



Fővárosi Önkormányzat Foglalkoztató Intézete
Darvasto

1006-5/2013.

**INFORMATIKAI -SZÁMÍTÁSTECHNIKAI BIZTONSÁGI
ÉS
KÖZSZOLGÁLATI ADATVÉDELMI
SZABÁLYZAT**

1. sz. módosítás

Hatályos: 2013. január 1. napjától

Készítette:


Szappan Krisztina
gazdasági vezető

Jóváhagyta:


Vaski Ferenc
intézményvezető



I. INFORMATIKAI – SZÁMÍTÁSTECHNIKAI BIZTONSÁGI SZABÁLYZAT

Intézményünk **Informatikai - Számítástechnikai Biztonsági Szabályzatát** (továbbiakban ISZBSZ) az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg:

1. Az Informatikai - Számítástechnikai Biztonsági Szabályzat célja

Az Informatikai - Számítástechnikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa intézményünkben az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai - Számítástechnikai Biztonsági Szabályzat célja továbbá:

- a titok-, munka-, 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.

A szabályzatban meghatározott védelemnek működni kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen Informatikai - Számítástechnikai Biztonsági Szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai - Számítástechnikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az ISZBSZ személyi hatálya az intézmény valamennyi fő- és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az Intézet tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
- 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

érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviselői szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

adatkezelő: az a természetes vagy jogi személy, illetve 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 általa megbízott adatfeldolgozóval végrehajtatja;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges;

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából;

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése;

adatifeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

adatifeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi;

adatfelelős: az a közfeladatot ellátó szerv, amely az elektronikus úton kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett;

adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatait honlapon közzéteszi;

adatállomány: az egy nyilvántartásban kezelt adatok összessége;

4. Az ISZBSZ biztonsági fokozata

Intézményünk **alapbiztonsági** fokozatba tartozik, **általános** informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

Az Informatikai - Számítástechnikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Bizonylati rend,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Belső ellenőrzési kézikönyv,
- Belső kontroll rendszer.

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 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:

- a rendszer elemeinek elhelyezésére szolgáló helyiségekre,
- 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, előírászerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

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

Intézményünkben számítógépes hálózat működik, melyhez hozzáférhetnek az egyes munkaállomások. Az informatikai nyilvántartás, feldolgozás az egyes feladatokhoz rendelt **munkaállomásokon** történik.

A munkaállomást üzemeltető egyben az önálló egység **védelmi felelőse is**.

Munkaállomás	Feladat	Üzemeltető = védelmi felelős
1. Lakók térítési díj elszámolása	Név szerinti nyilvántartás a személyi térítési díjakról.	szociális ügyintéző- letéti könyvelő
2. Lakók pénzügyi elszámolása	Név szerinti nyilvántartás a lakók készpénzvagyonáról, pénzforgalmáról (letét)	pénzügyi adminisztrátor
3. Lakók ingóságainak nyilvántartása	Név szerinti nyilvántartás a lakók saját tulajdonú ruházatáról, műszaki cikkeiről és egyéb ingóságairól.	szociális ügyintéző II.
4. Gyógyszer-nyilvántartás	Lakók gyógyszerellátásának név szerinti nyilvántartása SZ2000 program	ápolók
5. Ügyfélterminál és pénztár	A költségvetési elszámolási számlák, továbbá a lakók közös letéti számlájának pénzforgalma, pénztári készpénzforgalom (intézményi és letéti pénztár)	pénzügyi ügyintéző
6. Élelmezés	Élelmezési anyagok raktári nyilvántartása, könyvelése, bizonylatolása.	élelmezésvezető
7. Analitika	Készletanalitika, számlázás, befektetett eszközök nyilvántartása, értékcsökkenés elszámolása	számviteli ügyintéző
8. Könyvelés	Főkönyvi könyvelés, költségvetési, beszámolási adatok	könyvelő

Munkaállomás	Feladat	Üzemeltető = védelmi felelős
9. Bér- és munkaügyi nyilvántartás	Alkalmazottak személyi, munkaügyi és bérügyi adatainak kezelése, feldolgozása és továbbítása. KGR – MÁK	bér- és munkaügyi előadó
10. Titkárság	Elhelyezéssel kapcsolatos adatok nyilvántartása, feldolgozása	titkárnő
11. Pedagógia	Lakókkal kapcsolatos adatok, dokumentációk nyilvántartása	gondozási egység felelősök
12. Mozgáskoordináció fejlesztő csoport	Lakók reumatológiai szűrésének és kontrollszűrésének orvosi leletei, és a fejlesztés során ehhez kapcsolódó adatok	mozgásterapeuta
13. Foglalkoztatás-koordinátor	Lakók szociális foglalkoztatásával kapcsolatos adatok kezelése	foglalkoztatás-koordinátor

7.1. Adatvédelmi felelős feladatai

- ellátja az adatfeldolgozást,
- betartja a védelmi előírásokat.

7.2. A rendszergazda feladatai

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- felelős az informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésének ellenőrzése,
- felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- ellenőrzi a vásárolt szoftverek helyes működését, vírusmentességét, a használat jogszerűségét,
- a vírusvédelemmel foglalkozó szervezetekkel kapcsolatot tart,
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- tevékenységéről rendszeresen beszámol az intézmény vezetőjének.

7.3. A rendszergazda ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

7.4. A rendszergazda jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthez 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.

7.5. Az adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie:

- erkölcsi feddhetetlenség,
- összeférhetetlenség – az adatvédelmi felelős funkció összeférhetetlen minden olyan vezetői munkakörrel, amelyben adatvédelmi kérdésekben a napi munka szintjén dönteni, intézkedni kell,
- informatika szintjén:
 - az informatikai hardver eszközök és a védelmi technikai berendezések ismerete
 - üzemeltetésben jártasság,
 - szervezőképesség.
- a szakterületre vonatkozó jogi szabályozás ismerete.

8. 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.

Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkor előírásainak.

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

Minden dolgozóval, aki az adatok gyűjtése, felvétele, tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése során információkhoz jut **adatkezelési nyilatkozatot** kell aláíratni. (1. sz. melléklet)

Az adatkezelési nyilatkozat naprakészen tartásáért a **bér- és munkaügyi előadó** a felelős.

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

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 szolgáltatásban bekövetkező zavarok:
 - feszültség-kimaradás,
 - feszültség-ingadozás,
 - 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),
- megtevesztő 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,
- illegális másolattal 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. A működés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezatlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

11. Az informatikai eszközök környezete, azok védelme:

11.1. A szerverszoba minimális igénye

A szerverszerkényt biztonságos, védett helyre kell telepíteni. Intézményünkben 2 db szerverszekrény található:

- 1 db a 6. sz. épület emeleti folyósón,
- 1 db a 2. sz. épület emeletén a Demeter-teremben.

A szerverszekrények e célra rendszeresített tűzálló, zárható fémszekrények.

A szervergépek szünetmentes tápegységgel ellátottak, így áramkimaradás esetén működésük biztosított.

11.2. A munkaállomásokra vonatkozó előírás

Csak zárható helyiségben szabad tárolni. Ha a helyiségben nem tartózkodik senki, az ajtót bezárva kell tartani.

Szünetmentes tápegységgel kell ellátni az egyes munkaállomásokat, hogy váratlan áramkimaradás esetén is biztosított legyen a folyamatosság.

11.3. Egyéb vagyónvédelmi előírások

- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős,
- biztosítani kell, hogy a számítógép monitorán megjelenő adatokat illetéktelen személyek ne olvashassák el.

11.4. Adathordozók

- Floppykat, CD-t, DVD-t könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni,
- a használni kívánt adathordozót (floppy, CD, DVD) 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 más szervezetnek átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

11.5. Vírus védelem

A szerverek és munkaállomások vírusvédelmére az alábbi szabályokat kell betartani:

- A szerverekre és minden munkaállomásra vírusellenőrző szoftvert kötelező telepíteni.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi frissítését.
- A felhasználók részéről tilos a vírusellenőrző szoftver beállításainak módosítása.

11.6. Tűzvédelem

Minden olyan hivatali, irodahelyiség, amelyben informatikai eszközt használnak, illetve munkaállomás működik a „D” tűzveszélyességi osztályba tartozik, amely **mérsékelt tűzveszélyes** üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépteremre vonatkozóan az intézmény Tűzvédelmi szabályzata tartalmazza.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

Az informatikai eszköz elhelyezésére szolgáló helyiségben elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

12. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

12.1. A gépterem védelme

Elemi csapás (vagy más ok) esetén a gépteremben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértákról a megsérült adatok visszaállítása,
- új adatfeldolgozás, helyiségek kialakítása,
- 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.

A javítást, karbantartást külső szakszerviz útján biztosítani kell.

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,
- hozzáférési lehetőség:
 - = a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz.

12.3.2. Adathordozók védelme

Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni.

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

12.3.3. Selejtezés, sokszorosítás, másolás

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári raktározási hibából követően felhasználásra alkalmatlan (deformálódott) mágneslemez, CD-t, DVD-t, pen-drive-ot,
- véglegesen elhasználódott anyagot (pl. leporelló).

Az alkalmatlan mágneslemezeket, CD-eket, DVD-eket fizikai roncsolással használhatatlanná kell tenni.

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

12.3.5. Mentések, file-ok védelme

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

A szervergépen a fájlok védelme megoldott ún. raid eljárással. A szervergépben 2 db winchester található, melyek „tükröz” winchesterek, mindkettőre rákerülnek a mentett adatok, így az egyik leállása, meghibásodása esetén a másik átveszi a helyét.

A munkaállomások kezelői kötelesek az általuk készített dokumentumokat, fájlokat a szerverre menteni, így biztosított a védelem.

12.4. Szoftver védelem

12.4.1. Felhasználói programok védelme

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

Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni.

A felhasználói programok névreszóló belépési jelszóval védettek.

13. A központi számítógépek és a hálózat munkaállomásainak működésbiztonsága

13.1. Központi gépek (szerverek)

Szünetmentes áramforrást kötelező használni, amely megvédi a berendezést a feszültség-ingadozásoktól, áramkimaradás esetén adatvesztéstől.

13.2. Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak az intézményvezetővel, a gazdasági vezetővel és a rendszergazdával történt egyeztetés után lehet.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

Vírusfertőzés gyanúja esetén az adatfeldolgozást be kell szüntetni, és a rendszergazdát azonnal értesíteni kell.

Az intézmény 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 nem szabad.

14. Internet hozzáféréssel kapcsolatos intézkedések:

Az intézmény mikrohullámú adatátvitellel működő internet elérési lehetőséggel rendelkezik. Az internetes gépeken minden esetben működtetni kell a vírusvédelmet. Dolgozók részére magáncélú internetes hozzáférést intézményünk **nem biztosít**.

15. Honlap működtetése

Intézményünk www.darvasto.hu névvel honlapot működtet.

Az egyes fő- és al-menüpontokhoz a rendszergazda jogosult az adatokat, információkat hozzárendelni, az alábbi személyek utasítására, illetve értesítése alapján:

Főoldal – Megközelíthetőség	az intézményvezető utasítása alapján
Főoldal – Elérhetőségeink	a titkárnő köteles figyelemmel kísérni az adatokat, és változás esetén a rendszergazdát értesíteni
Főoldal – Hírek, információk	az intézményvezető utasítása alapján
Főoldal – Programajánló	az intézményvezető utasítása alapján
Főoldal – Állásajánlat	a bér- és munkaügyi előadó adja át a szükséges dokumentumot a rendszergazdának, valamint tájékoztatja a rögzítés dátumáról
Főoldal – Egyéb szolgáltatásaink	az intézményvezető utasítása alapján
Főoldal – Közérdekű adatok	<p>A „Szabályzat a közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosság hozatalának rendjéről” alapján.</p> <p>A szabályzat 2. sz. melléklete szerinti általános közzétételi lista I. Szervezeti és személyzeti adatok, valamint II. Tevékenységre, működésre vonatkozó adatok közzétételéért az intézményvezető felelős. A szükséges adatokat, illetve változásokat a titkárnő köteles átadni a rendszergazda részére.</p> <p>III. Gazdálkodási adatok közzétételéért a gazdasági vezető felelős. Az adatokat a pénzügyi csoportvezető köteles a rendszergazda részére átadni.</p>
Intézményünkről főmenü	Az e főmenüben található al-menüpontokban lévő dokumentumokat változás esetén a titkárnő köteles a rendszergazda részére átadni.
Bekerülés feltételei	az intézményvezető utasítása alapján
Szolgáltatások	az intézményvezető utasítása alapján

Szociális foglalkoztatás – Mi a szociális foglalkoztatás?	az intézményvezető utasítása alapján
Szociális foglalkoztatás – Az intézmény lakóinak képzése	az intézményvezető utasítása alapján
Szociális foglalkoztatás – Dokumentumok	Az itt található dokumentumokat változás esetén a titkárnő köteles a rendszergazda részére átadni.
Szociális foglalkoztatás – Termékkatalógus	A termékkatalógus folyamatos karbantartása a foglalkoztatás szervező feladata.
Képgaléria	A képgalériában kizárólag az intézményvezető engedélyével helyezhetők el fényképek.
Alapítvány	Az intézmény lakóinak integrációját, művészeti és sporttevékenységét segítő civil szervezetek információi találhatóak meg. Az adatokat a szervezetek kérése alapján helyezi el a rendszergazda.

II. KÖZSZOLGÁLATI – ADATVÉDELMI SZABÁLYZAT

A Közzolgálati Adatvédelmi Szabályzat intézményünk közzolgálati nyilvántartásával összefüggő legfontosabb adatvédelmi, informatikai-biztonsági szabályokat tartalmazza különös tekintettel az adatkezeléssel, adattovábbítással és nyilvánosságra hozatallal kapcsolatos adatvédelmi követelményekre.

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A Közzolgálati adatvédelmi szabályzat célja

A szabályzat célja, hogy rögzítse és összefoglalja azokat a követelményeket és biztosítókat, amelyek a helyi sajátosságokra figyelemmel biztosítják az adatvédelmi és adatbiztonsági szabályok kialakítását.

1.2. A Közzolgálati adatvédelmi szabályzat hatálya

1.2.1. A szabályzat tárgyi hatálya

A szabályzat hatálya kiterjed intézményünknel a közzolgálati és ellátotti nyilvántartással és a hozzá kapcsolódó iratok jogszabályszerű kezelésével összefüggő teljes adatkezelési és informatikai folyamatra.

1.2.2. A szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed intézményünk valamennyi szervezeti egységére, különös tekintettel azokra, ahol személyi adatokat használnak, kezelnek, tárolnak, vagy továbbítanak, valamint a betekintésre jogosultakra és az ügykezelés folyamatában személyi irattal érintkezőkre.

1.2.3. A szabályzat időbeli hatálya

A szabályzat időbeli hatálya kiterjed a közalkalmazotti alapnyilvántartással és a kapcsolódó személyi iratokkal, valamint az ellátotti iratokkal összefüggő teljes adatkezelési és informatikai folyamatra, az irat beérkezésétől, keletkezésétől a megsemmisítésig.

1.3. A Szabályzat elkészítése az alábbi jogszabályokon alapul

- az információs önrendelkezési jogról és az információszabadságról szóló a 2011. évi CXII. törvény,
- a statisztikáról szóló 1993. évi XLVI. törvény,
- a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény,
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény,
- az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés.

2. RÉSZLETES SZABÁLYOK

2.1. A személyi iratok kezelésének adatvédelmi követelményei

2.1.1. Személyi irat fogalma

Személyi irat minden – bármilyen anyagon, alakban, és bármilyen eszköz felhasználásával keletkezett – adathordozó, amelyre a közalkalmazotti jogviszony létesítésekor, fennállása alatt, megszűnésekor, illetve azt követően keletkezik, és a közalkalmazott személyével összefüggésben adatot, megállapítást tartalmaz.

2.1.2. A személyi iratok köre

- A személyi anyag iratai,
- a közalkalmazotti jogviszonnyal összefüggő egyéb iratok,
- a közalkalmazottnak a közalkalmazotti jogviszonyával összefüggő más jogviszonyaival kapcsolatos iratok,
- a közalkalmazott saját kérelmére kiállított, vagy önként átadott adatokat tartalmazó iratok.

2.1.3. A személyi iratok kezelése

A közalkalmazotti jogviszony létesítésekor összeállításra kerül a közalkalmazott személyi anyaga. A személyzeti iratokat külön gyűjtőszámon kell iktatni és tartalmuknak megfelelően csoportosítva keletkezésük sorrendjében az e célra személyenként rendszeresített dossziében kell őrizni.

A személyi anyagban a személyzeti iratokon kívül más irat nem tárolható.

Az irattározás a közalkalmazotti jogviszony fennállásáig a bér- és munkaügyi előadónál történik. Ha a közalkalmazotti jogviszony nem jön létre, az ezzel kapcsolatos döntést követő 8 napon belül vissza kell adni az érintettnek a jogviszony létrehozását kezdeményező iratokat, illetve a személyi anyagot vissza kell küldeni annak a szervnek, amely azt korábban megküldte.

2.1.4. A személyi iratok megőrzése

A közalkalmazotti jogviszony megszűnése esetén a személyi anyagot irattározni kell.

A személyi anyagot a jogviszony megszűnésétől számított **ötven évig** meg kell őrizni.

Levéltárba adásáról az Iratkezelési Szabályzat szerint kell eljárni.

2.2. A személyi anyagot kezelők személyes felelőssége:

2.2.1. A közalkalmazotti jogviszonnal összefüggő adatok kezeléséért felelős:

- intézmény vezetője,
- a közalkalmazott felettese,
- a bér- és munkaügyi előadó,
- a közalkalmazott a saját adatainak közzététele tekintetében tartozik felelősséggel.

2.2.1.1. Az intézmény vezetőjének felelőssége

Felel a közalkalmazotti jogviszonnal összefüggő adatok védelmére és kezelésére vonatkozó jogszabályok, valamint az e szabályzatban rögzített előírások megtartásáért, illetve e követelmények teljesítésének ellenőrzésért.

E felelősségi körében köteles gondoskodni:

- az informatikai és adatvédelmi szabályzat kiadásáról,
- az ellenőrzés módszereinek és rendszerének kialakításáról és működtetéséről,
- a közalkalmazotti jogviszonnal összefüggő adatok védelmével kapcsolatos követelmények intézményen belüli közzétételéről.

2.2.1.2. A bér- és munkaügyi előadó felelőssége

A bér- és munkaügyi előadó felelősségi körén belül köteles:

- gondoskodni arról, hogy az általa kezelt adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának.
- adathelyesbítés, javítás kérelme esetén kezdeményezi az intézmény vezetőjénél a helyesbítés engedélyezését, és az intézményvezető döntése alapján haladéktalanul köteles eljárni.

2.2.1.3. A közalkalmazott felelőssége

A közalkalmazott felelős azért, hogy az általa az intézmény részére átadott, bejelentett adatok **hitelesek, pontosak, teljesek és aktuálisak** legyenek.

3. AZ ELLÁTOTTAK SZEMÉLYES ADATAINAK KEZELÉSE

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló törvény meghatározza az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit és céljait.

Személyes adatot csak törvényes cél eléréséhez szükséges esetekben és mértékben lehet kezelni.

Az ellátottak egészségügyi és személyi azonosító adatainak kezelése és feldolgozása során biztosítani kell az adatok biztonságát véletlen, vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

3. 1. Adatkezelés

Intézményünk, mint szociális ellátást, szolgáltatást nyújtó intézmény – kezelheti a lakók, ellátottak minden olyan egészségügyi és személyazonosító adatát, amely az intézményi elhelyezés, gondozás szempontjából szükséges.

Az adatok kezelésére a tv. II. fejezet rendelkezései értelemszerűen irányadók.

3.1.1. Az egészségügyi és személyazonosító adatok kezelésére jogosultak köre

- a betegellátó, (kezelést végző orvos, egészségügyi szakdolgozó, gyógykezelést végző személy, gyógyszerész)
- az intézményvezető,
- az intézményvezető által adatkezeléssel megbízott személy.

3.1.2. Az egészségügyi és személyazonosító adatok továbbítására jogosultak köre

- az intézményvezető,
- a betegellátó.

3.2. Egészségügyi és személyazonosító adatok nyilvántartása

Az ellátottak egészségügyi és személyazonosító adatait Intézményünk **egészségügyi csoportja** tartja nyilván.

3.2.1. Az egészségügyi dokumentáció tartalma

- kórlap, kitöltésére jogosult:
 - intézményvezető ápoló (személyazonosító adatokat illetően)
 - intézményi orvos (vizsgálati eredmények, feljegyzések)
 - kezelőorvos (a betétlapokon történő bejegyzések)
- szakorvosi vizsgálatok, kórházi zárójelentések,
- TAJ kártya,
- Közgyógyellátási igazolvány.
 - Kezelés: Névvel ellátott személyenkénti dosszié.
 - Tárolás: Orvosi rendelő
 - Adatok védelméért felelős: intézményvezető ápoló

3.2.2. Gyógyszerellátás nyilvántartása

A nyilvántartása gépi adatfeldolgozással történik, amely biztosítja a személyenkénti kimutatót, elszámolást.

Az adatfeldolgozást végző személy: ápolók

Az adatok védelméért felelős személy: intézményvezető ápoló

3.3. Titoktartás

Az adatkezelő a működése során tudomására jutott orvosi titkot köteles megtartani.

Az adatkezelő mentesül a titoktartási kötelezettség alól az alábbi esetekben:

- az egészségügyi és személyazonosító adat továbbítására az érintett, illetve törvényes képviselője írásban hozzájárult, az abban foglalt korlátozásokon belül,
- az egészségügyi és személyazonosító adat továbbítása törvény előírásai szerint kötelező.

3.4. Felelősség

Az egészségügyi és személyazonosító adatok védelméért, a nyilvántartás megőrzéséért az adatot kezelő **intézmény vezetője** felelős.

Az intézmény vezetője tevékenysége során

- gondoskodik az adatvédelmi szabályok betartásáról,
- ellenőrzi az adatkezelők és adatfeldolgozók ez irányú tevékenységét,
- kezdeményezi az adatvédelem, illetve az adatbiztonság területén kifejlesztett technológiák és eszközök alkalmazását,
- biztosítja az adatkezeléssel és feldolgozással foglalkozó személyek oktatását,
- dönt a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról és megsemmisítéséről.

ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2012. január 1. napján lép hatályba, ezzel egyidejűleg a 2011. január 1. napjától érvényben volt szabályzat hatályát veszti.

Darvastó, 2012. március 19.

Fővárosi Önkormányzat
Foglalkoztató Intézete
Darvastó

Adatkezelési és titoktartási nyilatkozat

Alulírott.....(név)

e nyilatkozattal kötelezem magamat, hogy a Fővárosi Önkormányzat Foglalkoztató Intézete Darvastó munkáltatóval kötött közalkalmazotti jogviszonyom fennállása alatt tudomásomra jutott adatot megőrzöm, a feladatellátásom során előttem ismertté vált olyan adatokról, tényekről illetéktelen szervnek vagy személynek tájékoztatást nem adok, amelyek kiszolgáltatása az állam, az intézmény, munkatársaim vagy a lakók számára hátrányos vagy jogellenes előnyös következményekkel járna.

A munkavégzés során csak a részemre hozzáférhető adatokkal dolgozom, más adatok hozzáféréseire kísérletet sem teszek.

Darvastó, 20.....

aláírás

FELHASZNÁLÓI PROGRAMOK

Program neve (azonosítója)	Program készítőjének neve	Feldolgozási rendszer megnevezése
CT-EcoStat gazdasági és gazdálkodási programrendszer	CompuTrend Kft.	Pénzügy modul Főkönyv modul Készlet modul Tárgyi eszköz modul Élelmezés modul Kötelezettségvállalás modul Szerződés, rendelés modul Leltár modul Térítési díj nyilvántartó modul Gépjármű üzemeltetési modul
NYILVÁNTARTÓ	Axon Számtech Kft Sümeg	Letéti könyvelési program (int.lakók pénzkezelése)
KGR	Magyar Államkincstár	Munkaügyi nyilvántartás
RECEPT KÉSZÍTÉS	Vita-Soft Bt.	Recept felírása, készítése
SZ2000W	Oépssoft Bt.	Elhelyezésre várók nyilvántartása Lakó- és gyógyszernyilvántartó program Térítési díj értesítés
KONTROLLER	Net-Team Zrt Budapest	Iktatóprogram
OTP ÜGYFÉLTERMINÁL	OTP Bank Nyrt Budapest	Költségvetési elszámolási számlák, továbbá a lakók közös letéti számlájának pénzforgalma