészíteni:
a) szoftvernyilvántartás;
b) jogosultság nyilvántartás;
c) eszköz átadás-átvételi adatlap.
(6) Az üzembiztonság érdekében a szerverek operációs rendszereit (a beállításokkal együtt) lehetőség szerint tartalék adathordozón is tárolni kell, amely szükség esetén azonnal betölthető.

56. (1) Szoftvert a számítógépre csak kijelölt informatikus tölthet le, másolhat és telepíthet, valamint a számítógépről csak kijelölt informatikus távolíthat el.
(2) A felhasználó a munkaállomás használata során a munkaállomásra telepített alkalmazásokat használhatja. A felhasználó új alkalmazások telepítését vagy a meglévő alkalmazásokat illető jogosultságváltozást a szervezeti egység vezetője engedélyével igényelhet. Az intézményvezető (vagy az általa ezzel megbízott munkatárs) jogosult az igény felülvizsgálatára, és ha szükséges, biztonsági okból annak elutasítására.
(3) A felhasználó a számítógépre telepített alkalmazásokat a felhasználói leírás szerinti módon, szakszerűen köteles használni.
(4) Tilos a szoftvereket és adatokat harmadik fél számára másolni, illetve továbbadni. Előbbiek alól kivételt képez a szoftverekről és adatokról való biztonsági másolatok kijelölt informatikus által történő elkészítése, amely a rendelkezésre állás folyamatosságát hivatott biztosítani.
(5) A szoftverek adathordozóit, üzemeltetési és felhasználói dokumentációját, licenc dokumentációját az intézményvezető által megbízott munkatárs tárolja és tartja nyilván.

57. (1) A hibabejelentéseket a kijelölt informatikusok személyes, telefonos megkeresésével illetve vele párhuzamosan e-mailben lehet elvégezni.
(2) A kijelölt informatikus feladata, hogy szükség esetén gondoskodjon a szükséges hibaelhárításról, az eszköz javításáról, az eszköz helyettesítéséről, az eszköz szervizbe szállításáról.
(3) A kijelölt informatikus feladata, hogy tájékoztassa az érintett felhasználót az eszköz javítási folyamatáról, illetve sorsáról.
(4) Azokban az esetben, ha a hiba az Intézmény rendszereinek működésére komoly kihatással van (pl. üzembiztonságot veszélyeztető helyzet, katasztrófahelyzet áll fenn), vagy más jellegű, de

rendkívül fontos eset következik be (pl. bűncselekmény gyanúja áll fenn), az észlelő köteles haladéktalanul értesíteni az intézményvezető által megbízott munkatársat.

58. A külső üzemeltetői erőforrások (harmadik fél) bevonása esetén pontosan meg kell határozni a feladatok és a felelősségek megosztását, jelen szabályzatban meghatározott biztonsági követelmények rögzítése mellett.

59. (1) A hálózati végpontok és az azokra csatlakoztatott eszközök végpontvédelméről minden informatikai eszköz esetében gondoskodni kell. A védelem során gondoskodni kell, hogy:
a) illetéktelenek ne férjenek szabadon maradt hálózati végpontokhoz;
b) illetéktelenek ne léphessenek be a számítógépekbe;
c) ne legyen támadható vezeték nélküli vagy vezetékes kapcsolat a rendszerben;
(2) Az Intézmény területén hálózati végpontot csak ellenőrzött körülmények között lehet létesíteni.

60. (1) Minden olyan asztali vagy hordozható számítógépet, mobiltelefont végpont védelemmel kell ellátni, mely alkalmas:
a) hálózathoz csatlakozásra;
b) adatok kimásolására és továbbítására;
c) USB adathordozó eszköz csatlakozásra;
d) vezeték nélküli kapcsolatok létesítésére.
(2) A vírusvédelmi rendszert az Intézmény minden számítógépére telepíteni kell
(3) Tilos olyan eszközt az informatikai hálózathoz csatlakoztatni, amelyre nincs telepítve vírusvédelem.

61. A végpontvédelmi intézkedések nem akadályozhatják az alapvető működési feladatokat, ezért biztosítani kell a munka során használt engedélyezett (nyilvántartott) és a feladat végrehajtásához szükséges eszközök (nyomtató, szkenner, stb.) zavartalan működését.

62. A kijelölt informatikus általános feladatai:
a) elvégzi a vírusvédelmi szoftverek megfelelő beállítását, a rendszer konfigurálását;
b) ellenőrzi a vírusvédelmi rendszerek rendszeres frissítését;
c) listát készít a rendszeresen manuálisan frissítendő számítógépekről (pl. mobileszközökről), a nyilvántartás szerinti eszközöket frissíti, és a frissülés megtörténtét ellenőrizi a számítógépeken, illetve a vírusvédelmi szoftver program nyilvántartásaiban;
d) megbizonyosodik róla, hogy az informatikai rendszerbe kapcsolt munkaállomáson, szerveren, egyéb informatikai eszközön a vírusvédelmi program telepítve van és a vírusdefiníciós adatbázis naprakész;
e) tájékoztatja a felhasználókat a vírusvédelmi eszközök működéséről, használatáról;
f) megvizsgálja a felhasználók jelzése alapján a vírusgyanús eseteket;
g) elvégzi a vírusfertőzés bekövetkeztekor a szükséges vírusmentesítési lépéseket;
h) figyelemmel kíséri a vírusvédelem hatékonyságát.

63. (1) A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az üzemeltetett rendszerek előre nem látható esemény (katasztrófa, vagy hardver, illetve szoftver meghibásodása, emberi mulasztás) bekövetkezte után, szükség esetén rövid időn belül helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell, hogy az üzemidő-kiesés, adatsérülés, adatvesztés kockázata minimális legyen.
(2) A mentés ütemezését mentési egységenként lehetőleg úgy kell kialakítani, hogy a mentés a munkafolyamatokat, illetve a munkafolyamatok a mentési eljárást ne akadályozzák.
(3) A biztonsági mentés a napi adatbiztonságot szolgáló rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a napi munka során felmerülő kisebb meghibásodásokból származó adatvesztések, adatbázis-konzisztenciahibák megszüntetését a lehető legkisebb időráfordítással. Előbbi esetben a mentés:
a) egy (azonos tűzszakaszban elhelyezett)másik szerverre;
b) vagy az adott szerverbe beépített tartalék HDD-re;
c) vagy a szerverhez kapcsolt külső HDD-re valósul meg.

(4) A mentést követően ellenőrizni szükséges a mentésről készített digitális naplót vagy meg kell győződni a mentés megtörténtéről. A biztonsági mentés használata mellett biztosítani kell egy tűzvédelmi mentést is.
(5) A tűzvédelmi mentés a napi adatbiztonságot szolgáló rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a súlyosabb meghibásodásokból származó (katasztrófa, hardver, illetve szoftver meghibásodás esetén történő) rendszerösszeomlások, adatvesztések, adatbázis-konzisztenciahibák megszüntetését a lehető legkisebb időráfordítással. A tűzvédelmi mentés történhet egy másik szerverre, ha az nem azonos tűzszakaszban található a mentett eszközzel (hálózaton keresztül történő mentés), amelynek használata esetén a következőket kell biztosítani:
a) a munkanap kezdetén az előző napi mentés sikerességét ellenőrizni kell;
b) ha a mentés adathordozóra történik, akkor biztosítani kell:
ba) a mentési adathordozók rendszeres váltott cseréjét;
bb) figyelemmel kell lenni az adathordozók felhasználhatóságának paramétereire (pl. hányszor írható);
bc) az adathordozók előírás szerinti tárolását.
(6) Egyedi mentéssel kell biztosítani azon munkaállomások és mobil eszközök háttértárolóin keletkezett alkalmazások és felhasználói állományok mentését, amelyekről
a) nem történik rendszeres napi mentés a hálózatra vagy
b) az eszközzel kapcsolatban egyedi mentési igény merül fel;
c) azon hálózati közös meghajtók rendkívüli mentését, amire vonatkozó igény a tárkapacitás túlterheltsége miatt merült fel.
(7) A hálózaton tárolt telepítő készletek és programok mentéséről folyamatosan gondoskodni kell.

64. (1) A mobil adathordozó eszközök (pl. pendrive, külső HDD) kiadása, állapotváltozása, visszavétele az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység (vagy az informatikai referens munkakörben foglalkoztatott munkatársnak) feladata.
(2) A mentés elkészítéséhez használt adathordozó típusok kiválasztásánál az alábbiakat kell figyelembe venni:
a) a mentendő adatmennyiségnek megfelelő tárolókapacitás;
b) a megfelelő adatmegőrzési idő – legalább 5 (öt) év különleges beavatkozás, speciális eljárások alkalmazása nélkül –;
c) megfelelő ellenállás a környezeti viszonyoknak (hőmérséklet, páratartalom, fény stb.);
d) adat-visszaállítás esetére szükséges eljárások és eszközök rendelkezésre állása.

65. Az Intézmény elektronikus szoftvereinek telepítőkészletei, illetve adatainak mentésére és archiválására használt adathordozói, a mentés dokumentuma, a helyreállítást biztosító leírások:
a) biztonságos módon, a mentés helyétől (telepítés helyétől) különböző helyen elhelyezett tűzbiztos fémszekrényben vagy
b) a mentés helyétől (telepítés helyétől) különböző tűzszakaszban elhelyezkedő helyiségben tárolandók és az elhelyezésükre
c) megfelelő mechanikai védelemmel (pl. ablakráccsal, biztonsági zárral),
d) elektronikus védelemmel (riasztórendszerbe integrált, füst-, illetve hő-érzékelővel) ellátott,
e) lehetőleg regisztrált kulcsfelvétellel hozzáférhető,
f) közművezetékektől mentes helyiséget kell kijelölni.

66. (1) A mobil adathordozó eszközöket nyilván kell tartani.
(2) Az operációs rendszerek, programok, eszközkezelők telepítő állományait tartalmazó adathordozókról nyilvántartást kell vezetni, amely történhet digitális formában, illetve az informatikai nyilvántartás keretében.

9. Elektronikus információs rendszerek

67. (1) Az Intézmény a szervezet tevékenységének támogatására, az adatok tárolására és a gazdasági, szervezeti munkafolyamatok kezelésére elektronikus informatikai rendszereket alkalmaz. A rendszereket a jelen szabályzat 68. pontja tartalmazza.
(2) Olyan feladatokra, amelyek ellátásához az Intézmény informatikai infrastruktúrája nem elégséges, külső informatikai szolgáltatóktól igénybe vehet informatikai szolgáltatásokat, amennyiben az informatikai szolgáltatások (informatikai rendszerek) megfelelnek a 2013. évi L. törvényben foglaltaknak.
(3) A (2) bekezdésben foglalt rendszerek jogszabályi megfelelésének ellenőrzése az informatikai biztonsági referens feladata, s ezt a 14. pont (2) bekezdésben leírtak szerint látja el.

68. (1) Az Intézmény által használt információs rendszerek:
a) Belső adattároló rendszer (Belső File Rendszer);
b) Integrált Gazdasági Rendszer;
c) Ügyviteli és Iktatási Rendszer (Dokumentumkezelő- és Iktató rendszer);
d) Humánpolitikai Rendszer;
e) Az Intézmény weboldala

69. (1) Annak érdekében, hogy az 2013. évi L. tv. hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából.
(2) Az elektromos információs rendszerek biztonsági osztályba történő besorolásának előkészítése az informatikai biztonsági referens feladata, amelyet a szervezeti egységekkel, illetve az információs rendszerek szállítóival, fejlesztőivel közreműködve végez el.
(3) Amennyiben az információs rendszerek biztonsági szintje nem éri el a szervezet törvény általi besorolásának biztonsági szintjét, úgy az informatikai biztonsági referens cselekvési (intézkedési) tervet készít a megfelelő biztonsági szint eléréséhez figyelemmel a törvényben megszabott szintlépések közötti határidőre is.
(4) Az informatikai biztonsági referens a biztonsági osztályba sorolást a 2013. évi L. tv-ben előírt időszakonként, azaz legalább 3 (három) évente vagy szükség esetén soron kívül felülvizsgálja.

10. A rendszerek hozzáférési jogosultságainak kezelése

70. (1) A szervezeti egység vezetője írásban köteles tájékoztatni az intézményvezetőt a felhasználókra vonatkozó minden változásról (felvétel, munkakörváltozás, kilépés), amely az informatikai vagy kommunikációs rendszert érinti. A szervezeti egység vezetője jogviszonyának megszűnésekor a munkáltatói jogkör gyakorlója gondoskodik a jogosultságok töröltetéséről.
(2) A felhasználói jogosultságok igénylése és kiosztása esetében törekedni kell arra, hogy egy felhasználó csak a munkavégzéshez szükséges és elégséges legszűkebb jogosultságokkal rendelkezzen. A túl széles jogosultsági kör az Intézmény adatintegritásának veszélyeztetésével jár, amelyért a felhasználónak jogosultságokat igénylő szervezeti egység vezető teljes felelősséggel tartozik.
(3) Az Intézmény minden felhasználója a belépésekor az alábbi jogosultságokkal és hozzáférésekkel rendelkezik alapértelmezetten:
a) elektronikus levelezési címmel – felhasználói postafiókkal;
b) az összes felhasználót tartalmazó terjesztési lista tagsággal (központilag kezelt terjesztési lista);
c) a szervezeti egységéhez tartozó technikai fiókhoz a megfelelő jogosultsággal való hozzáféréssel;
d) a felhasználó szervezeti egységének kialakított hálózati megosztáshoz, illetve az intézmény saját tárolóján kialakított hálózati megosztásokhoz;
e) a dokumentumkezelő- és iktatórendszerben alkalmazotti szerepkörrel (ügyintézőnek rögzíthető) – ennél magasabb jogosultságot igényelni kell;
f) a központi kommunikációs rendszerhez való hozzáféréssel.

(4) A vezető beosztású felhasználók a fentieken felül rendelkeznek vezetői szintjüknek megfelelő terjesztési lista tagsággal (központilag kezelt terjesztési lista).
(5) Az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység illetve a kijelölt informatikus a jogosultságok igénylésének, módosításának, megszüntetésének céljából belső használatra létrehozott igénylőlapot használ, melynek kötelező tartalmi elemei a következők:

a) Új igény (új felhasználó) esetén:

aa) a felhasználó adatai (név, szervezeti egység, beosztás, munkavégzés helye);

ab) eszközigénylés (számítógép, laptop – intézményvezetői engedélyhez kötött–, mobiltelefon – intézményvezetői engedélyhez kötött –;

ac) az alapértelmezetten járó jogosultságok és hozzáférések részletezése;

ad) a szervezeti egység számára létrehozott terjesztési listák és technikai fiókok választása (technikai fióknál a hozzáférési szint megadása szükséges);

ae) további terjesztési listák tagságának igénylési lehetősége;

af) további technikai fiók hozzáférésének lehetősége (a technikai fiók felelősének aláírása és a hozzáférési szint megjelölése szükséges);

ag) az elérhető informatikai rendszerekhez való hozzáférés igénylése, amennyiben részletezhető, akkor a hozzáférés szintjének megadása (pl. szerepkör vagy modulok megjelölésével). Amennyiben a megjelölt informatikai rendszert nem az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység illetve a kijelölt informatikus kezeli, az igényt írásban (akár elektronikus levél formájában) jelezni kell az illetékes szervezeti egység felé;

ah) az igényt az intézményvezető aláírása hitelesíti.

b) Új speciális hozzáférés igénylése (adott felhasználói fiókjához illetve annak bizonyos elemeihez) esetén:

ba) az igénylő felhasználó (aki hozzáférést kér) adatai (név, szervezeti egység, beosztás);

bb) a hozzáférni kívánt felhasználói postafiók adatai (felhasználó neve, beosztása, e-mail címe);

bc) a hozzáférni kívánt elem, jogosultság megjelölése (Mappa hozzáférés, Naptár hozzáférés, Levélküldési jogosultság);

bd) mappa esetén alapesetben a Beérkezett üzenetek mappa és az Elküldött üzenetek mappa hozzáférési szintjének magadása;

be) adott almappához tartozó jogosultsági szintjének megadása;

bf) naptár esetén a jogosultsági szint megadása;

bg) levélküldési jogosultság igénylése esetén a jogosultsági szint megadása (levélküldés meghatalmazottként jog vagy az adott email címről való küldés jogosultsága – kizárólag különlegesen indokolt esetben –);

bh) a hozzáférési periódus megjelölése (állandó – visszavonásig érvényben lévő – vagy előre definiált – ideiglenes – időszak megjelölésével –);

bi) a hozzáférés kérésének indoklása;

bj) az igénylés hitelesítéséhez szükséges:

bk) az igénylő aláírása,

bl) az igényelt felhasználói fiókot használó felhasználó aláírása,

bm) az intézményvezető aláírása.

c) Felhasználói jogosultságok és hozzáférések megszüntetése (felhasználó kilépése, illetve hosszabb távollét) esetén:

ca) a kilépő felhasználó elektronikus levelezési postafiókjával kapcsolatos teendők:

cb) a postafiók archiválásának igénye;

cc) a postafiók megszüntetésének időpontja;

cd) a postafiók megszüntetéséig mely felhasználóknak legyen betekintési jogosultságuk a kilépő felhasználó postafiókjának Beérkezett Üzenetek mappájára;

ce) a kilépő felhasználó számítógépének adatainak archiválásának kérése;

cf) a számítógép visszaadásáról történő döntés az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység részére

(alapesetben az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység elviszi a kilépő felhasználó számítógépét az informatikai raktárba).

d) A felhasználó szervezeti egység váltása esetén:

da) a felhasználó adatai (név, régi szervezeti egysége, régi beosztása, új szervezeti egysége, beosztása);

db) a régi szervezeti egység vezetőjének rendelkezései:

dc) az elektronikus levelezéssel kapcsolatos kérdések;

dd) a felhasználói postafiók archiválásának kérése;

de) az archivált adatok mely felhasználók részére kerüljenek beállításra;

df) az adatok a felhasználói postafiókból törléséről való rendelkezés (kéri vagy nem kéri);

dg) a felhasználó számítógépével kapcsolatos kérdések

dh) az adatok archiválásának elrendelése;

di) a számítógép átadása (az új szervezeti egységnek, az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egységnek, átadás megtagadása).

dj) az új szervezeti egység vezetőjének rendelkezései:

dk) az új szervezeti egységhez tartozó terjesztési lista tagság és a technikai fiókhoz való előre meghatározott hozzáférési szint automatikusan beállításra történik (tájékoztató);

dl) a dokumentumkezelő- és iktatórendszerben a felhasználó az új szervezeti egységhez kerül hozzárendelésre automatikusan (tájékoztató);

dm) egyéb terjesztési lista tagság kérése;

dn) egyéb technikai fiókhoz való hozzáférés kérdése (hozzáférési szint megadásával);

do) elérhető informatikai rendszerekhez való hozzáférés igénylése (, amennyiben részletezhető, akkor a hozzáférés szintjének megadása);

dp) a szervezetváltási kérelmet mindkét szervezeti egység vezetőjének aláírása hitelesíti; a szervezeti igazgató beosztásokat érintő szervezeti egység váltás esetén az intézményvezető aláírása hitelesíti a kérelmet.

e) Egy informatikai rendszerhez már működő hozzáférés szintjének módosítása, illetve megszüntetése esetén elegendő a hozzáférést igénylő felhasználó közvetlen vezetőjének elektronikus bejelentése (e-mail, Helpdesk rendszer – jogosultság változás), kivéve speciális hozzáférés esetén (más felhasználói fiókhoz történő hozzáférési szint emelése), amely esetbe új igénylőlap kitöltése szükséges.

(6) A felhasználóval kapcsolatban felmerülő alábbi informatikai igényeket írásban kell jelezni az intézményvezető által megbízott munkatársnak:

a) informatikai eszközigénylés, mozgatás, áthelyezés és átvezetés;

b) informatikai rendszerhez hozzáférés-változtatási igény (igénylés, módosítás vagy törlés);

c) alkalmazástelepítési vagy -eltávolítási igény;

d) inaktívvá válás esetén újraaktiválás kérése;

e) munkavégzési hely vagy feladat változása esetén egyedi vagy tömeges eszközmozgatási és telepítési igény;

f) hálózattal kapcsolatos igény (kiépítés, bővítés, elbontás);

g) informatikai szolgáltatáshoz, alkalmazáshoz, hálózati mappához (könyvtár) való hozzáférés, valamint ezekkel kapcsolatos jogosultság változása (igénylés, módosítás vagy törlés).

(7) Az írásban bejelentett igény alapján az intézményvezető által megbízott munkatárs elvégzi vagy külső fél által szolgáltatott rendszer esetén elvégezteti az informatikai rendszerben:

a) az adatok átvezetését, a szükséges beállításokat;

b) letiltja vagy engedélyezi az informatikai szolgáltatásokat (pl. levelezés, internet, hálózati mappa elérése, nyomtatás stb.);

c) elvégzi a jogosultságok nyilvántartását,

amennyiben az adott rendszerből az informatikus által lekérdezhető, akkor a jogosultságok rendszerben történő átvezetésével,
egyéb esetben külön (elektronikus vagy papíralapú) jogosultsági nyilvántartás vezetésével;
d) a kijelölt informatikus átadja, átveszi, átvezeti, beállítja, illetve törli az informatikai eszközöket és jogokat a belépő, kilépő, meglévő felhasználóknak;
e) elvégzi az informatikai eszközök nyilvántartására vonatkozó teendőket;
f) kilépő dolgozó vagy munkakör változás esetén elvégzi és a szervezet vezetője, illetve a humánpolitikáért felelős munkatárs/a humánpolitikáért felelős szervezeti egység vezető munkatárs felé igazolja a nyilvántartás szerint a dolgozó nevén lévő eszközök átvezetését, valamint jogosultságainak kivezetését a rendszerből.

71. Az Intézmény informatikai rendszerét úgy kell kialakítani és olyan szoftvereket szabad használni, hogy a rendszerbe felhasználó csak authentikáció (a felhasználónév és a jelszó megadása) után jelentkezhessen be.

72. (1) Hálózati rendszergazdai jogosultság kizárólag az intézményvezető engedélyével adható.
(2) A hálózati felhasználói jogosultságot a szervezeti egység vezetőjének írásban tett kérelmére az intézményvezető által ezzel megbízott munkatárs adja meg.
(3) A hálózati rendszergazdai jogosultság kizárólag a rendszergazdai feladatokat ellátó munkatársak részére adható.
(4) Az azonosítónak egyedinek, személyhez kapcsolhatónak kell lennie. Az induló jelszó kiosztására, az adminisztrátori jelszó kezelésére ugyanazok a szabályok érvényesek, mint a felhasználói jelszó kezelésére.
(5) A nem személyhez köthető teljes jogú adminisztrátori azonosító ne lehet napi használatban, az csak olyankor használható, amikor elengedhetetlen.
(6) A nem személyhez köthető adminisztrátori azonosítókat és jelszavakat lezárt és az adminisztrátor által aláírt borítékban az intézményvezető őrzi zárt helyen, lehetőség szerint páncélszekrényben.

73. Az Intézmény informatikai rendszerébe felvett és ott jogosultságokat kapott felhasználókat, a jogosultság nyilvántartás segítségével az annak vezetésére kötelezett, kijelölt informatikus tartja nyilván és naprakészen.

74. (1) A felhasználók hálózati mappákhoz való hozzáférésének jogosultsági szintjeit az adott felhasználó szervezeti egységének vezetője állapítja meg. A hozzáférést írott kérelem alapján az intézményvezető által megbízott munkatárs állítja be.
(2) Az informatikai eszközöket, ha hozzáférhetőség vagy fontosság miatt indokolt (számítógép, nyomtató, multifunkciós eszköz, switch stb.), és ha az eszköz operációs rendszere megengedi, valamint a hálózathoz való hozzáférést minden esetben felhasználói azonosítóval (felhasználói név és jelszó) kell védeni.

75. Az adminisztrátori jogokat személyi vagy munkaköri változás esetén, illetve legalább évente felül kell vizsgálni.

76. (1) A nem használt (tartalék, javításra váró vagy javításból érkezett) informatikai eszközök tárolásáról az intézményvezető által megbízott munkatárs gondoskodik.
(2) A rövid, eltávozással járó szünet – 10 (tíz) perc vagy kevesebb – idejére a számítógépet a felhasználónak a hozzáférés ellen zárolni kell.
(3) A munkaállomást illetéktelen személy (pl. ügyfél) jelenlétében a felhasználó nem hagyhatja felügyelet nélkül zárolatlan állapotban.

11. Biztonsági kockázatmenedzsment

77. (1) Az Intézmény információ biztonsági referense évente egyszer a rendelkezésre álló információk alapján (amelyet a szervezeti egységek írásban bocsátanak rendelkezésre) kockázatelemzést köteles készíteni.

(2) A kockázatelemzés során az egyes veszélyforrások által képviselt kockázatokat kell megállapítani, illetve feltárni. A kockázat meghatározása a veszély megvalósulásának valószínűsége és az okozható kár alapján vagy más nézőpontból, az adott veszélyt képviselő sérülékenység kihasználhatósága és ennek hatása alapján történik.
(3) Az Intézmény információ biztonsági referense elemzés során a kockázatokat kategóriákba sorolja, értékeli. A tanulságokat jelentésben tárja az Intézmény gazdálkodási feladatait ellátó szervezeti egysége elé.

78. (1) A kockázatelemzésről szóló jelentés alapján az Intézmény gazdálkodási feladatait ellátó szervezeti egysége felkéri az Intézmény informatikai feladataiért felelős munkatársát/ az informatikai feladatok ellátásáért felelős egység vezető munkatársát a kockázatok csökkentését célzó intézkedési terv elkészítésére az informatikai biztonsági referens közreműködésével. Az informatikai biztonsági referens feladata az intézkedési terv határidejének és a benne foglalt intézkedések végrehajtásának ellenőrzése, amelyről írásos tájékoztatást ad az intézményvezetőnek.

79. (1) A kockázatkezelés lépései:
a) kockázatok feltárása, csoportosítása és hatáselemzése;
b) szükséges lépések, módszerek meghatározása és hatáselemzés;
c) megoldási tervek és alternatívák készítése;
d) döntés és megvalósítás;
e) monitoring és utóellenőrzés.
(2) A kockázatkezelés szabályai:
a) a valós kockázatokat kell figyelembe venni;
b) minden körülményt figyelembe kell venni;
c) a súlyosság mértéke szerint kell haladni a kockázat megoldása és elhárítása során;
d) a megoldások közül azt a módszert (eszközt kell választani), amelyik a legnagyobb eredményt hozza a legkisebb erőforrás ráfordítással;
e) a kockázatkezelésre fordított erőforrások, a védekezés költségei arányosak kell, hogy legyenek a kockázat mértékével.

12. Ellenőrzés

80. Az IT-biztonság kontrollja az alábbi eszközökkel biztosítható:
a) dokumentált eszközkezelés (üzembe helyezési, eszközátadási, eszközszállítási, leltározási és selejtezési események dokumentálása);
b) a jogosultságok és hozzáférések dokumentálása;
c) ellenőrzött szoftverkezelés (jogtisztaság, tesztelt szoftverek, szoftvernyilvántartás vezetése, telepítés jogosultság szabályozása);
d) mentések és archívumok készítésére, valamint tárolására vonatkozó előírások és kapcsolódó nyilvántartások vezetése;
e) a munkahelyek, hálózatok, informatikai helyiségek kialakítására és üzemeltetésére vonatkozó előírások betartása, kapcsolódó események naplózása;
f) hibakezelési rendszer alkalmazása és ellenőrzése, elemzése;
g) az IT biztonsági többszintű ellenőrzése.

81. (1) Az információ biztonsági referens az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az IT-biztonsági dokumentumokat és jelentés formájában az intézményvezetőt, valamint az Intézmény informatikai feladataiért felelős munkatársát/ az informatikai feladatok ellátásáért felelős egység vezető munkatársát tájékoztatja.
(2) Az IT-ellenőrzések területei:
a) környezeti veszélyek – pl. természeti károk, tűz, stb.;
b) fizikai veszélyek – lopás, rongálás, betörés;
c) informatikai veszélyek – vírusok, számítógépes betörés, stb.;
d) humán veszélyek – szabotázs, gondatlanság, tudatlanság, felelőtlenség, stb.;
e) szervezeti veszélyek – szervezeti problémák, irányítási gondok, stb.

(3) Az IT-ellenőrzések rendszere az Intézménynél:
a) alapszintű ellenőrzés: az Intézmény informatikai feladataiért felelős munkatársa/ az informatikai feladatok ellátásáért felelős egység informatikusai által;
b) Középszintű ellenőrzés:
ba) a szervezeti egység vezetők személyes részvételével;
bb) az Intézmény informatikai feladataiért felelős munkatársának/ az informatikai feladatok ellátásáért felelős egység vezető munkatársa, vagy az informatikai biztonsági referens ellenőrzései;
bc) az Intézmény belső ellenőrzésért felelős/a Belső ellenőrzésért felelős egység munkatársa ellenőrzései;
c) felsőszintű ellenőrzés: központi szakmai irányító szervek, hatóságok ellenőrzései felügyeleti kontrollja, illetve ellenőrzése.

13. Átmeneti intézkedések

82. (1) Jelen szabályzatban előírtak alapján utólagosan el kell készíteni a szükséges nyilvántartásokat, ami – figyelemmel a nagy tömegű utólagos adatgyűjtésre és manuális munkára – a szabályzat hatályba lépésétől számított 6 (hat) hónapon belül történik meg.
(2) Az elkészítendő nyilvántartások:
a) tárolási nyilatkozat: elkészítendő az összes jelenleg felhasználónál található mobil eszközre;
b) szoftvernyilvántartás: elkészítendő az összes jelenleg érvényes és alkalmazott szoftver telepítőkészletére;
c) jogosultság nyilvántartás: elkészítendő az összes jelenlegi felhasználó minden olyan jogosultságára, ami a rendszerekből nem kérdezhető le;
(3) Az informatikai helyiségek fizikai környezetének kialakítására vonatkozó előírásoknak való megfelelést és a szervezeti szintű alkalmazások működését befolyásoló informatikai és távközlési eszközök szünetmentes tápegységgel való ellátottságát meg kell vizsgálni. Előbbiek megfelelőségének hiányában intézkedési tervet kell készíteni jelen szabályzat hatályba lépésétől számított 6 (hat) hónapon belül.
(4) A mentések technikai, műszaki hátterének meglétét, a tűzvédelmi terveket meg kell vizsgálni. Előbbiek megfelelőségének hiányában intézkedési tervet kell készíteni jelen szabályzat hatályba lépésétől számított 6 (hat) hónapon belül.
(5) A felhasználók informatikai eszközökkel való ellátottságát, a saját tulajdonú eszközök (pl. pendrive, notebook) hivatali célra történő használatát meg kell vizsgálni. Előbbiek megfelelőségének hiányában intézkedési tervet kell készíteni jelen szabályzat hatályba lépésétől számított 6 (hat) hónapon belül.
(6) Az elektronikus informatikai rendszerek nyilvántartását és a rendszerek biztonsági szintbe való besorolását (az elvárt és a jelenlegi biztonsági állapot leírását) és a hozzá kapcsolódó cselekvési tervet (intézkedési tervet) el kell készíteni, amely az informatikai biztonsági referens feladata, amelynek határideje jelen szabályzat hatályban lépésétől számított 6 (hat) hónap.
(7) Az elektronikus informatikai rendszerek biztonsági szint besorolásának felülvizsgálatát az informatikai biztonsági referens végzi bevonva a rendszert használó és abban adatot, információt tároló szakmai szervezeti egységeket.
(8) A belső biztonság tudatosság fejlesztésére szolgáló belső képzés kialakítása az Intézmény gazdasági feladatai ellátásért felelős munkatársának/a Gazdasági Szervezet vezető munkatársának feladata.
(9) Jelen szabályzat ellenőrzésére eljárásrendet kell kialakítani, amely az Intézmény gazdálkodási feladatait ellátó szervezeti egységének vezető munkatársának feladata, kialakításának határideje jelen szabályzat életbe lépésétől számított 6 (hat) hónap.

14. Záró rendelkezések

83. (1) Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán jelen szabályzat valamely rendelkezése a hatályos jogszabályok rendelkezéseivel nem áll többé összhangban, akkor az érintett rendelkezés helyébe minden külön rendelkezés nélkül a hatályos jogszabályi rendelkezés lép.
(2) Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán a hatályos jogszabály a jelen szabályzatban foglalt értelmező rendelkezéstől eltérően határoz meg valamely fogalmat, akkor ezen rendelkezés helyébe minden további rendelkezés nélkül a mindenkor hatályos jogszabályi rendelkezés lép.

84. (1) Az intézmény vezetőjének kell gondoskodni, hogy a szabályzatban foglalt előírásokat az érintett munkatársak megismerjék, annak tényét a szabályzat 1. számú mellékletében szereplő megismerési nyilatkozaton aláírásukkal igazolják a hatálybalépés napjával egyidejűleg.

(2) A szabályzat 2023. december 15. napján lép hatályba.

Gánt, Bányatelep, 2023. december 14.

.....

Farkas Judit

Intézményvezető

1. számú melléklet

NYILATKOZAT

Alulírott kijelentem, hogy az Aranyalma Integrált Szociális Intézmény Fejér Vármegye informatikai biztonságról szóló szabályzatát a mai napon teljes terjedelmében megismertem, azt magamra nézve kötelezőnek fogadom el.

Név	Munkakör	Dátum	Aláírás