SZÁMÍTÁSTECHNIKAI VÉDELMI SZABÁLYZAT

A példány sorszáma:

A példány tulajdonosa:

Számítástechnikai Védelm
i Szabályzat (SZVSZ)

Tartalomjegyzék

A Dr. Kenessey Albert Kórház- Rendelőintézet Számítástechnikai Védelmi Szabályzatát - a továbbiakban SZVSZ - az Államtitok és Szolgálati titok számítástechnikai védelméről szóló 3 / 1988. / XI.22. / KSH rendelkezése, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. Évi LXVI. Törvény, a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. tv., az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. tv., a 2011.évi CXII. tv. valamint az MT, a KJT és egyéb idevonatkozó jogszabályok alapján a következők szerint határozom meg :

1., SZVSZ célja, általános rész

Az SZVSZ alapvető célja, hogy a számítástechnika alkalmazása során biztosítsa az intézményünknél az alábbiakat :

- titok- és vagyonvédelemre vonatkozó 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 lekérdezhető és alkalmazható adatok körének meghatározását
- adatállományok biztonságos mentését
- a számítógépes rendszerek zavartalan működését
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását
- az adatvédelem és adatbiztonság feltételeit
- a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a meg-tervezéstől kezdve az üzemeltetésen keresztül a felhasználásig

A jelen SZVSZ az adatvédelem általános érvényű előírásait tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Szabályozza a számítástechnikai eszközök használatának, a szoftverkészítés folyamatának adatvédelmi biztonsági szabályait. Előírja a zavartalan működéshez szükséges karbantartás és ellenőrzés szükséges lépéseit.

2., Szabályzathoz kapcsolódó szabályozások

Az SZVSZ az alábbiakban felsorolt előírásokkal összhangban készült, az ott leírtak figyelembe vételével kell alkalmazni.

- *Felesleges vagyontárgyak selejtezésének szabályzata*
- *Leltározási szabályzat*
- *Intézeti iratkezelési, dokumentációs és adatvédelmi szabályzat*
  / utóbbihoz szervesen kapcsolódik /

3., Az SZVSZ hatálya

Az SZVSZ személyi hatálya az intézmény valamennyi fő- és másodállású, mellék- és részfoglalkozású dolgozójára, illetve a számítástechnikai eljárásban résztvevő valamennyi személyre és más szervezetek dolgozóira egyaránt kiterjed. A számítástechnikai eszközt alkalmazó személy munkaköri leírásának tartalmaznia kell az SZVSZ előírásainak kötelező elsajátítását és alkalmazását.

Tárgyi hatálya kiterjed :

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül / elsődleges adathordozók, bizonylatok, biztonsági másolatok, nyomtatott formátum, stb. /
- az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi számítástechnikai berendezésre, valamint az eszközök műszaki dokumentációira is
- a számítástechnikai folyamatban szereplő összes dokumentációra / fejlesztési, programozási, üzemeltetési, stb. /
- a rendszer- és felhasználói programokra
- az adatok felhasználására vonatkozó utasításokra
- az adathordozók tárolására és felhasználására

4., SZVSZ értelmező rész, adatkezelés, adatvédelem, adatbiztonság

1. *Adatkezelő* : az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a személyes adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetve a végrehajtással adatfeldolgozót bízhat meg. Egészségügyi intézmény vonatkozásában adatkezelő – az egészségügyi és személyazonosító adatok kezelésére jogosult - a betegellátó, az intézményvezető és az adatvédelmi felelős.

2. *Adatfeldolgozó* : az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából az egészségügyi és személyazonosító adatok feldolgozását végzi. Az adatfeldolgozó tevékenységi körén belül. Illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

3. *Adatkezelés* : az alkalmazott eljárástól függetlenül a személyes adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is.

4. *Adatfeldolgozás* : az adatkezelési műveletek, technikai feldolgozások elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.

5. *Betegellátó* : a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, valamint gyógyszerész.

6. *Egészségügyi adat* : az ellátott testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó, általa vagy róla más személy által közölt, illetve az egészségügyi ellátóhálózat által észlelt, vizsgált, mért, leképzett vagy származtatott adat, továbbá az előzőekkel kapcsolatba hozható, az azokat befolyásoló mindennemű adat.

7. *Egészségügyi dokumentáció* : a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától.

8. *Elektronikus irat* : számítástechnikai program felhasználásával - elektronikus formában rögzített - elektronikus úton érkezett, illetve továbbított irat, amelyet elektronikus adathordozón tárolnak.

9. *Gyógykezelés* : minden olyan tevékenység, amely az egészség megőrzése, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógyítása, a megbetegedés következtében kialakult állapotromlás szinten tartása vagy javítása céljából az érintett közvetlen vizsgálatára, kezelésére, ápolására, orvosi rehabilitációjára, illetve mindezek érdekében az érintett vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerek, gyógyászati segédeszközök, gyógyfürdőellátások kiszolgálását, a mentést és betegszállítást, valamint a szülészeti ellátást is.

10. *Iratkezelési szabályzat* : az intézmény írásbeli ügyintézésére vonatkozó szabályok összessége, amely az intézmény szervezeti és működési szabályzata figyelembevételével készül.

11. *Orvosi titok* : a gyógykezelés során az adatkezelő és adatfeldolgozó tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve a befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat. Az adatkezelő és adatfeldolgozó az orvosi titkot köteles megtartani.

12. *Számítástechnikai adathordozó* : számítástechnikai eljárással adatokat rögzítő, tároló adathordozó (mágnesszalag, hajlékony és merev lemez, CD-DVD ROM, pendrive, stb.), amely az adatok nyilvántartását, azonosítását, kezelését és visszakeresését biztosítja.

13. *Személyazonosító adat* : a családi és utónév, a leánykori név, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely és a tartózkodási hely, a társadalombiztosítási azonosító jel együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására.

14. *Szervezeti és működési szabályzat (SZMSZ)*: az intézmény tevékenységének alapdokumentuma, amely rögzíti az intézmény, azon belül a szervezeti egységek feladatait és a feladatokhoz rendelt hatásköröket.

Adatkezelés, adatvédelem, adatbiztonság

Az egészségügyi intézményben az SZVSZ hatálya alá tartozó dolgozó számára az adatkezelés, adatvédelem és adatbiztonság kérdéskörét szabályozza az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. tv. Az adatvédelmi felelős feladata az ezzel kapcsolatos eljárási utasítás kidolgozása és megismertetése az intézmény dolgozóival.

Alapvetően adatkezelőnek számít valamennyi intézményi dolgozó, így a munkája során tudomására jutott valamennyi egészségügyi és személyazonosító adat orvosi titoknak számít, köti az orvosi titoktartás felelőssége. A számítástechnikai adatkezelés és adatvédelem ennek figyelembe vételével kell történjen.

Adatkezelés = egészségügyi és személyazonosító, valamint minden egyéb gyógykezeléssel kapcsolatos adat kezelése, rögzítése, felhasználása, továbbítása. Az egészségügyi és személyes adatok 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.

Adatvédelem = orvosi titoknak minősülő valamennyi egészségügyi és személyazonosító, illetve a gyógykezeléssel kapcsolatos összes adat megfelelő kezelése, biztosítva, hogy illetéktelen személy vagy felhasználó azokhoz ne férhessen hozzá.

Adatbiztonság = A számítástechnikai alkalmazás, adatrögzítés során azon megfelelő eljárások alkalmazása, mellyel biztosítható, hogy a kezelt adatok ne vesszenek el, ne sérüljenek, ne károsodjanak, visszakereshetőek legyenek, adatkezelésre jogosulatlan személy ne férhessen hozzá.

Számítógépes iktatás és iratkezelés

Számítógépes iktatásnál ugyanazokat a követelményeket kell teljesíteni, mint a hagyományos iktatásnál. A programnak biztosítania kell az ügyenkénti nyomtathatóságot. A számítógépes nyilvántartás nem helyettesítheti azokat az átadókönyveket, amelyekben az átadás - átvétel tényét a sajátkezű aláírás bizonyítja. A számítógépes rendszerbe vitt érkeztetési és iktatási adatok utólagos módosításának tényét a jogosultsággal rendelkező ügyintéző azonosítójával és a javítás idejének megjelölésével naplózni kell, ugyanitt rögzíteni kell a módosítás előtti szövegrészt is.

Az adatvédelmi szabályok megtartásával, az iktatási adatbázist hozzáférhetővé kell tenni mindaddig, amíg az az ügyintézéshez szükséges. Az iktatási adatbázisról naponta mentést kell készíteni.
Az elektronikus adatbázist év végén hitelesítve le kell zárni.

A nem papíralapú, elektronikus adathordozón érkezett iratok (Pl. CD, DVD ROM stb.) mellé kísérőlapot kell csatolni és ezeket együtt kell kezelni. A kísérőlapon fel kell tüntetni az adathordozó iktatószámát, tartalmi paramétereit. Egy adathordozón csak egy témához tartozó iratok adhatók át.

Elektronikus posta, elektronikus adattovábbítás esetén biztosítani kell a fentebbiek figyelembevételével az adatvédelmet és adatbiztonságot, ki kell zárni illetéktelen személy hozzáférhetőségét.

Továbbiakban az adatkezelés, adatvédelem és adatbiztonság eszközeit összevontan értelmezzük.

5., Védelmet igénylő tárgyak, adatok, a védelem eszközei

A védelem tárgya :

- az alkalmazott hardver eszközök és azok működési biztonsága
- számítástechnikai eszközök üzemeltetéséhez szükséges okmányok és dokumentumok
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásukig
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága
- személyhez fűződő és vagyoni jogok / jogtalan belső és minden külső fél elkerülése /
- az alkalmazott biztonsági intézkedések, azok tervei, előírásai és eljárási szabályai

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.

6., A védelem felelőse, a rendszergazda és az üzemeltetésvezető tevékenységi köre

Az adatvédelmi felelős kijelölése

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény vezetője által kinevezett adatvédelmi felelősnek kell gondoskodni. Az adatvédelmi felelős az intézményt vezető főigazgató főorvosnak van közvetlenül alárendelve.

Adatvédelmi felelős feladatai

- ellátja az adatfeldolgozás felügyeletét
- ellenőrzi a védelmi előírások betartását
- ellátja a számítástechnikai titokvédelmi munka szervezését és felügyeletét
- a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával biztonságot növelő intézkedések kialakítása
- felelős a számítástechnikai rendszerek és eszközök üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról
- védelmi eszközök működésének, szervízellátás biztosításának folyamatos ellenőrzése
- adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása, karbantartása
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése
- adatvédelmi feladatok ismertetése, oktatása, dolgozók szükség szerinti tájékoztatása
- a védelmi rendszer érvényesülésének ellenőrzése
- az SZVSZ kezelése, naprakészen tartása, szükség szerinti módosítása
- felelős az intézmény számítógépes 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
- vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulását
- ellenőrzi a rendszer önadminisztrációját
- tevékenységéről rendszeresen beszámol az intézmény vezetőjének, évente egy alkalommal írásbeli beszámolót is készít, szükség szerint soron kívüli tájékoztatást ad

Az adatvédelmi felelős ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az SZVSZ előírásainak betartását, szükség szerint módosítási javaslatot tesz annak tartalmára
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot

- ellenőrzi a számítástechnikai munkafolyamat bármely részét előzetes bejelentési kötelezettség nélkül
- adatvédelmi szempontból ellenőrzi az SZVSZ naprakészségét, illetve azok végrehajtását

Az adatvédelmi felelős feladatait beosztottjai / köztük a rendszergazda és az üzemeltetésvezető informatikus / segítségével hajtja végre.

Az adatvédelmi felelős jogai :

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

Adatvédelmi felelős kiválasztása

Az alábbi követelményeknek kell megfelelnie :

- erkölcsi feddhetetlenség
- számítástechnikai ismeretek szintjén : számítástechnikai hardver eszközök és a védelmi technikai berendezések alapszintű ismerete, üzemeltetésben jártasság, szervezőkészség, a szakterületre vonatkozó jogi szabályozás ismerete.

Az adatvédelmi felelős megbízatása

A felelőst az intézmény vezetője bízza meg. Írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat megbízatása visszavonásáig.

A rendszergazda és üzemeltetésvezető informatikus kötelezettségei

Feladata: A számítástechnikai eszközök üzemeltetése és az ehhez kapcsolódó számítástechnikai szolgáltatások biztosítása. A szükség szerinti ellenőrzési, karbantartási feladatokat elvégzi.

Kötelezettségei:

- biztosítja az üzemképességet és megszervezi a műszaki ellátást
- véleményezi a rendszerszoftver módosítását
- irányítja és ellenőrzi az adatrögzítők / operátorok, asszisztensek, stb. / munkáját
- közreműködik a hardver és szoftver eszköz bázis fejlesztésében és az eldöntött fejlesztésről véleményt ad
- segíti az adatvédelmi felelős munkáját

A rendszergazda illetve üzemeltetésvezető lehet egy és ugyanazon személy, illetve a megbízatást több dolgozó is megkaphatja. Az adatvédelmi felelős javaslata alapján az intézmény vezetője jelöli ki őket, megbízatásuk visszavonásig érvényes.

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

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk :

- **közlésre szánt**
- **minősített adat**

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. A minősített adatok feldolgozásakor a hozzáférési jogosultságot az Iratkezelési - Dokumentációs és Adatvédelmi Szabályzatban leírtak szerint kell értelmezni és alkalmazni. A kijelölt dolgozók előtt a titokvédelmi és egyéb rendszabályokat, a betekintési jogosultság terjedelmét ismertetni kell. A minősített adatok védelmét a feldolgozás, adattovábbítás, tárolás során a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell / szoftver, hardver, adatvédelem /.

8., Számítástechnikai eszközbázist veszélyeztető helyzetek

A. Elemi csapások, környezeti ártalmak, közüzemi szolgáltatásban bekövetkező zavarok

pl. földrengés, légszennyezettség, fokozott tűz- és robbanásveszély, feszültségingadozás

Általános biztonsági óvintézkedések szükségesek, jelen szabályzatban részletezésére nem térünk ki.

B. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás

- behatolás a számítástechnikai 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

Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés, előkészítés, rendszer illetve program megvalósítása során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszközpark lehetőségeit
- hibás adatrögzítés, adatelőkészítés, az ellenőrzés hiányos betartása
- hibás adatállomány működése
- helytelen adatkezelés
- program tesztelés elhagyása, a működés hiányos ellenőrzése

A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság
- szervezetlenség
- képzetlenség
- szándékosan elkövetett illetéktelen beavatkozás
- illetéktelen hozzáférés
- üzemeltetési dokumentáció hiánya
- nem kellő jártasság az alkalmazásban

Amennyiben emberi tényezőre vezethető vissza a számítástechnikai eszközbázist ért kár, ennek kivizsgálása, az intézményvezető hatáskörébe tartozóan személyi felelősségre vonás szükséges.

9., A számítástechnikai eszközök környezetének védelme

Általános vagyonvédelmi előírások betartása

- csak az illetékes dolgozók használhatják a számítástechnikai eszközöket / munkaköri leírás tartalmazza ezen illetékességet /
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős
- a számítástechnikai eszközök illetéktelen használatának tényét az adatvédelmi felelősnek haladéktalanul jelenteni kell
- a tűzvédelem általános szabályait kell alkalmazni

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 kell elvégezni. A hardver eszközök ellenőrzését évente legalább egyszer el kell végezni hibátlan működés esetén is.

A munkák szervezésénél figyelembe kell venni :

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

Az adatvédelmi felelős által előírt ellenőrzési feladatokat az üzemeltetésvezető végzi el a 12. és a 13. fejezetben leírtak szerint.

Adathordozók védelme

- csukott helyen kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni
- a használni kívánt adathordozót használat után a tárolás helyére vissza kell tenni
- a munkaasztalon lehetőség szerint azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek
- intézményi saját adathordozót más intézménynek átadni csak engedéllyel szabad / átadást csak az intézmény vezetője vagy helyettese engedélyezheti /
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni

10., A számítástechnikai alkalmazás folyamatának védelme

Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen
- tesztelt adathordozóra lehet adatállományt rögzíteni
- a bizonylatokat és adathordozókat csak e célra kialakított és megfelelő tároló-helyen szabad tartani
- adatrögzítés **szoftver védelme** / a programokat ellenőrző funkciókkal kell ellátni /, biztosítani kell a rögzített tételek visszakeresésének és javításának lehetőségét
- **hozzáférési lehetőség** : a bejelentkezési azonosítók használatával lehet szabályozni, hogy ki milyen szinten férhet hozzá adatokhoz
  /alapelv : a tárolt minősített adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá /

Adathordozók védelme

Az adathordozók logikai védelméről, a számítástechnikai berendezések rendeltetésszerű üzemeltetéséről végső soron a rendszergazda köteles gondoskodni, beleértve a feldolgozások igényeinek megfelelő mágneses adathordozók biztosítását, 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 emberi és/vagy számítógépes olvasásra alkalmas formában kell feltüntetni.

Adathordozók tárolása

Az adathordozók tárolására külön helyet kell biztosítani, ahol sérülésmentes megőrzésük garantálható. Az adathordozók szállítása csak megfelelő módon kialakított dobozban történhet.

Nyilvántartás

Az adathordozókról egyedi azonosítóként nyilvántartást kell vezetni /L.1.sz.melléklet/
A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.
A hardver, szoftver és egyéb kiegészítő eszközök nyilvántartását külön leiratban kell rögzíteni.
/ Lásd 12. Fejezet: Számítógépek működtetésével kapcsolatos szabályok! /

Karbantartás

Az adathordozókat l évenként tisztítani, ellenőrizni kell.

Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, optikai lemezeket (CD-DVD ROM), amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Tehát:

- fizikailag sérült, javíthatatlan
- gyári, raktározási hibából fakadóan felhasználásra alkalmatlan / pl. deformálódott /
- mágneslemeznél, ha a kapacitás a névleges érték 75 %- nál kevesebb
- véglegesen elhasználódott / leporello /

Az alkalmatlan, elöregedett mágneslemezeket **fizikai roncsolással** használhatatlanná kell tenni.
Bizalmas illetve minősített adatokat tartalmazó mágneses adathordozókról törlő programokkal kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.
A selejtezést **A felesleges vagyontárgyak** s**elejtezésének szabályzat** - ának és az Intézeti iratkezelési - dokumentációs és adatvédelmi szabályzatának megfelelően kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. Ezt módosíthatja a szoftvert biztosító céggel kötött egyedi szerződés. Programozóink által készített saját programok másolása - intézményi célból való felhasználásra - korlátozás nélkül elvégezhető.

Biztonsági illetve archív adatállomány előállítása másolásnak számít.

Leltározás

A mágneses adathordozókat és optikai lemezeket a **Leltározási Szabályzatnak** megfelelően kell leltározni.

File - ok védelme

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

Felhasználói programok védelme

Programhoz való hozzáférés

A kezelés folyamán az illetékes felhasználó hozzáférését biztosítani kell, az illetéktelen próbálkozást ki kell zárni.

A programokhoz, modulokhoz, menü pontokhoz való hozzáférést a Finanszírozási és Számítástechnika Csoport állítja be. Mind az új belépők, mind az új munkahelyen, új munkakörben dolgozó személyek esetében a”Rendszerhasználati jogosultság igénylése „- lap kitöltésével (lásd: Bizonylati Albumban) történik, melyet az aktuális dolgozó közvetlen felettese hagy jóvá. A jogosultság beállítása a dolgozó beosztásának függvényében történik, úgy hogy a feladatát maradéktalanul el tudja látni.

Programok megőrzése, nyilvántartása

Lásd 1.számú melléklet !

A 9. fejezetben foglaltak felügyelete és ellenőrzése az üzemeltetésvezető informatikus feladata, munkaköri leírásának részét képezi.

11., A központi számítógép /ek/ és a munkaállomások működésbiztonsága

Központi gépek / Szerver / :

Szünetmentes áramforrást kell használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól megfelelő gyakorisággal / napi, heti, stb. / mentést kell készíteni. 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. A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

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.
Intézeti számítógépen idegen programot illetve adathordozót alkalmazni csak vírusellenőrzést követően a rendszergazdával történt egyeztetés után lehet. Intézményünkben a vírusellenőrzést a kliens gépekre telepített vírusellenőrző szoftverek (automatikusan) ill. a Finanszírozási és Számítástechnika Csoport munkatársai végzik, idegen adathordozó bemutatása nekik történjen. Egyebekben a fentebbieket értelemszerűen kell alkalmazni.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. Az intézmény számítógépeiről programot, illetve adatállományt másolni a jogos belső felhasználói igények kielégítésén kívül nem szabad.
Folyamatos igénynek kitett munkaállomáson célszerű szünetmentes áramforrást használni.

12., Számítógépek működtetésével kapcsolatos szabályok

Az ebben a fejezetben leírtak betartása minden számítástechnikai eszközt alkalmazó munkahelyi dolgozó számára kötelező, munkaköri leírásának részét képezi.

A „Számítógépek működtetésével kapcsolatos szabályok” az alábbiakat érintik:

- Hardver kezelése, védelme
- Hardver javítás igénylésének módja
- Adathordozók védelme, vírusvédelem
- Adatvédelem
- Hálózati program alkalmazásának módja

A., Hardver kezelése, védelme

- Hardver eszközöket csak azon dolgozók használhatják, akiknek ez munkaköri leírásukban szerepel. Illetéktelen személy a hardver eszközhöz nem férhet hozzá, tehát azokat zárható, vagy jól ellenőrizhető helyen (pl. kezelő, nővérszoba, iroda) kell tárolni.
- Hardver biztonságos és rendeltetésszerű használatáért a felhasználó a felelős.
- Használat befejezése után minden esetben ki kell kapcsolni a hardver eszközöket.

B., Hardver javítás igénylésének módja

- Hibát észlelő felhasználónak vagy jelzése alapján felettesének kötelessége azt jelezni a Finanszírozási és Számítástechnika Csoport részére.
- A munkahely a hiba elhárításának igénylését kizárólag a Finanszírozási és Számítástechnika Csoport rendszergazdája vagy helyettese részére adja le. Önállóan javítást nem kezdeményez.
- Rendszergazda vagy helyettese lehetőség szerint a hibát elhárítja, vagy köteles a munkahely felé visszajelezni 24 órán belül (vagy a következő munkanapon) a hibaelhárítás várható idejét.

C., Adathordozók védelme, vírusvédelem

- Adathordozót csukott helyen kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak
- Az adathordozókat a gyors hozzáférés érdekében azonosítóval, címkével kell ellátni
- A használni kívánt adathordozót használat után a tárolás helyére vissza kell tenni
- A munkaasztalon lehetőség szerint csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek
- Intézményi saját adathordozót más intézménynek átadni tilos
  /átadást írásbeli kérelemre csak az intézményvezető vagy helyettese engedélyezheti /
- Új adathordozó (lemez, CD-DVD ROM, pendrive) igénylése, beszerzése csak az intézeten belül lehetséges
  (Központi raktár munkahelytől igényelhető, szükség esetén Finanszírozási és Számítástechnika Csoporttól)

Vírusvédelem

A biztonságos számítástechnikai működéshez alapfeltétel, hogy a rendszert és eszközöket veszélyeztető program „vírusok” intézetünkbe jutását elkerüljük. Minden óvintézkedés ellenére szinte elkerülhetetlenek az ilyen jellegű meghibásodások, melyek adott esetben komoly anyagi kárt is jelenthetnek a kórház számára. A munkahelyi felhasználók kötelessége:

- Bármilyen szokatlan meghibásodás esetén a felhasználó azonnal jelezze azt a számítástechnikai rendszergazda vagy helyettese felé
- Saját vagy külső felhasználó (rokon, barát, ismerős, stb.) által adott adathordozó (egyedi program, játék, stb.) alkalmazása intézeti számítógépen tilos !
- Intézményi számítógépre munkahelyi dolgozó általi önálló szoftvertelepítés tilos !
- Számítógépes vírus által szándékosan vagy gondatlanságból elkövetett károkozás esetén az érintett munkahely illetve személy felelősségének és a kártérítés módjának megállapítása a Számítástechnikai Védelmi Szabályzatban leírtak szerint történik.

Saját vagy külső felhasználótól kapott adathordozó, program intézeti alkalmazásának egyetlen módja :

- Munkahelyi dolgozó a Finanszírozási és Számítástechnika Csoportnál kezdeményezi a címkével ellátott adathordozó „víruskereső” vizsgálatát, melyet az informatikus kollégák azonnal elvégeznek
- Vírusmentesség esetén az informatikus kolléga a címkén azt dátummal ellátva jelzi
- Ezt követően az adathordozó, program szabadon alkalmazható, de csak a munkahelyi számítógépen
- Amennyiben a vírusmentes lemez a „bevizsgálást” követően külső számítógépen is alkalmazásra kerül, újabb munkahelyi felhasználáskor ismételt vírusvizsgálat kötelező a fentebb leírt módon

D., Adatvédelem

Biztosítani kell, hogy illetéktelen személy (külső, vagy olyan munkahelyi dolgozó, akinek munkaköri leírásában a számítógép alkalmazáshoz való jogosultság nem szerepel) a számítógépen tárolt adatokhoz ne férhessen hozzá. Ennek elsősorban betegjogi szempontból van jelentősége a betegek adatainak titkossága miatt. A munkahelyi felhasználók kötelessége:

- Engedély nélkül, illetve rendeleti előírás vagy belső szabályozás hiányában intézeti működéssel kapcsolatos adatot külső, intézettel munkaviszonyban nem álló személy vagy intézmény részére kiadni tilos
- Internet alkalmazása: illetéktelen hozzáférés elkerülése érdekében (pénzügyi és betegadatok, betegjogok védelme !) Internet alkalmazás csak a hálózati programokból kilépett számítógéppel lehetséges.

E., Hálózati program alkalmazásának módja

A betegellátó munkahelyek adatrögzítői integrált hálózati programot alkalmaznak munkájuk során. A zavartalan és biztonságos működés érdekében a Finanszírozási és Számítástechnika Csoporton belül rendszergazdai központi szabályozásra, valamint a felhasználói munkahelyen az alkalmazás szabályozására van szükség. A központi szabályozás részleteit a Finanszírozási és Számítástechnika Csoport Működési Rendje írja elő. Jelen fejezetrészben a munkahelyi felhasználókat érintő feladatok kerültek rögzítésre.

- Hálózati programba belépési jogosultság szükséges
- Jelszó titkossága érdekében a jelszó intézeti szintű megváltoztatása kétévente célszerű. Ezen túlmenően felhasználó kérésére szükség esetén A Finanszírozási és

Számítástechnika Csoport kezdeményezi valamennyi felhasználó felé az új jelszó kialakítását, az ezzel kapcsolatos hálózati feladatokat is elvégzi.

- Titkos jelszó illetéktelen személy tudomására nem juthat. Minden felhasználó önálló felelőssége saját jelszavának, ezen keresztül az általa végzett betegadat kezelés titkossága.
- Betegadatok rögzítése esetén, ha bármely okból a munkafolyamat megszakad, az éppen rögzített menüpontnál az előírt mentés funkciót alkalmazni kell
- Hálózati program alkalmazásának befejezése esetén két eset lehetséges :
  1. Megfelelő módon a programot bezárva kikapcsolja a számítógépet
  2. A program menü sorában az első főmenü oldalig kilép a megfelelő módon
- A hálózati programot a központi karbantartás időintervallumában használni nem szabad. Ezen időszakról a rendszergazda a felhasználói munkahelyeket köteles értesíteni
- Hálózati programhiba esetén a hibát észlelő felhasználó azonnal jelezze azt a Finanszírozási és Számítástechnika Csoport felé
- Hibaelhárítást a lehető leggyorsabban el kell végezze a rendszergazda vagy programozó helyettese.
- Hétvégi időszakban – péntek 16 órától hétfő reggel 07 óráig – informatikai készenléti ügyelet működik a rendszer működésének biztonsága érdekében.
- Hálózati hiba esetén az informatikai készenléti ügyeletest kell értesíteni (telefonszám megtudható a Telefonközpont munkatársától).
- Hibaelhárítás esetén a hálózatból valamennyi felhasználó munkahelynek ki kell lépnie a lehető legrövidebb időn belül. Ilyen esetben központi üzenetet küld a rendszergazda vagy helyettese. Az üzenet kiküldését követően a programból 15 percen belül ki kell lépni, vagy a program automatikusan az aktuális adatok mentése nélkül kilépteti a felhasználót.

13., Számítástechnikai ellenőrzés módja

A megfelelő minőségű információs technika elengedhetetlenül szükséges a Dr. Kenessey Albert Kórház – Rendelőintézet működéséhez, kiegészítő eszköze a hatékony betegellátásnak. Ebből kifolyólag alapvető fontosságú az intézmény mindenkor rendelkezésre álló számítástechnikai eszközeinek megbízható, folyamatos és lehetőség szerint hibátlan működése. Jelen fejezet meghatározza a rendszergazda irányításával végzett információs technika (IT) ellenőrzési feladatokat a Finanszírozási és Számítástechnika Csoport működési rendjének megfelelően. A számítástechnikai ellenőrzési feladatok kialakításáért és szükség szerinti módosításáért felelős a Finanszírozási és Számítástechnika Csoportvezető. A benne foglaltak kivitelezéséért felelős a rendszergazda. Az adatvédelmi ellenőrzésért felelős az adatvédelmi felelős.

A „Számítástechnikai ellenőrzési módja” fejezetben leírt koncepció konkrétan és csakis az információs technika biztonságos és folyamatos működéséhez szükséges ellenőrzési és karbantartási feladatokat tartalmazza.

A Finanszírozási és Számítástechnika Csoport hatáskörébe tartozó feladat a kórház számítástechnikai helyzetének felmérése, naprakész ismerete, a módosítás illetve IT bővítés és korszerűsítés érdekében javaslatok tétele. A számítástechnikai eszközök és programok rendszeres és szakaszos ellenőrzése szükséges a folyamatos működéshez, elengedhetetlen adatvédelmi szempontból, másrészt a géppark minőségének biztosítása miatt. Kiegészítő feladat az információs technikát igénybe vevő dolgozók folyamatos és szükséges mértékű képzése a biztonságos használat érdekében.

Ellenőrzési feladatok :

1. Felmerülő működési és egyéb hibák folyamatos korrigálása a lehető legrövidebb időn belül a rendszergazda irányításával a Finanszírozási és Számítástechnika Csoport munkatársai által. Szükség esetén segítségkérés az átalánydíjas szervízszolgáltatást végző cég(ek)től
2. Külső szolgáltató garanciális szerviz ellenőrzésén túlmenően a számítástechnikai eszközpark szükség szerinti időszakos ellenőrzése, alapkritérium: évente legalább egy alkalommal történő ellenőrzése a rendszergazda által meghatározott ütemben és nyilvántartás alapján
3. Vírusvédelem – szakaszos ellenőrzés keretein belül adatvédelem szempontjából kockázatnak kitett munkahelyeken vírusmentesítő, - megelőző ellenőrzés

Az ellenőrzés illeszkedhet az átalánydíjas szervízszolgáltatást nyújtó cég negyedéves karbantartási feladataihoz. Ezen ellenőrzési szabályzat az alábbiak szerint négy csoportba rendezi a felhasználói munkahelyeket. A csoportosítás figyelembe veszi a kórház területi felépítését, valamint az egyes munkahelyeken található számítástechnikai eszközök számát. A csoportosítás a feladatból adódó terhek kiegyenlítése érdekében módosítható a rendszergazda javaslatára a Finanszírozási és Számítástechnika Csoportvezető jóváhagyásával. Kiegészítő szerződés: Átalánydíjas szervízszolgálati szerződés, vagy garanciális, illetve díjas szervízszolgálati szerződés központosított közbeszerzési eljárásban nyertes cég részéről.

1. számú melléklet

Adathordozók nyilvántartása

A felhasználói munkahelyeken / osztály, ambulancia, gazdasági terület, stb. / keletkező minősített és egyéb, az intézményi működés és betegellátás szempontjából fontosnak ítélt adatokat megadott időszakonként archiválni / menteni / kell, a központi archiválástól függetlenül. Az archivált adatokat tartalmazó adathordozó / floppy lemez, CD-DVD ROM, pendrive / címkéjének az alábbi adatokat szükséges tartalmaznia a visszakereshetőség - más felhasználó által is - végett :

1. Az adatok megnevezése

2. Az adatok keletkezésének ideje vagy időintervalluma

3. Többlemezes archíválás esetén a lemez vagy CD-DVD ROM sorszáma

4. Mentés módszere / pl.tömörítés típusa /

5. A kimentett adatok helye a winchesteren / alkönyvtár megnevezése /

6. A mentést végző neve

A kimentett adatokat tartalmazó adathordozókat témakörönként rendszerezve kell tárolni.