Napsugár Integrált Szociális Intézmény Csongrád-Csanád Vármegye

6760. Kistelek, Kossuth.u.41
tel: 06-62/598-010, e-mail: kistelek@napsugar-otthon.hu

Iktatószám: 90603-A/929- 49 /2023

Informatikai biztonsági szabályzat

Hatályos: 2023.03.03.-tól

1. Az Informatikai Biztonsági Szabályzat célja

Az Informatika Biztonsági Szabályzat (a továbbiakban: IBSZ) alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése
- GDPR előírásainak való megfelelés.

A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembehelyezésen keresztül az üzemeltetésig.
A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed az intézmény székhelyének és telephelyeinek munkavállalóira.

2.2. Tárgyi hatálya

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

3. Az adatkezelés során használt fontosabb fogalmak

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. *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.
29. *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.
30. *Hardver:* az informatikai rendszer fizikai elemei.
31. *Hálózat:* két vagy több számítógép, illetőleg általánosságban informatikai rendszerek összekapcsolása, amely a komponensei közötti adatcserét teszi lehetővé.
32. *Helpdesk rendszer:* olyan információs rendszer, amely a felhasználók hibabejelentéseinek és egyéb informatikát érintő bejelentéseinek kezelését és az intézkedések dokumentálását és nyomon követését teszi lehetővé.
33. *Hozzáférés:* olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.
34. *Informatika:* olyan tudomány, amely elméletet, szemléletet és módszertant ad a számítógépes információfeldolgozás tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.
35. *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.
36. *Informatikai eszközök:* minden olyan hardver és szoftver elem, mely az informatikai és számítástechnikai rendszerek működésében részt vesz.
37. *Informatikai rendszer:* a hardverek és szoftverek olyan kombinációjából álló rendszer, amelyet az adat- illetve információkezelés különböző feladatainak és folyamatainak teljesítésére alkalmaznak.
38. *Informatikai támadás:* minden olyan hardver vagy szoftver elem működését befolyásoló tényező, amely szándékosan akadályozza azok működését vagy kárt tesz azokban.
39. *LAN (Local Area Network):* helyi számítógépes hálózat.
40. *Működőképesség:* a rendszernek és elemeinek, az elvárt és igényelt üzemelési állapotban való fennmaradása.
41. 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.
42. *Pótlólagos szoftver:* olyan kiegészítő szoftver, amelyet a védelem erősítésének érdekében alkalmaznak.

43. *Program:* eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.
44. *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.
45. *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.
46. *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.
47. *SPAM:* kéretlen üzleti, politikai vagy vallási célú e-mail, fax vagy SMS, legtöbbször kereskedelmi célú és nagy mennyiségben kiküldött üzenet.
48. *Szoftver:* valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.
49. *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.
50. *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.
51. *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.
52. *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.
53. *WAN (Wide Area Network):* nagy távolságú számítógép-hálózat.

4. Az IBSZ biztonsági fokozata

Az intézmény adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Leltározási szabályzattal,
- Számviteli politikával
- Selejtezés rendjéről szóló szabályzattal
- Adatvédelmi Szabályzattal

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket. Az Intézmény informatikai hálózatára kizárólag az Intézmény által biztosított eszközöket (számítógépeket, laptopokat, mobil eszközöket) lehet rácsatlakoztatni.
Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,

6.2. A védelem eszközei

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

7. *A védelem felelőse*

A védelem felelőse a mindenkori intézményvezető-helyettes és a rendszergazdák.
A jelen szabályzatban foglaltak végrehajtásáról és feltételeinek biztosításáról az intézmény vezetőjének kell gondoskodnia.

7.1. Adatvédelmi felelősök feladatai

a) Intézményvezető-helyettes feladatai:
– az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
– javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
– meghatározza a védett adatok körét,
– ellátja az adatkezelés és adatfeldolgozás felügyeletét,
– ellenőrzi a védelmi előírások betartását,
– az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,

– az adatvédelmi feladatok ismertetése,
– ellenőri tevékenységét adminisztrálja.
– ellenőrzi a szoftverek használatának jogszerűségét

b) Rendszergazda feladatai:
– a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
– felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért,
– gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
– feladata a védelmi eszközök működésének folyamatos ellenőrzése,
– felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
– gondoskodik a folyamatos vírusvédelemről, az intézmény által biztosított vírusmentesítő program telepítésével
– a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
– folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
– ellenőrzi a rendszer adminisztrációját,

7.2. Az intézményvezető-helyettes ellenőri feladatai
– rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
– előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.
- A számítógépes meghajtókon tárolt adatokat negyedévente felülvizsgálja, a célhoz már nem kötött adatokat törli.

7.3. Az intézményvezető-helyettes jogai
- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a vállalkozás vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett munkavállalók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az intézményvezető-helyettes feladata.

8.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:
– közlésre szánt, bárki által megismerhető adatok,
– minősített, titkos adatok.
Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.
Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot, ami a munkaköri leírásban kerül rögzítésre. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.
Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.
Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.
A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért a rendszergazda a felelős.

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

9. Az informatikai eszközbázist veszélyeztető helyzetek

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

9.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- földrengés,
- árvíz,
- tűz,
- villámcsapás stb.
- környezeti kár:
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,

- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség-kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

10. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

10.1. Tervezés és előkészítés során előforduló veszélyforrások

– a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
– hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

10.2. A rendszerek megvalósítása során előforduló veszélyforrások

– hibás adatállomány működése,
– helytelen adatkezelés,
– programtesztelés elhagyása.

10.3. A működés és fejlesztés során előforduló veszélyforrások

– emberi gondatlanság,
– szervezetlenség,
– képzetlenség,
– szándékosan elkövetett illetéktelen beavatkozás,
– illetéktelen hozzáférés,
– üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök környezetének védelme

11.1. Vagyonvédelmi előírások

– az informatikai eszközöket csak az intézmény arra felhatalmazott alkalmazottai használhatják,
– az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

11.2. Adathordozók

– könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
– az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
– a használni kívánt adathordozót (CD) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni,
– a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,
– adathordozót másnak átadni csak engedéllyel szabad,
– a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.3. Tűzvédelem

A szerver helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
Az intézmény szerverszobáihoz 10 méteren belül legyen elhelyezve 1 tűzoltó készülék.
Az intézmény helyiségében, ahol a szerver található elektromos vagy más munkát csak a gondnok/üzemeltetési koordinátor tudtával, ill. engedélyével szabad végezni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
– menteni a még használható anyagot,
– biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
– archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

12.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik.
A munkák szervezésénél figyelembe kell venni:
– a gyártó előírásait, ajánlatait,
– a tapasztalatokat.
Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

12.3. Az informatikai feldolgozás folyamatának védelme

12.3.1. Az adatrögzítés védelme

– adatbevitel hibátlan műszaki állapotú berendezésen történjen,
– tesztelt adathordozóra lehet adatállományt rögzíteni,
– a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
– az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
– hozzáférési lehetőség:

- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.
  Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások,
    - ellenőrző rögzítési utasítások,
    - tesztelő és törlő programok kezelési utasításai,
    - megőrzési utasítások,
    - gépkezelési leírások.

12.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

12.3.3. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

12.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

12.3.6. Selejtezés, sokszorosítás, másolás

A selejtezést az intézmény selejtezési szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

12.3.8. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

12.3.9. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.
A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák a felelősek.

12.4. Szoftver védelem

12.4.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

12.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem
A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása:

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni.
A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.
A programok nyilvántartásáért és működőképes állapotban való tartásáért a leltárfelelősöknek kell gondoskodni. A jogtiszta szoftverek, vírusellenőrzők biztosítása a rendszergazda felmérése alapján az intézményvezető feladata.

13. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.
A vásárolt szoftverekről biztonsági másolatot kell készíteni.

13.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
A vállalkozás informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.
Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

14. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői (részlegvezetők) folyamatosan ellenőrzik.

15. Záró rendelkezések:

Az Informatikai Biztonsági Szabályzat 2023. 03.03-án lép hatályba, rendelkezéseit a folyamatban levő ügyekre is alkalmazni kell.
Az Informatikai Biztonsági Szabályzatban érintett munkavállalók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Kistelek,202303.03.

…….
intézményvezető

Jóváhagyta:

…….
Vármegyei Gazdasági Osztály vezetője

MEGISMERÉSI NYILATKOZAT

A Csongrád Megyei Napsugár Otthon 90603-A/241-107/2020 iktatószámon kiadott Informatikai biztonsági szabályzatát megismertem.
Tudomásul veszem, hogy az abban foglaltakat a munkavégzésem során köteles vagyok betartani.

NÉV	BEOSZTÁS	DÁTUM	ALÁÍRÁS