Almási Balogh Pál Kórház

3600 Ózd, Béke u. 1-3.

Iktató szám: 11.051-42/2013.

INFORMATIKAI VÉDELMI SZABÁLYZAT

Hatályba lépés ideje
2013. augusztus 01.

Készítette:

Körmendi János
döntéselőkészítési osztályvezető

Jóváhagyta:

Dr. Eszenyi Géza
főigazgató

Módosítások jegyzéke:

Módosította Aláírás/dátum	Változat száma	Módosított oldalszám	Jóváhagyta Aláírás/dátum	Ellenőrizte Aláírás	Kibocsátás időpontja

INFORMATIKAI VÉDELMI SZABÁLYZAT

Az Almási Balogh Pál Kórház (továbbiakban kórház) Informatikai Védelmi Szabályzata (továbbiakban IVSZ) a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló többször módosított 1992. évi LXIII. törvény, a számvitelről szóló 2000. évi C. törvény, valamint az államtitok és szolgálati titok informatikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezése alapján a következők szerint rendelkezik:

1.A Informatikai Védelmi Szabályzat célja

Az IVSZ alapvető célja, hogy a számítástechnika alkalmazása során biztosítsa az intézménynél az alábbiakat:

- titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- munkaállomásokon (USER) lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,

- a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt, a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

A jelen IVSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.
Szabályozza a informatikai eszközök használatának, és a szoftverkészítés folyamatának adatvédelmi biztonsági szabályait.

2. A Informatikai Védelmi Szabályzat hatálya

Az IVSZ személyi hatálya a kórház valamennyi fő- és másodállású, mellék-, és részfoglalkozású dolgozójára, illetve az informatikai eljárásban résztvevő más szervezetek dolgozóira egyaránt kiterjed.

Tárgyi hatálya kiterjed

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül (elsődleges adathordozók a bizonylatok, különböző tablók stb.),
- a szervezet tulajdonában lévő, illetve az általa bérelt valamennyi számítástechnikai berendezésre, valamint a gépek műszaki dokumentációira is,
- a informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

3. A szabályzathoz kapcsolódó szabályozások

A rendelet értelmében, ha a szervezet alapbiztonsági fokozatba tartozik, akkor technikai, technológiai, bizonylati fegyelem betartását, a dokumentációk meglétét az egységes eljárások előírásait és a hatékony működést biztosító feltételeket kell rögzíteni.

Az IVSZ-t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Ügyrend,
- Bizonylati szabályzat,
- Leltárkészítési és leltározási szabályzat,
- Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata,
- Intézet adatvédelmi szabályzata,
- Belső ellenőrzési szabályzat.

4. Védelmet igénylő adatok, eszközök köre

4.1. A védelem tárgya:

- az alkalmazott hardver eszközök és azok működési biztonsága,
- a informatikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk,
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága,
- személyhez fűződő és vagyoni jogok (jogtalan belső és minden külső fél),
- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai.

4.2. A védelem eszközei:

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

5. A védelem felelőse

A védelem felelőse az intézet informatikai vezetője (továbbiakban informatikai adatvédelmi felelős) és az üzemeltetés-vezető rendszergazda (informatikus).

A jelen szabályzatban foglaltak szakszerű végrehajtásáról, valamint az egységes adatvédelemi munka megszervezéséről az intézet adatvédelmi felelősének kell gondoskodni.

Az adatvédelmi felelős a kórház vezetőjének van közvetlenül alárendelve.

5.1. Informatikai adatvédelmi felelős feladatai:

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellátja a informatikai titokvédelmi munka szervezését és felügyeletét,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős a informatikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésnek ellenőrzése,
- az IVSZ kezelése, naprakészen tartása, módosítások átvezetése,
- felelős az intézmény számítógépes rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,

- ellenőrzi az intézetnél a beszerzett, illetve üzemeltetett hardver és szoftver nyilvántartásokat,
- 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,
- ellenőrzi a rendszer önadminisztrációját,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- tevékenységéről rendszeresen beszámol az államháztartás szervezete (intézmény, hivatal) vezetőjének.

5.2. A informatikai adatvédelmi felelős ellenőri feladatai:

- évente egy alkalommal részletesen ellenőrzi az IVSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot,
- előzetes bejelentési kötelezettség nélkül ellenőrzi a informatikai munkafolyamat bármely részét,
- adatvédelmi szempontból ellenőrzi az IVSZ naprakészségét, illetve azok végrehajtását.

5.3. A informatikai adatvédelmi felelős jogai:

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

5.4. A rendszergazda feladata, kötelezettségei

Feladata: a számítógépes bázis üzemeltetése és az ehhez kapcsolódó informatikai szolgáltatások biztosítása.

Kötelezettségei:

- biztosítja az üzemképességet és megszervezi a műszaki ellátást,
- engedélyezi a rendszerszoftver módosítását,
- dönt háttérgépre való áttérésről és megszervezi az át-, illetve visszatérés lebonyolítását,
- irányítja és ellenőrzi a számítógépes munkahelyeken folyó munkát,
- közreműködik a hardver és szoftver eszköz bázis fejlesztésében, és az eldöntött fejlesztésről írásbeli véleményt ad,
- segíti és szükség esetén helyettesíti a Informatikai védelmi felelős munkáját.

6. Az IVSZ alkalmazásának módja

Az IVSZ megismerését az érintett dolgozók részére az adatvédelmi felelős általa kijelölt informatikus, oktatás formájában biztosítja. Szükség esetén erről nyilvántartást vezet.

A Informatikai védelmi szabályzatban érintett munkakörökben az egyes munkaköri leírásokat át kell vizsgálni és ki kell egészíteni az IVSZ előírásainak megfelelően.

6.1. A Informatikai védelmi szabályzat karbantartása

Az IVSZ-t a számítástechnikában - valamint az intézményi fejlesztések során bekövetkezett változások miatt időközönként aktualizálni kell. Ez a informatikai adatvédelmi felelős feladata. E tevékenységről, annak konkrét tartalmáról évente egyszer írásbeli beszámolót kell készíteni, az intézeti adatvédelmi felelős részére.

6.2 Adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie:

- erkölcsi feddhetetlenség,
- informatikai ismeretek szintjén:

= informatikai hardver eszközök és a védelmi technikai berendezések ismerete,

= üzemeltetésben jártasság,

= szervezőkészség,

– a szakterületre vonatkozó jogi szabályozás ismerete.

6.3. Az adatvédelmi felelős megbízatása

A felelőst a kórház főigazgatója az intézeti adatvédelmi felelős javaslatnak figyelembevételével bízza meg. Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

6.4. 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 adat (ezek titoknak minősülnek).

A számítógépes 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 mindenkori előírásainak.

7. Informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas számítógépek és egyéb hardver berendezések fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel, a veszélyhelyzetek elháríthatók legyenek.

7.1. Elemi csapások, környezeti ártalmak

1. Elemi csapás: földrengés, árvíz, (a keletkezett kár csak a biztosító kártérítésével ellensúlyozható).
2. Környezeti kár:
   - légszennyezettség, nagy teljesítményű elektromágneses térerő,
   - fokozott tűz- és robbanásveszély.

(Ezeket a körülményeket a létesítmény építésénél, illetve az épület használatba vétele előtt figyelembe kell venni).

3. Közüzemi szolgáltatásba bekövetkező zavarok:
   - feszültség-kimaradás,
   - feszültségingadozás,
   - vízhiány.

7.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás

- behatolás a 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,
- illegális másolattal vírusfertőzött szoftver behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása (hibás működést, vagy az eszközök meghibásodását idézheti elő).

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

8.Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások:

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,

- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

A rendszerek megvalósítása során előforduló veszélyforrások:

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása (működés hiányos ellenőrzése).

A működés és fejlesztés során előforduló veszélyforrások:

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

9. A informatikai eszközök környezetének védelme

9.1. Vagyonvédelmi előírások

- a szerverszoba helyiségeit biztonsági zárakkal kell felszerelni,
- csak az illetékes dolgozók tartózkodhatnak a szerverszobában,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- az irodahelyiségben elhelyezett informatikai eszközöket csak a kijelölt dolgozók használhatják,
- a informatikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

9.2. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni (erről nyilvántartást kell vezetni),
- a használni kívánt adathordozót (floppy, 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 más szervezetnek átadni csak engedéllyel szabad (az átadást csak a vezető engedélyezheti),

- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

9.3. Tűzvédelem

A szerverszoba a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

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

Ebben meg kell határozni az alábbiakat:

- tűzvédelmi eljárásokat,
- tűzmentesítési eljárásokat,
- menekülési útvonalakat,
- fontosabb mentési eljárásokat.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a szerverszoba és az adatállomány-tároló helység között.

Az intézmény azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os csak halonnal oltó tűzoltó készüléket kell elhelyezni. Nagyobb tűzoltó készüléket 1-nél több számítógép esetén kell használni.

A nagy fontosságú, pl. törzsadat-állományokat 2 pld-ban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.

Ezen adatállományok kijelölése a rendszergazda feladata.

10. A számítástechnika alkalmazásánál felhasználható védelmi eszközök és módszerek

10.1. A szerverszoba és a számítógépet befogadó irodahelyiség védelme

Elemi csapás illetve részleges vagy teljes károsodásakor a lehetséges intéznivalókat a „**KATASZTRÓFA-TERV**" tartalmazza:

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

10.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetés, karbantartás és szervizelés rendjét külön utasításban kell szabályozni.

A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- tapasztalatokat,
- hardver tesztek által feltárt hibákat.

10.3. A számítástechnika-alkalmazás folyamatának védelme

10.3.1. Az adatrögzítés védelme

- az 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,
- adatrögzítés szoftver védelme (a programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biz-

tosítani kell). Biztosítani kell a rögzített tételek visszakeresésének és javításának lehetőségét,

- hozzáférési lehetőség:
  = a bejelentkezési azonosítók használatával lehet szabályozni, hogy ki milyen szinten férhet hozzá (Alapelv: a tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá),
- adatrögzítés folyamatához kapcsolódó dokumentációk
  = adatrögzítési utasítások,
  = ellenőrző rögzítési utasítások,
  = tesztelő és törlő programok kezelési utasításai,
  = megőrzési utasítások,
  = gépkezelési leírások.

10.3.2. Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani.

A informatikai berendezések üzemeltetéséért a Döntéselőkészítési Osztályvezető köteles gondoskodni a feldolgozások igényeinek megfelelő mágneses adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

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

10.3.3. Adathordozók tárolása

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

Adathordozót a kórházból ki-, illetve oda bevinni csak az üzemeltetésért felelős vezető engedélye alapján lehet.

10.3.4. File-ok védelme

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó mágneses lemezekről másolatot kell időnként készíteni.
A másolt lemezek csak az illetékes vezető engedélyével adhatók ki.

10.4. Szoftver védelem

10.4.1. Rendszerszoftver védelem

A rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

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

10.4.2. Felhasználói programok védelme

10.4.2.1. Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést biztosítani kell, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

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

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

- a program azonosítója,
- a program készítőjének neve,
- a feldolgozási rendszer megnevezése.

A program dokumentáció a rendszerdokumentációnak része.

10.4.2.2. Programok megőrzése, nyilvántartása

- a programokról naprakész nyilvántartást kell vezetni,

- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A számvitelről szóló 2000. évi C. törvény értelmében szervezetünknek az éves beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában, valamint az adatok feldolgozásánál alkalmazott, működőképes állapotban tárolt számítógépes programot legalább 10 évig meg kell őrizni.
A programok nyilvántartásáért és működőképes állapotban való tartásáért felelős a rendszergazda.

10.4.2.3. Programok fizikai védelme

A védelem érdekében a felhasználás helyétől elkülönítetten, behatolástól védetten egy-egy duplikált példányt kell tárolni a programkönyvtárba elhelyezett programokról.

10.5. Információk védelme az adatfeldolgozási rendszer egyes szakaszaiban

a./Fejlesztés, tervezés fázisa

Fontos a tartalmilag helyes adatok előállítása, a rendszer biztonságos üzemeltetése és a veszélyek elleni védekezés.
Az eredmény megjelenítése (papíralapú, képernyő) tervezésekor ügyelni kell a szükséges és elégséges információmennyiség biztosításáról. Gondoskodni kell az eredményadatok ellenőrzési módszereinek kidolgozásáról.

A bemeneti információk és adathordozók tervezésekor fokozottan kell ügyelni az ellenőrzési szempontok beépítésére.

b./ Szervezési fázis

A felhasználó igénye szerint minősíteni kell az előkészítendő rendszert. A minősítést a rendszer szervezési dokumentációjában rögzíteni kell.

El kell készíteni az adatok kimentésének és a kiindulási adatok meghatározott idejű megőrzésének előírását.

c./ Programozási fázis

- törekedni kell az áttekinthető programok készítésére,
- kísérő információkkal kell ellátni a programokat, így később szükségessé váló módosítások nagyobb biztonsággal és kevesebb ráfordítással végezhetők el,
- a programstruktúrát modulárisan kell felépíteni,

- a modulok inputját - outputját egyértelműen definiálni kell,
- biztosítani kell, hogy a tesztelés teljes körű legyen.

10.6. Dokumentálás

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

- rendszer megnevezése,
- dokumentáció típusa,
- a rendszer adatvédelmi minősítése,
- a kidolgozók névsora,
- példányszám és tárolás helye,
- az átadás ideje,
- módosítások megnevezése és ideje.

11.A központi számítógép(ek) és a hálózat munkaállomásainak működésbiztonsága

11.1. Központi gépek (Server)

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gépek háttértárairól naponta biztonsági mentést kell készíteni. A mentés heti forgóban felülírással készüljön, így mindig 1 heti adatvisszaállítást kell lehetővé tenni.
Az alkalmazott hálózati operációs rendszer (Windows, Linux) adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

11.2. Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet.

Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell. Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.

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

A kórház számítógépeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

Olyan floppy lemezeket, melyeken a formattálás után az operációs rendszer rossz szektorokat mutat ki, tilos felhasználni.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

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

12. Kiegészítő rendelkezések

13. Záradék

A IVSZ az intézmény Szervezeti és Működési Szabályzatának mellékletét képezi

2013. augusztus hó1-napjával

lép hatályba.

A személyes és közérdekű adatok védelmére vonatkozóan részletes útmutatás az 1992. évi LXIII. törvény tartalmazza.

Ózd, 2013. augusztus 1.

.....
főigazgató

1. sz. melléklet

GÉPTERMI (SZERVERSZOBA) REND

1. A szerverszobába az oda munkavégzésre beosztottakon kívül csak az alábbi személyek tartózkodhatnak:
   - az intézmény vezetője,
   - az intézet adatvédelmi felelőse,
   - műszaki szakemberek.

   Más személyek benntartózkodását csak a informatikai adatvédelmi felelőse engedélyezheti.

2. A gépterembe ételt, italt bevinni, és ott elfogyasztani TILOS !

3. SZIGORÚAN TILOS a gépteremben égő cigarettával belépni, illetve ott dohányozni!

4. A berendezések belsejébe nyúlni TILOS! Bármilyen, nem a gépkezeléssel összefüggő beavatkozást csak szakember végezheti.

5. A számítógépeket csak rendeltetésszerűen és kizárólag az ütemezett munkák elvégzésére lehet használni.

6. Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet!

7. A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabványok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármilyen beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

   A fenti rendelkezések megsértése esetén fegyelmi felelősségre vonás kezdeményezhető.

2. sz. melléklet

ADATHORDOZÓK NYILVÁNTARTÁSA

Optikai lemezek nyilvántartása

Mentésekben résztvevő optikai lemezek:
Külön optikai lemezt kell fenntartani a heti rendszermentésekhez.
A rendszerprogramokat tartalmazó optikai lemez külső borítóján és a belső fedőlapon a következő adatokat kell feltüntetni:

- lemez azonosítója,
- lemez tartalma,
- mentés kelte.

Minden optikai lemezről külön nyilvántartást kell vezetni a következő adatokkal:

- lemez azonosítója,
- utolsó aktualizálás ideje,
- lemez tartalma (pl. rögzítési adatok vagy rendszerprogramok).

Megőrzési idő: 1-5 év.