**Bajai Szent Rókus Kórház**
**6500 Baja, Rókus u. 10.**
**Tel.: 79/422-233, Fax: 79/425-575**

# MŰKÖDÉSI SZABÁLYZAT

# INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

**A PÉLDÁNY SORSZÁMA: ……**

**A PÉLDÁNY TULAJDONOSA:**

**NÉV:** ……..
**MUNKAKÖR:** ……..
**OSZTÁLY/RÉSZLEG:** ……..



Vonatkozó minőségirányítási eljárás: **ME 04-04 Egészségügyi feljegyzések számítógépes készítése, tárolása**

# TARTALOM

2011. 05. 20.

# MELLÉKLET

1. Nyilatkozat
2. Adatkezelési nyilatkozat
3. Géptermi rend

## 1. CÉL

Az Informatikai Biztonsági Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a Bajai Szent Rókus Kórháznál az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek az érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat 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.

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

## 2. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT HATÁLYA

### 2.1. Személyi hatálya

Az IBSZ személyi hatálya az intézmény valamennyi 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 intézmény 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.

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt minőségügyi dokumentumokkal összhangban kell alkalmazni:

- Adatvédelmi Szabályzat

- Szervezeti és Működési Szabályzat,
- Leltározási szabályzat,
- Hasznosítási és selejtezési szabályzat.

## 3. AZ IBSZ BIZTONSÁGI FOKOZATA

Intézményünk alapbiztonsági fokozatba tartozik. Intézményünk általános informatikai feldolgozást végez.

## 4. 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.

### 4.1. 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, előírásszerű felhasználására, reprodukálhatóságára,
- a személyhez fűződő és vagyoni jogokra.

### 4.2. 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.

## 5. A VÉDELEM FELELŐSE

A védelem felelőse az intézményi adatvédelmi felelős. A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézményi adatvédelmi felelősnek kell gondoskodnia.

### 5.1. Az intézményi adatvédelmi felelős feladatai

- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét,
- kialakítja a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával a biztonságot növelő intézkedéseket,
- felelős az 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,
- az adatvédelmi feladatok ismertetése, oktatása,
- a védelmi rendszer érvényesülésének ellenőrzése,
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- felelős az intézmény informatikai rendszere hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért,
- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- 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 intézmény vezetőjének.

### 5.2. Az intézményi adatvédelmi felelős 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.

### 5.3. Az intézményi adatvédelmi felelős jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény 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.

### 5.4. Az intézményi 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.
- az informatika szintjén:
  - az informatikai hardver eszközök és a védelmi technikai berendezések ismerete,
  - üzemeltetésben jártasság,
  - szervezőkészség.
- a szakterületre vonatkozó jogi szabályozás ismerete.

### 5.5. Az intézményi adatvédelmi felelős megbízása

Az intézményi adatvédelmi felelőst az intézményvezető bízza meg. Az intézményi adatvédelmi felelős megbízólevél alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

## 6. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT ALKALMAZÁSÁNAK MÓDJA

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére az intézményi adatvédelmi felelős oktatás formájában biztosítja (1.sz.melléklet), melyről nyilvántartást vezet.

### 6.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.
Az Informatikai Biztonsági Szabályzat folyamatos karbantartása az intézményi adatvédelmi felelős feladata.

### 6.2. 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.
Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.
A hivatali titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.
A kijelölt dolgozók előtt a titokvédelmi 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 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 hetente át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének azonnal jelenteni kell.
A naplófájlok áttekintéséért, értékeléséért a *rendszergazdák* felelősök.
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 (2.sz. melléklet).
A hivatkozott munkakörben dolgozó új belépővel a Bér-, munka-, és személyügyi osztály íratja alá a nyilatkozatot egy példányban, mely a dolgozó személyi anyagának részét képezi.
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).

## 7. 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.

### 7.1. 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.

### 7.2. 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 jelszó gyakori *(napi, heti)* megváltoztatásának az elmulasztása,
- 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.

## 8. AZ ADATOK TARTALMÁT ÉS A FELDOLGOZÁS FOLYAMATÁT ÉRINTŐ VESZÉLYEK

### 8.1. Tervezés és előkészítés során előforduló veszélyforrások

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

### 8.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

### 8.3. A működés és fejlesztés során előforduló veszélyforrások

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

# 9. AZ INFORMATIKAI ESZKÖZÖK KÖRNYEZETÉNEK VÉDELME

## 9.1. Vagyonvédelmi előírások (lásd. 3. melléklet)

- a gépterem *(informatikai szoba)* külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- csak az illetékes dolgozók tartózkodhatnak a gépteremben,
- a gépterem kulcsának felvétele illetve leadása csak aláírás ellenében történhet,
- munkaidőn túl a gépteremben csak engedéllyel lehet dolgozni,
- a számítógép monitorát úgy kell elhelyezni, hogy a megjelenő adatokat illetéktelen személyek ne olvashassák el,
- a gépterembe történő illetéktelen behatolás tényét az intézmény vezetőjének azonnal jelenteni kell,
- az informatikai eszközöket csak a kijelölt dolgozók használhatják,
- az 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, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (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.

## 9.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.
A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell. Külön tűzszakaszt kell képezni a gépterem és az adatállomány- tároló helyiség között.
A gépteremben csak a napi munkavégzéshez szükséges mennyiségű gyúlékony anyagot szabad tárolni (pl. leporellót).
A gépteremben dohányozni tilos!
A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni.
Ezen adatállományok kijelölése az informatikai csoport-koordinátor feladata.

# 10. AZ INFORMATIKAI RENDSZER ALKALMAZÁSÁNÁL FELHASZNÁLHATÓ VÉDELMI ESZKÖZÖK ÉS MÓDSZEREK

## 10.1. A gépterem (informatikai szoba) 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, 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,
- a tapasztalatokat,
- a hardver tesztek által feltárt hibákat.
- Alapgép szétbontását (kivéve a garanciális gépeket) csak a hardver karbantartó személy(ek) végezheti el. Billentyűzet, monitor, nyomtató cseréjének idejét dokumentálni kell.

## 10.3. Az informatikai feldolgozás folyamatának védelme

### 10.3.1. 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 adatrögzítés szoftver védelme. A programokat ellenőrző funkciókkal kell ellátni, ellenőrző számok, kontrollösszegek használatát biztosítani kell. Biztosítani kell továbbá 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 szervezeti egységek személyei férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerver*(ek)* rendszergazda jelszavát és az operációs rendszerek rendszergazda jelszavát lezárt borítékban, zárható szekrényben kell tárolni. A boríték felbontását dokumentálni kell.
- adatrögzítési folyamat bizonylatolása.

A másodlagos adathordozókat kísérő jeggyel kell ellátni melynek tartalma:

- témaazonosító, bizonylat neve,
- rekord (tételszám),
- rögzítést ill. ellenőrzést végző személyek nevei.
- 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.
Az informatikai eszközök üzemeltetéséért az informatikai csoport-koordinátor felelős.
Köteles gondoskodni a feldolgozások igényeinek megfelelő adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.
Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval kell ellátni. Az azonosítókat mind emberi, mind informatikai olvasásra alkalmas formába kell feltüntetni.
Az operációs rendszer adta lehetőségek figyelembe vételével biztosítani kell a külső és belső címek azonosságát.
A belső címke felépítésével illetve használatánál figyelembe kell venni a megőrzési időpont ellenőrzésének szükségszerűségét (aktuális ellenőrzés).
Tilos a privát adathordozókat szolgálati célra igénybe venni, illetve tilos szolgálati adathordozókat magáncélra igénybe venni.

### 10.3.3. Adathordozók tárolása

Az adathordozók tárolására a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.
Adathordozót a részlegből ki-, illetve oda bevinni csak az informatikai csoport-koordinátor engedélye alapján lehet.
Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet.

### 10.3.4. Az adathordozók nyilvántartása

Az adathordozókról nyilvántartást kell vezetni.
Az azonosító adaton kívül a felírás és megőrzés dátumát, védettség tényét, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell tartalmaznia.
A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.
A nyilvántartás vezetéséért: a rendszergazdák felelősök.

### 10.3.5. Az adathordozók megőrzése

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

### 10.3.6. Az adathordozók karbantartása

Az adathordozók állapotát 5 évenként ellenőrizni kell.

### 10.3.7. Selejtezés, sokszorosítás, másolás

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.
**Selejtezni kell:**

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából következően felhasználásra alkalmatlan (deformálódott) mágneslemezt, CD-t, DVD-t, ha a kapacitás a névleges érték 75 %-ánál kevesebb,
- véglegesen elhasználódott anyagot *(pl. leporelló).*
- Az alkalmatlan mágneslemezeket, CD-ket DVD-ket fizikai roncsolással használhatatlanná kell tenni.
- Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adathordozókról, törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. *(Az üzemi másolás nem minősül másolásnak.)* Biztonsági illetve archív adatállomány előállítása másolásnak számít.

### 10.3.8. Mentések, fájlok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A szerverek mentését naponta el kell végezni. A mentés automatikus és az éjszakai órákban fut. A mentett állományoknak tartalmazniuk kell a rendszerek installálása során létrehozott konfigurációs, és a rendszerek működtetése során keletkezett valamennyi adatot. Tartalmazniuk kell továbbá az operációs rendszer (Windows, Linux) konfigurációs állományait. A fenti adatok mentése lehetővé teszi, hogy egy szerver teljes károsodás esetén is új gépre az operáció rendszer újratelepíthető a felhasználói beállításokkal, illetve maguk az adott rendszerek is teljes értékűen visszaállíthatók.
Az operációs rendszerek 1-1 példányban mentendők és a mentésekre előírt módon tárolandók. A rendszerszoftverek 1-1 példányban mentendők. Az intézmény Gazdasági rendszere valamennyi eleme adatállományai naponta mentendők. Az intézmény Egészségügyi rendszere valamennyi eleme adatállományai naponta mentendők. A munkák során a munkaállomások adathordozóján létrehozott dokumentumok mentése az azt létrehozó munkatársak *(felhasználók)* feladata. Amennyiben a felhasználó ezen állományokat a rendszergazda által megadott szerver adott munkaterületére bemásolja, és mentései igényét írásban kéri, ezen állományok mentése is az automatikus napi mentésekkel megtörténik. Dokumentálni kell, hogy ki és mikor végezte el a mentést. A fenti mentések adathordozói a mentésekre előírt módon tárolandók. Az intézmény Gazdasági rendszere mentéséért a gazdasági rendszerek

rendszergazdája rendszergazda felelős. Az intézmény Egészségügyi rendszere mentéséért az egészségügyi rendszerek rendszergazdája rendszergazda felelős.

## 10.4. Szoftver védelem

### 10.4.1. Rendszerszoftver védelem

Az üzemeltetésért felelős 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 csak a rendszergazdának van jogosultsága
- a módosítással egy időben, a dokumentációban is a változásokat át kell vezetni,
- a változtatásokról nyilvántartást kell vezetni.

### 10.4.2. 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, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek. Lokális gépekre programot csak a rendszergazda tudtával lehet telepíteni. A telepítést dokumentálni kell. A dokumentálásnak tartalmaznia kell azt, hogy milyen programot, mikor és ki telepített fel a számítógépre. A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt. A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

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

A program dokumentáció a rendszerdokumentációnak része.

**Programok megőrzése, nyilvántartása**

- a programokról naprakész nyilvántartást kell vezetni,
- a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.
- A számvitelről szóló többször módosított 2000. évi C. törvény értelmében intézményünk 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 informatikai csoport-koordinátor felelős.

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

### 10.5. Dokumentálás

Kiemelkedő szerepe van a megfelelő szintű és részletezésű 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 felülírással készül, így mindig 1 nappal korábbi állapotú adat visszaállítást kell lehetővé tenni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftver eszközökről biztonsági másolatot kell készíteni. Az eredeti példányokat a másolatoktól fizikailag el kell különíteni.

### 11.2. Munkaállomások (USER-ek)

A hálózatra idegen programot, adatot másolni csak a rendszergazdával történt egyeztetés után lehet. Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén a rendszergazdát azonnal értesíteni kell.
Vírusmentesítő programot futtatni csak a rendszergazda felügyelete mellett szabad.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.
Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.
A hálózati vezeték *(UTP)* 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 a rendszergazda tudta és engedélye nélkül nem szabad.

## 12. ELLENŐRZÉS

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