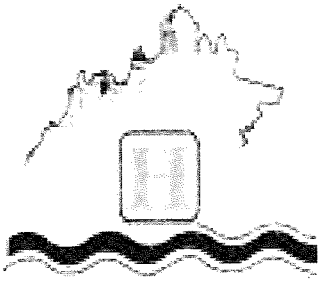
52-55

VASZARY KOLOS KÓRHÁZ, ESZTERGOM

Informatikai adatvédelmi és adathozzáférési szabályzat



Készítette: Mitru Roland

Mitru Roland — **2015. január 20.**
mb. informatikai osztályvezető

Ellenőrizte:

Lugosi Krisztina — **2015. január 20.**
gazdasági igazgató

Jóváhagyta:

Dr. Kanász Gábor — **2015. január 20.**
főigazgató főorvos

Nyilvántartott példányszám: 2 db (Informatikai Osztály, Titkárság)

Hatályos: 2015. január 20.

TARTALOMJEGYZÉK

1. Bevezetés

Az Informatikai adatvédelmi és adathozzáférési szabályzat – a továbbiakban Szabályzat – a Vaszary Kolos Kórház Esztergom – továbbiakban Intézmény – nyilvántartásával összefüggő legfontosabb adatvédelmi, informatikai-biztonsági szabályokat tartalmazza különös tekintettel az adatkezeléssel, adattovábbítással és nyilvánosságra hozatallal kapcsolatos adatvédelmi követelményekre.

2. Általános rendelkezések

2.1 A Szabályzat célja, hatálya

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

A *Szabályzat tárgyi hatálya* kiterjed az Intézmény dolgozói illetve az intézetben ellátott járó és fekvőbetegek nyilvántartásával összefüggő teljes adatkezelési és informatikai folyamatra.

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

A *Szabályzat időbeli hatálya* kiterjed a nyilvántartással és a kapcsolódó személyi iratokkal összefüggő teljes adatkezelési és informatikai folyamatra, az irat beérkezésétől, keletkezésétől a megsemmisítésig.

2.2 Jogszabályi alap

A Szabályzat elkészítése az alábbi jogszabályokon alapul.

- Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény.
- A statisztikáról szóló 1993. évi XLVI. törvény.

2.3 A szabályzat tartalma

Az Intézmény Szabályzata a következő témákhoz kapcsolódóan tartalmaz előírásokat:

- a személyi iratok kezelésének adatvédelmi követelményei,
- az adatnyilvántartás vezetésének adatvédelmi szabályai,
- a betekintési jog gyakorlásának szabályai,
- a nyilvántartásban és a személyi iratokban szereplő személyes adatokat kezelők személyes felelőssége,
- a nyilvántartást kezelő, személyes adatot tartalmazó számítógépes információs rendszer adatvédelmi és adatbiztonsági szabályai

2.4 A szabályzat hatályba lépésének dátuma

A Szabályzat hatályba lépése annak jóváhagyása napján.

3. Részletes szabályok

3.1 A személyi iratok kezelésének adatvédelmi követelményei

3.1.1 A személyi irat fogalma

Személyi irat minden - bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett - adathordozó, amely a *dolgozó esetén* közalkalmazotti illetve egyéb – intézményi gyakorlatban lehetséges - jogviszonyok, mint vállalkozói munkaviszony, szabadfoglalkozású jogviszony, önkéntes segítői jogviszony, egyéni egészségügyi vállalkozói jogviszony, társas vállalkozással létrejövő jogviszony létesítésekor, *beteg esetén* az ellátás megkezdésekor fennállása alatt, megszűnésekor, illetve azt követően keletkezik és a személlyel összefüggésben adatot, megállapítást tartalmaz.

3.1.2 A személyi iratok köre közalkalmazottak esetén

- a személyi anyag iratai (a továbbiakban: személyzeti irat),
- a közalkalmazotti jogviszonnyal összefüggő egyéb iratok,
- a közalkalmazottnak a közalkalmazotti jogviszonyával összefüggő más jogviszonyaival kapcsolatos iratok (adóbevallás, fizetési letiltás stb.),

- a közalkalmazott saját kérelmére kiállított vagy önként átadott adatokat tartalmazó iratok.

3.1.3 A személyi iratok köre ellátott betegek esetén

- a személyi adatok,
- a betegellátással összefüggő iratok,
- a beteg saját kérelmére kiállított vagy önként átadott adatokat tartalmazó iratok.

3.1.4 A személyi iratok keletkezése, kezelése, iktatása, megőrzése

Összeállításra kerül a személy személyi anyaga.

A személyi iratra csak olyan adat és megállapítás vezethető, amelynek alapja közokirat vagy a személy írásbeli nyilatkozata, a munkáltatói jogkör gyakorlójának írásbeli rendelkezése, bíróság vagy más hatóság döntése vagy jogszabályi rendelkezés. A személyi anyagban a személyzeti iratokon kívül más irat nem tárolható.

A személyi anyagot „Betekintési lap" kimutatással kell ellátni, melyen dokumentálni kell a személyi anyagba történő betekintés tényét, jogosultjának személyét, jogszabályi alapját és a betekintés időpontját.

A személyi iratokat elektronikus formában kell tárolni.

Külön szoftvereket kell működtetni a közalkalmazottak és betegek iratainak tárolására.

A közalkalmazotti jogviszony megszűnése a személyi anyagot le kell zárni és azt irattárazni kell.

A személyi anyagot a fenti időponttól számított ötven évig meg kell őrizni.

A fekvőbeteg ügyekkel, kapcsolatos iratokkal az Intézmény hatályos Iratkezelési szabályzata foglalkozik részletesen azok nem selejtezhetőek, irattárazásukat helyben kell biztosítani.

3.2 A *közalkalmazotti nyilvántartás* vezetésének adatvédelmi szabályai

3.2.1. Közalkalmazotti alapnyilvántartás jogszabályi háttere

Az Intézmény a vele munkavégzésre irányuló jogviszonyt (közalkalmazott, vállalkozó, szabadfoglalkozású, stb.) létesítők alapadatairól nyilvántartást vezet.

A közalkalmazotti alapnyilvántartás adatkörét az 1992.évi XXXIII. törvény (Kjt) 5. számú melléklete határozza meg. (1. sz. melléklet)
A mellékletben nem szereplő körben adatszerzés nem végezhető, ilyen adatot nyilvántartani nem lehet.

3.2.2 Közalkalmazotti alapnyilvántartás kezelője

Az alapnyilvántartás által előírt adatok kezelője a humánpolitikai-munkaügyi osztály. A számítógépes nyilvántartás mellett nélkülözhetetlen a papír alapú nyilvántartás, hiszen így aláírásával igazolja minden érintett a nyilvántartásba felvezetett adatok valódiságát. Az adatokban történt változásokat bejelentés után az adatkezelésért felelős személy haladéktalanul köteles rögzíteni, illetve a papír alapú nyilvántartást elkészíteni.

A személyzeti feladatot ellátó közalkalmazott felelősségi körén belül köteles:
- gondoskodni arról, hogy az általa kezelt - a közalkalmazotti jogviszonnyal összefüggő - adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának.
- gondoskodni arról, hogy a személyi iratra csak olyan adat, illetve megállapítás kerülhessen, amelynek alapja:
- közokirat vagy a közalkalmazott írásbeli nyilatkozata;
- a munkáltatói jogkör gyakorlójának írásbeli rendelkezése;
- bíróság vagy más hatóság döntése;
- jogszabályi rendelkezés;
- a közalkalmazotti jogviszonnyal illetve egyéb – intézményi gyakorlatban lehetséges - jogviszonnyal, mint vállalkozói munkaviszony, szabadfoglalkozású jogviszony, önkéntes segítői jogviszony, egyéni egészségügyi vállalkozói jogviszony, társas vállalkozással létrejövő jogviszonnyal összefüggő adat helyesbítését és törlését kezdeményezni a személyzeti szervezet vezetőjénél, ha megítélése szerint a személyi iraton szereplő adat a valóságnak már nem felel meg.

3.2.3 Nyilvános adatok

A Kjt 83/B. (2) alapján a közalkalmazotti alapnyilvántartás adatai közül a munkáltató megnevezése, a közalkalmazott neve, továbbá a besorolására vonatkozó adat közérdekű,

ezeket az adatokat a közalkalmazott előzetes tudta és beleegyezése nélkül nyilvánosságra lehet hozni.

3.2.4 Adatszolgáltatás

A közalkalmazotti alapnyilvántartásból statisztikai célra csak személyazonosításra alkalmatlan módon szolgáltatható adat.

3.2.5 Betekintésre jogosultak köre

A munkáltatónál vezetett közalkalmazotti alapnyilvántartásba – az érintetten kívül – a következők jogosultak betekinteni, illetőleg abból adatot átvenni a rájuk vonatkozó jogszabályban meghatározott feladataik ellátása céljából:

- közalkalmazott felettese,
- minősítést végző vezető,
- feladatkörének keretei között a törvényességi ellenőrzést végző szerv,
- munkaügyi, polgári jogi, közigazgatási per kapcsán a bíróság,
- közalkalmazott ellen indult büntetőeljárásban a nyomozó hatóság, az ügyész és a bíróság,
- személyzeti, munkaügyi és illetmény-számfejtési feladatokat ellátó szerv e feladattal megbízott munkatársa feladatkörén belül,
- az adóhatóság, a nyugdíjbiztosítási igazgatási szerv és az egészségbiztosítási szerv, az üzemi baleseteket kivizsgáló szerv és a munkavédelmi szerv

3.3 A *betegnyilvántartás* vezetésének adatvédelmi szabályai

Az intézet az ellátott járó- és fekvőbetegeiről a szabályzat 2. számú mellékletében meghatározott adatkörre kiterjedő nyilvántartást vezet (betegnyilvántartás). Az ellátott fekvő- illetve járó betegekről kitöltött adatlap formailag és tartalmilag aktuális változata a mindenkori hatályos az egészségügyi szolgáltatások Egészségbiztosítási Alapból történő finanszírozásának részletes szabályairól a 43/1999.(III.3.) Kormányrendelet mellékletében található.

Adatlapot kell kitölteni annak a betegnek az adatairól, aki
- járóbeteg rendelésen megjelent és ellátták (Ambuláns ellátási lap)
- fekvőbeteg osztályra felvették (ADATLAP kórházi (osztályos) ápolási esetről)

A nyilvántartást az ellátó egység dolgozói vezetik.
A betegnyilvántartás adatai közül bármely adatot a beteg előzetes tudta és beleegyezése nélkül nyilvánosságra nem lehet hozni.

A beteg adatait a beteg vagy meghatalmazottja veheti át, más személynek azt kiadni nem lehet.
A betegnyilvántartásban szereplő személyes adatok védelméért, az adatkezelés jogszerűségéért, valamint az előírt adatszolgáltatásokért az ellátó egység vezetője a felelős.

Az adatkezelő betegellátás során a beteg nyilvántartott adatairól adattovábbítási nyilvántartást vezet, melyet az adat kiadásától számított 25 évig meg kell őrizni.
A nyilvántartásnak tartalmaznia kell, hogy kinek, milyen célból, milyen terjedelemben továbbítottak adatot. A beteg jogosult megismerni ezen adatokat.
Ennek pontos feltételeit a kórház Iratkezelési szabályzata tartalmazza.

3.3.1 A betegnyilvántartásba való betekintési jog szabályai

A betegnyilvántartásba való betekintési jog szabályait az intézmény hatályos Irat és adatkiadási szabályzata tartalmazza.

3.3.2 A betegnyilvántartásban szereplő személyes adatokat kezelők személyes felelőssége

A betegnyilvántartásban összefüggő adatok kezeléséért felelős
- az adatokhoz hozzáférő adminisztrátor vagy nővér,
- a beteg ellátó orvosa,
- az ellátó egység vezetője.

Az adminisztrátori feladatot ellátó intézeti alkalmazott felelősségi körén belül köteles:
- gondoskodni arról, hogy az általa kezelt - a betegellátással összefüggő - adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának.
- gondoskodni arról, hogy a beteg személyi dokumentációjába csak olyan adat, illetve megállapítás kerülhessen, amelynek alapja:
- közokirat vagy a közalkalmazott írásbeli nyilatkozata;
- bíróság vagy más hatóság döntése;
- jogszabályi rendelkezés;
- gondoskodni arról, hogy a beteg betegellátási dokumentációjába csak olyan adat, illetve megállapítás kerülhessen, amelynek alapja:

- más betegellátó egység orvosi dokumentuma;
- a beteg kezelőorvosa által szóban vagy írásban közölt dokumentum;

Az adminisztrátori feladatot ellátó alkalmazott minden olyan alkalmazott, aki az intézetnél tevékenysége során a betegellátási nyilvántartással és személyi irattal összefüggő adatot kezel.

Az ellátó orvos felelősségi körén belül köteles:

- gondoskodni arról, hogy az általa kezelt - a betegellátással összefüggő - adat és megállapítás az adatkezelés teljes folyamatában megfeleljen a jogszabályi rendelkezések tartalmának.
- gondoskodni arról, hogy a beteg betegellátási dokumentációjába csak olyan adat, illetve megállapítás kerülhessen, amelynek alapja:
- más betegellátó egység orvosi dokumentuma;
- a beteg kezelése során általa szóban vagy írásban közölt megállapítás;

Az ellátó orvos feladatot ellátó alkalmazott minden olyan alkalmazott, aki az intézetnél tevékenysége során az orvosi nyilvántartással összefüggő adatot kezel.

Az ellátó egység vezetője felelősségi körén belül köteles intézkedni arról, hogy a betegellátás adatait a megfelelő személyi, illetve betegellátási iratra az adat keletkezésekor, illetőleg változásakor haladéktalanul rávezessék.

3.4 Az alkalmazotti, ill. betegnyilvántartást kezelő, személyes adatot tartalmazó *számítógépes információs rendszer* adatvédelmi és adatbiztonsági szabályai

3.4.1 A számítógépes információs rendszer célja

A személyes adatokat tartalmazó számítógépes információs rendszer (számítógéppel vezetett nyilvántartás) védelmének szabályozása azt a célt szolgálja, hogy biztosítsa az információs rendszerben az adatkezelés fizikai biztonságát, a működtetés rendjét.

3.4.2 A számítógépes információs rendszer adatvédelmi és adatbiztonsági szabályai

A számítógépes információs rendszernek biztosítani kell az adatbiztonságot, a fizikai biztonságot, az üzemeltetés és a technikai biztonságot továbbá szabályozni kell az információtovábbítást.

Az adatbiztonság szabályozásának biztosítania kell:

- az adatkezelésre használt számítástechnikai és manuális eszközökhöz történő illetéktelen fizikai hozzáférés megakadályozását,
- az adathordozók tartalma illetéktelen megismerésének, lemásolásának, megváltoztatásának vagy az adathordozó eltávolításának a megelőzését,
- annak megakadályozását, hogy az adatkezelésre használt számítástechnikai és manuális eszköztárba illetéktelen bevitelt hajtsanak végre, vagy a tár tartalmát illetéktelenül megismerjék, töröljék, vagy bármilyen módon megváltoztassák,
- annak megakadályozását, hogy adatkezelésre használt távadat-átviteli vonalon az adatokhoz illetéktelenül hozzáférjenek,
- a hozzáférési jogosultság betartását,
- azoknak az azonosítását, akiknek az adatkezelésből adatokat továbbítanak,
- annak azonosítását, hogy a számítástechnikai, valamint manuálisan vezetett eszköztárba milyen adatokat, mikor és ki rögzített, illetve intézkedett a rögzítésről,
- annak megakadályozását, hogy az adatok továbbítása alkalmával az adatokat illetéktelenül megismerjék, lemásolják, töröljék, vagy bármilyen módon megváltoztassák.

A fizikai biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- az adathordozó eszközök elhelyezésére szolgáló helyiségeket úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen,
- azokba a helyiségekbe, ahol adatkezelés folyik, a személyek belépését a hivatalos feladataikkal összhangban megállapított felhatalmazás alapján kell szabályozni, ellenőrizni,
- számítástechnikai eszközzel olvasható és manuális adathordozók tárolását, felhasználását és a hozzáférést ellenőrizni kell,
- az adathordozókról, azok mozgásáról, tartalmáról és felhasználásukról nyilvántartást kell vezetni,
- meg kell határozni azoknak a személyeknek a körét, akik az adathordozó eszközöket üzemeltethetik,
- gondoskodni kell arról, hogy a számítástechnikai eszközök biztonsági megoldásainak dokumentációjához csak az arra felhatalmazott személyek férjenek hozzá.

Az üzemeltetési biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- össze kell állítani és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott személyek névsorát, feladataikat körül kell határolni,
- meg kell határozni az adatokhoz való hozzáférés szintjének szabályait,
- külső személy - például karbantartás, javítás, fejlesztés céljából - a számítástechnikai eszközökhöz lehetőleg úgy férjen hozzá, hogy a kezelt adatokat ne ismerje meg,
- a számítástechnikai rendszert - ideértve a programokat is - dokumentálni kell; a rendszer vagy annak bármely eleme csak az arra illetékes személy felhatalmazásával változtatható meg, amelyet ellenőrizni kell,
- a hozzáférés jelszavait időközönként, de az üzemeltető személyének megváltozásakor azzal egyidejűleg meg kell változtatni; jelszót ismételten nem lehet kiadni,
- a számítástechnikai rendszer üzemeltetéséről - hagyományos vagy automatikus módon - nyilvántartást kell vezetni, amelyet az arra illetékes személynek folyamatosan ellenőriznie kell,
- a rendszerbe kerülő adatokat tartalmazó (hagyományos vagy számítástechnikai eszközzel olvasható) dokumentumokat úgy kell kezelni, hogy elvesztésük, elcserélésük vagy meghibásodásuk elkerülhető, kiküszöbölhető legyen,
- olyan tervet kell kidolgozni, amely a számítástechnikai eszközök előre nem látható üzemzavarának hatását ellensúlyozni képes intézkedéseket tartalmaz.

A technikai biztonság szabályozásakor különösen fontosak az alábbi szempontok:

- az adatok és programok véletlen vagy szándékos megrongálását számítástechnikai módszerekkel is meg kell akadályozni,
- az adatállományok kezelését úgy kell megszervezni, hogy részleges vagy teljes megsemmisülésük esetén tartalmuk rekonstruálható legyen, az adatállományok tartalmát képező adattételek számát folyamatosan ellenőrizni kell,
- a hozzáférést jelszavakkal kell ellenőrizni,
- az adatok és az adatállományok változását naplózni kell,
- az adatbevitel során a bevitt adatok helyességét ellenőrizni kell,
- on-line adatmozgás kezdeményezésének jogosultságát ellenőrizni kell,
- programfejlesztés vagy próba céljára valódi adatok felhasználását - ha a próbát külső szerv vagy személy végzi - el kell kerülni.

Az információtovábbítás szabályozásakor különösen fontosak az alábbi szempontok:

- meg kell határozni, hogy a számítógépes információs rendszeréből adatot szolgáltatni
- mely jogszabály alapján,
- kinek, mely szervnek,
- milyen tartalommal lehetséges;
- a rendszer adminisztrációjának teljes körűen tükröznie kell az adatszolgáltatást.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

A Vaszary Kolos Kórház Esztergom, - továbbiakban intézmény – (ideértve a dorogi külső telephelyet is) Informatikai Biztonsági Szabályzatát (továbbiakban IBSZ) a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló többször módosított 1992. évi LXIII. törvény, a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló többször módosított 1992. évi LXVI. törvény, valamint az államtitok és szolgálati titok számítástechnikai védelméről szóló 3/1988. (XI.22.) KSH rendelkezés alapján a következők szerint határozom meg:

1. Az Informatikai Biztonsági Szabályzat célja

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

Az Informatikai Biztonsági Szabályzat célja továbbá:

- a titok- és vagyonvédelemre vonatkozó védelmi intézkedések betartása,
- a tűzvédelemre vonatkozó 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.

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

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

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

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az 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.

3. Az adatkezelés során használt fontosabb fogalmak

Személyes adat: a meghatározott természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható;

Különleges adat:

a) a faji eredetre, a nemzeti, nemzetiségi és etnikai hovatartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más meggyőződésre,

b) az egészségi állapotra, a kóros szenvedélyre, a büntetett előéletre vonatkozó személyes adat;

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, a személyes adat fogalma alá nem eső adat;

Adatkezelés: az alkalmazott eljárástól függetlenül az 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;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

A*dattovábbítás:* ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

4. Az IBSZ biztonsági fokozata

Intézményünk alapbiztonsági fokozatba tartozik.

Intézményünk általános informatikai feldolgozást végez.

5. Kapcsolódó szabályozások

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

- Adatvédelmi Szabályzat
- Informatikai katasztrófaterv

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

6. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

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

6.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

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

6.2. A védelem eszközei

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

7. A védelem felelőse

A védelem felelőse az adatvédelmi felelős.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény adatvédelmi felelősének kell gondoskodnia.

A hatályos Sz-57 A közérdekű adatok megismerésére irányuló kérelmek intézésének, továbbá a kötelezően közzéteendő adatok nyilvánosságra hozatalának rendje szabályzatban rögzítettek szerint az Adatvédelmi felelős:

„A Kórház Főigazgatója által megbízott és az adatvédelmi feladatok ellátása körében a közzététellel kapcsolatos feladatok ellátását felügyeli és koordinálja. A Vaszary Kolos Kórházban ezt a feladatot a Gazdasági Igazgató látja el."

7.1. 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,
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése,
- 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.

7.2. Az 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.

7.3. Az 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.

7.4. 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.

7.5. Az adatvédelmi felelős megbízatása

Az adatvédelmi felelős írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

8. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az Informatikai Biztonsági Szabályzat megismerését az érintett dolgozók részére az adatvédelmi felelős oktatás formájában biztosítja. Erről nyilvántartást vezet.
Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

8.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell.
Az Informatikai Biztonsági Szabályzat folyamatos karbantartása az adatvédelmi felelős feladata.
E tevékenységről, annak konkrét tartalmáról évente egyszer írásbeli beszámolót kell készíteni.

8.2. Azonosítás és hozzáférési jogok

A védelmet igénylő adatokat, az információk osztályozását, a minősítésük alapján az adatokhoz való hozzáféréseket a *JOGOSULTSÁGKEZELÉS* tartalmazza.

9. Az informatikai eszközrendszert veszélyeztető helyzetek

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

9.1. Környezeti infrastruktúra okozta ártalmak

- Elemi csapás:
  - földrengés,
  - árvíz,
  - tűz,
  - villámcsapás, stb.
- Környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának felszökése vagy leesése,
  - piszkolódás (pl. por).
- Közüzemi szolgáltatásba bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

9.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

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

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,

- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a 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.

9.3. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

9.3.1. Tervezés és előkészítés során előforduló veszélyforrások

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

9.3.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

9.3.3. A működés és fejlesztés során előforduló veszélyforrások

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

10. Az informatikai eszközök környezetének védelme

Az informatikai eszközök környezetének védelme során az informatikai katasztrófaterv mentési terve alapján kell eljárni.

A mentési terv azon lépések sorozata, amelyeket azért hajtanak végre a katasztrófát megelőzően (a normál üzem során), hogy lehetővé tegyék a szervezet számára a reagálást a katasztrófára. A mentési terv biztosít elmentett eszközöket a helyreállításhoz.

- vagyonvédelmi előírások
- adathordozók
- tűzvédelem

11. Az informatikai feldolgozás folyamatának védelme

11.1. 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.

11.2. 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 osztályvezető 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.

11.3. 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 osztályvezető engedélye alapján lehet.

Az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet.

11.4. 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.

11.5. Az adathordozók megőrzése

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

11.6. Az adathordozók karbantartása

Az adathordozók állapotát 5 évenként ellenőrizni kell.

11.7. Selejtezés, sokszorosítás, másolás karbantartása

Olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell.

Selejtezni kell:

- a fizikailag sérült, javíthatatlan, a gyári, raktározási hibából követően 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.

A selejtezést az intézmény Felesleges vagyontárgyak hasznosításának és selejtezésének szabályzata, valamint Iratkezelési szabályzata alapján kell lefolytatni.

Sokszorosítást, másolást csak az érvényben lévő rendeletek szerint szabad végezni. *(Az üzemi másolás nem minősül másolásnak.)*

Biztonsági illetve archív adatállomány előállítása másolásnak számít.

11.8 Leltározás

Az adathordozókat a Leltárkészítési és leltározási szabályzatban foglaltaknak megfelelően kell leltározni.

Az informatikai eszközök leltárazásakor figyelembe kell venni az informatikai eszköznyilvántartást és anyaggazdálkodást.

11.9 Mentések, fájlok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A mentést minden módosítás után el kell végezni.

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 elemének adatállományai naponta mentendők, és egy hétre visszamenőlegesen több helyen is tárolandó.

Az intézmény egészségügyi rendszere valamennyi elemének adatállományai naponta mentendők, és egy hétre visszamenőlegesen több helyen is tárolandó.

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.

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

12.1. Központi gépek (Szerver)

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 egy nappal korábbi állapotú adat-visszaállítást kell lehetővé tenni.

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

12.2. Munkaállomások

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.

13. Ellenőrzés

Az intézmény éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

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.

Az Informatikai Biztonsági Szabályzat

2015. január 7. nappal

lép hatályba.

Ezzel egyidejűleg az 2012. január 1-én hatályba lépett, és 2014. augusztus 22-én aktualizált, Informatikai Biztonsági Szabályzat érvényét veszti.

Esztergom, 2015. január 7.

Az informatikai biztonsági szabályzatban foglaltak teljeskörűen érvényesek a dorogi telephely vonatkozásában is.

Esztergom, 2017. július 1.

Az esztergomi székhelyen és a dorogi telephelyen lévő szervertermek működéséről szóló szabályzat

1. Bevezetés

A szerverek olyan számítógépek a számítógépes hálózatban, amelyek a rajtuk tárolt vagy előállított adatok felhasználását más számítógépek számára elérhetővé teszik. Számítógépes hálózatokat minden nap használunk, a szervereken található adatok, információk folyamatos hozzáférésére van szükség, az esetleges szerverkiesés (a meghibásodás elhárításán túl) komoly károkat is okozhat. Ezért a szervereket tartalmazó helyiségek elhelyezése, kialakítása megfelelő körültekintést igényel.

2. Elhelyezés, berendezés

Az Intézmény esztergomi székhelyén a szerverterem kialakítására 2004-ben került sor, a gazdasági épület földszinti tanácsterem egy részéből. A helyiség 12 m^2 alapterületű, légkondicionálóval ellátott.

Megtervezésekor és kialakításakor több mindent figyelembe kellett venni.

Fontos szempont, hogy a szerverterem központi elhelyezkedésű, könnyen megközelíthető helyiség legyen. A fontosabb csővezetékek (fűtés, gáz, víz vagy szennyvíz) távol fussanak, mert az esetleges szivárgás nagy károkat okozhat a szerverterem berendezéseiben.

A helyiségnek megfelelő méretűnek kell lennie a szerverek és más szükséges berendezések befogadására, elegendő hely legyen a szerverek között a szellőzés, valamint a kábelezés megfelelő biztosítására, és egy esetleges jövőbeni bővítés se okozzon gondot.

Minél kisebb legyen a hőmérséklet-ingadozás, amely esetén a légkondicionáló berendezés fokozottabb működést igényel.

Légkondicionáló berendezés kialakítása és egy esetleges hálózati áramkimaradás esetére a központi szervereket szünetmentes tápegységre lehessen kapcsolni.

A szerverteremben ún. Salgó fémpolcok lettek kialakítva, amelyen több számítógép, tartozék kényelmesen elfér. A feszültség-, patch- és optikai kábeleken, valamint az elektronikai hosszabbítókon, elosztókon kívül az alábbi szerverek és szerverként működő számítógépek találhatóak.

- proxy szerver
  Linux (Debian) operációs rendszerrel futó számítógép, az intézmény internetes és levelező szolgáltatásait biztosítja.
- SANITAS szerver
  Linux (Debian) alapú számítógép, a SANITAS egészségügyi rendszer program- és adatbázisszervere.
- DELLSRV
  Windows 2013 Server, korábban a HOSPITALY rendszer szervere, most file szerver valamint mentési szerver.
- VASZARYSRV
  Windows 2000 Server, az EcoSTAT gazdasági programok kiszolgáló gépe (korábbi évek).
- Eco-szerver
  Linux (Debian) alapú szerver az EcoSTAT gazdasági programok kiszolgáló gépe (2011. évtől).
- AGFA szerver
  Windows 2003 Server és webszerver, a röntgen leletező és a képek webszerverre történő másolását (DICOM) kiszolgáló központi gép, szalagos egység a képek archiválására.
- ORGWARE szerver – a Munkaügyi, jelenléti program szervere (2014. októberétől)
- EMMA szerver – az EMMA egészségügyi rendszer program- és adatbázisszervere. (2015 júniusától)

3. Villamos hálózat

A megfelelő áramellátás biztosításához szünetmentes tápegységeket (UPS) kell használni, hogy áramszünet, ellátási zavar esetén a szerverek rendben le tudjanak állni.
Ehhez összesen három szünetmentes tápegységet használunk, amelyek segítségével áramszünet esetén a szerverek legalább 35-40 percig áramellátásban részesülnek.

Áramellátás megszűnésekor a szerverek rendeltetésnek megfelelően leállnak, amelyeket manuálisan kell újraindítani.

4. Klíma

A szerverteremben működő gépek számottevő hőmennyiséget termelnek, ugyanakkor bizonyos határokon túl érzékenyek a levegő hőmérsékletének és nedvességtartalmának változására. A szervertermek megfelelő klímája nélkülözhetetlen az ott működő berendezések hosszú távú, kifogástalan működéséhez, ezért légkondicionáló berendezést használunk.

A szerverterembe telepítetett légkondicionáló berendezés biztosítja az optimális hőmérséklet (20 - 25 °C).

Az optimális hőmérséklet eléréséhez figyelembe kell venni

- a szervergépek számát, elhelyezkedésüket,
- a terem méretét, megvilágítását,
- a légkondicionáló berendezés elhelyezkedését, teljesítményét.

A szerverterem hőmérsékletét napi szinten figyelni kell, és az erre kijelölt füzetbe fel kell tüntetni a leolvasás dátumát, a hőmérsékletet és a leolvasó aláírását.

A hőmérséklet leolvasását az erre a feladatra kijelölt informatikus(ok) végzi(k).

A klíma másik lényeges tényezője a levegő nedvességtartalma. Ha túl alacsony, akkor az növeli az elektrosztatikus feltöltődés esélyét, ha túl magas, akkor pedig korróziót, esetleg átütéseket okozhat. A szervertermek relatív páratartalmának optimális szintje 40-55 százalék közötti.

5. Tűzvédelem

A szerverteremben esetlegesen kialakuló tűz a közvetlen anyagi károkon (vagyis a berendezések károsodásán) túl a szerverek által biztosított szolgáltatások kiesését is okozza. Ezért a szervertermek tűzvédelme kapcsán a *passzív* tűzvédelem körültekintő megtervezésén túl fontos *aktív* tűzvédelmi alkalmazásokat is kiépíteni.

A passzív tűzvédelmi megoldások célja, hogy elfogadható szintre csökkentsék a tűz kialakulásának esélyét, valamint egy esetleges tűz esetén megakadályozzák, vagy megfelelő ideig késleltessék annak terjedését a szerverterem környezetében. A passzív tűzvédelem szempontjából legkritikusabb rész a kábelek, kábel- és csőátvezetések, a födémek, szellőző- és elszívócsatornák, valamint a nyílászáró.
Ezekre folyamatos és fokozott figyelmet kell fordítani.

Az aktív tűzvédelemi alkalmazások alatt a tűzjelző és tűzoltó rendszereket értjük.
A szerverteremben található tűzjelző tűz észlelése esetén – a telefonközponton keresztül – riasztja a tűzoltóságot.
Oltóanyagként – a villamos berendezések miatt a vízsugár értelemszerűen nem jöhet szóba – már csak azért sem, mert azokat a villamos berendezéseket is károsíthatja, amelyeket a tűz nem ért el. Hasonló a helyzet az oltóhabbal is, és nem megfelelő a porral töltött tűzoltó rendszer sem. Erre a célra mindenképpen gázzal töltött tűzoltó készülék alkalmas.

6. Biztonság

A szerverszobák, adatközpontok esetében nagyon fontos a biztonság, a megfelelő védettség.
A szerverterem mozgásérzékelő riasztója az informatikai terem riasztójával van összekötve, annak feloldása csak az informatikai osztályról lehetséges.
Belépési kóddal az informatikai osztály dolgozói (2 fő) rendelkeznek. Más személy csak informatikus kíséretével tartózkodhat a szerverteremben indokolt esetben.
Természet vagy személy által okozott kár, katasztrófa esetén az informatikai osztály biztonsági szabályzatát képező katasztrófatervnek, illetve az intézményi katasztrófatervnek megfelelően kell eljárni.

A dorogi telephely szervertermének működése

Az Intézmény dorogi telephelyének szerverterme a rendelőintézetben lett kialakítva. A szerverterem ujjlenyomat olvasóval védett, amelynek feloldásához csak a 2 rendszergazdának van engedélye.

A szerverteremben a rendelőintézet hálózati eszközei (switchek, optikai kábelek) illetve a telephelyen korábban használt programok szerverei vannak.

Ezek a szerverek már csak a korábbi programok mentésére szolgálnak illetve file szerverként, mivel a 2 kórház egyesítése után a gazdasági, medikai, munkaügyi programokat is az esztergomi központból futtatják a felhasználók.

Ennek kialakításakor a legfontosabb szempont a megfelelő biztonság volt. A dorogi telephely Esztergommal közös hálózatra való kötéséhez Esztergomban és Dorogon is 1-1 tűzfal beszerelésével lett kialakítva, amin csak és kizárólag a programok elérhetősége van biztosítva.

A szerverteremben légkondicionáló berendezés van beszerelve és az esetleges hálózati áramkimaradás esetén szünetmentes tápegység biztosítja a feszültség nélküli időszak áthidalását.

A szerverek megfelelő szellőzése érdekében a rackszekrényben a szerverek között elegendő hely lett hagyva.

A Dorogon korábban használt programok utolsó működő adatbázisáról mentés készült, amit az esztergomi székhelyen is tárolunk.

JOGOSULTSÁGKEZELÉS

1. Célja

A Jogosultságkezelés célja a védelmet igénylő adatok és információk osztályozása, minősítése alapján az adatokhoz való hozzáférések megfelelő szintű kezelése.

2. A védelmet igénylő adatok és információk osztályozása, minősítése

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.
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).

3. Azonosítás és hitelesítés

Az azonosítás és hitelesítési funkció keretében:

- az egyedi felhasználókat és a felhasználó csoportokat jelszóval kell azonosítani,
- a jelszóadást az erre a feladatra kijelölt rendszergazda végezheti el,
- jogosultság kiosztáskor a rendszergazda által kiadott jelszót a felhasználónak első bejelentkezése után meg kell változtatni, majd meghatározott időnként, 90 nap elteltével újra módosítania kell,
- a megváltoztatott jelszó nem egyezhet meg korábbi jelszóval,
- a jelszavak minimális hossza 6 karakter, amelyet lezárt borítékban a felhasználó az informatikának átadja megőrzésre,
- a jelszavakat titkosítva kell tárolni,
- nehezen megfejthető jelszóalkotás támogatását biztosítani kell,
- adott számú téves bejelentkezési kísérlet után az adott felhasználói jogosultsági rendszert bénítani kell,
- a téves bejelentkezés ténye rögzítendő és kivizsgálandó, ezt havi rendszerességgel szúrópróbaszerűen ellenőrizni kell.

Ahol indokolt, ki kell alakítani a többszintű (pl. operációs rendszer, adatbázis-kezelő, levelező rendszer, irodaautomatizálási rendszer stb.) hitelesítési és azonosítási rendszert az egyes szoftverek által nyújtott biztonsági funkciók, az alkalmazási területek és a biztonsági követelmények figyelembevételével.

4. Hozzáférés jogok szabályozása

A rendszer felhasználóihoz hozzáférési jogokat kell rendelni. A jogokat minimálisan egyedi, illetve csoport tulajdonosi szinten kell tudni megadni. A hozzáférés jogosultság menedzselésénél a következő hozzáférési jogokat kell alkalmazni:

olvasási jog (betekintés),
írási jog (létrehozás, módosítás),
törlési jog.

A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten történő megkülönböztetésére és szabályozására.

A rendszer objektumaihoz (fájlok, eszközök, folyamatok közötti kommunikációs csatornák) egyedi, illetve csoport tulajdonosokat kell rendelni az objektum létesítésekor. A hozzáférés vezérlése esetén az adott objektumhoz (pl. fájl) esetenként (pl. létesítéskor) rendelődnek hozzá a tulajdonosok jogai is.

A hozzáférési események esetén jogosultságellenőrzést kell végrehajtani. A hozzáférés-vezérlés a felhasználókhoz rendelt jogok és az objektumokhoz rendelt tulajdonosok és jogaik összevetése alapján történik.

A jogosultsági rendszernek támogatnia kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott rendszergazda végezheti el.

Új jogosultság kiosztására (pl. újonnan belépő dolgozó) csak vezetői jóváhagyás után kerülhet sor. Ezt az új felhasználó a Jogosultságkérő lap (*3/a. sz. melléklet*) kitöltésével igényli.

A jogosulatlan hozzáférési kísérleteket rögzíteni kell a biztonsági naplóban, amelynek értékelését rendszeresen el kell végezni.

Valamely felhasználó munkaviszonyának megszűnéséről a munkaügyi osztály az informatikai osztályvezetőt írásban tájékoztatja, ezután a feladatra kijelölt rendszergazda a felhasználó jogosultságait törli a rendszerből.

A jogosultsági rendszer kialakításakor speciális figyelmet kell fordítani a rendszerparancsok és adatállományok használatának szigorú és egyértelműen körülhatárolt szabályozására.

A jogosultság kezelésére vonatkozó mellékletben foglaltak a dorogi telephelyre is teljeskörűen érvényesek.

5. Mellékletek

3/a. sz. melléklet: Jogosultságkérő lap

3/b. sz. melléklet: EMMA egészségügyi rendszer: jogosultságok, csoportjogok

3/c. sz. melléklet: CT-Ecostat gazdasági rendszer: jogosultsági szintek

3/a. sz. melléklet

JOGOSULTSÁGKÉRŐ LAP

Felhasználó neve: _____

sztály / részleg: _____

Program: _____

énylet jogok / hozzáférések: _____

_____

_____

_____

_____

Kérés indoklása: _____

_____

_____

_____

_____

átum: _____

P.H.

_____ _____

oszt.vezető főorvos orvosigazgató

JOGOSULTSÁGKÉRŐ LAP

Felhasználó neve: _____

Osztály / részleg: _____

Program: _____

Igényelt jogok / hozzáférések: _____

_____

_____

_____

_____

Kérés indoklása: _____

_____

_____

_____

_____

Dátum: _____

P.H.

_____ _____

oszt.vezető főorvos orvosigazgató

JOGOSULTSÁGKÉRŐ LAP

Felhasználó neve: _____

sztály / részleg: _____

Program: _____

énylet jogok / hozzáférések: _____

_____

_____

_____

_____

Kérés indoklása: _____

_____

_____

_____

_____

átum: _____

P.H.

_____ _____

oszt.vezető főorvos orvosigazgató

JOGOSULTSÁGKÉRŐ LAP

Felhasználó neve: _____

Osztály / részleg: _____

Program: _____

Igényelt jogok / hozzáférések: _____

_____

_____

_____

_____

Kérés indoklása: _____

_____

_____

_____

_____

Dátum: _____

P.H.

_____ _____

oszt.vezető főorvos orvosigazgató

Jogosultságok									
EMMA multimedikai alkalmazás: **Jogosultság megnevezése és magyarázata:**	**Orvos**	**Adminisztrátor**	**Nővér**	**Kontr.**	**Gyógyt.**	**Bfelv. Recepció**	**Finansz.**	**Inform.**	
Receptírás, gyógyszerelés: A jog megadásával lehetőség van a vényíró használatára	IGEN	IGEN	NEM	NEM	NEM	NEM	NEM	IGEN	
Lelet /záró lezárás (validálás) lehetősége: A szöveg-szerkesztőben legyen-e lehetősége a felhasználónak a dokumentumok validálására	IGEN	IGEN	NEM	IGEN	IGEN	IGEN	IGEN	IGEN	
Más munkahely archív nyomtatványainak olvasása: Olvashassa-e a felhasználó más munkahelyek validált dokumentumait	IGEN	IGEN	NEM	IGEN	IGEN	IGEN	IGEN	IGEN	
Más munkahely archív nyomtatványainak nyomtatása: Nyomtathassa-e a felhasználó más munkahelyek validált dokumentumait	IGEN	IGEN	NEM	IGEN	IGEN	IGEN	IGEN	IGEN	
Ambuláns esemény törlése: A napi-listáról törölhessen-e betegeseményt / megjelenést	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Validálás visszavonása: Legyen-e lehetősége a felhasználónak a dokumentumok validálásának feloldására	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	IGEN	
Esemény-lánc azonosító kezelés: Összerendelhessen-e a felhasználó egy beteg esetében több ellátási eseményt, ellátási sorozattá	NEM	NEM	NEM	NEM	NEM	NEM	NEM	IGEN	
Paraméterezett lap definiálása: Készíthet-e dinamikus űrlapot	NEM	NEM	NEM	NEM	NEM	NEM	NEM	IGEN	
Fekvő felvevő osztály módosítási lehetősége: Módosíthatja-e a felvevő osztályt	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Beavatkozás törlése adatlapról nyugtázás nélkül: A kódolási lapon törölhessen-e anélkül beavatkozást, hogy megerősítő kérdést kapjon.	NEM	NEM	NEM	NEM	NEM	NEM	NEM	NEM	
Paraméterezett laphoz felhasználó definiálása: Kész űrlaphoz rendelhessen-e felhasználókat	NEM	NEM	NEM	NEM	NEM	NEM	NEM	IGEN	
Konzíliumkérést NEM adhat fel: Konzílium-kéréseket ne adhasson-e fel	NEM	NEM	NEM	IGEN	IGEN	IGEN	IGEN	NEM	
Ambuláns adatlap zárolás: Ambuláns eseményt / adatlapot zárolhasson-e	IGEN	IGEN	NEM	NEM	IGEN	IGEN	IGEN	IGEN	
Fekvő-ambuláns zárolás feloldás: A lezárt fekvő ill. ambuláns esemény / adatlap feloldásának joga	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Fekvő adatlap zárolás: Fekvő eseményt / adatlapot zárolhasson-e	IGEN	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Páciens egyesítés: Duplikáltan, vagy hibásan felvett, egy személyhez tartozó páciensadatok összevonásának joga	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Előjegyzési táblából törölhet: Szabadíthasson-e fel időpontot az előjegyzési naptárban, az előjegyzés-ből törölhessen-e beteget	IGEN	IGEN	NEM	NEM	NEM	IGEN	NEM	IGEN	
Recepciós funkció, központi ambuláns-fekvő felvétel: Központi járó-fekvő felvétel	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Új beteget nem vehet fel a törzsbe: A páciens-törzsbe NE vehessen fel beteget	NEM	NEM	IGEN	IGEN	NEM	NEM	IGEN	IGEN	
Újszülöttet felvehet a törzsbe: A pácienstörzsbe rögzíthessen-e újszülöttet	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	*Újszülött osztály egyéni jog*
Pathológiai adatokat kezelhet: A patológiai adatokat kezelhesse-e (pl boncolási adatlap)	IGEN	IGEN	NEM	NEM	NEM	NEM	NEM	NEM	*Pathológia egyéni jog*
Beteg adatot nem módosíthat a törzsben: Ne módosíthasson a felhasználó páciensadatot a páciens-törzsben	IGEN	IGEN	IGEN	IGEN	IGEN	NEM	IGEN	IGEN	
Fekvő eseményt NEM vehet fel: Ne indíthasson fekvő eseményt, ne vehessen a napilistára beteget	NEM	NEM	IGEN	IGEN	IGEN	NEM	IGEN	IGEN	
Járó eseményt NEM vehet fel: Ne indíthasson járó eseményt, ne vehessen a napilistára beteget	NEM	NEM	IGEN	IGEN	NEM	NEM	IGEN	IGEN	
Járó eseményt fekvő eseményre minősíthet: Járó eseményt a rögzített adatokkal fekvő eseménnyé minősíthet	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Járó eseményt járó eseményre minősíthet: Járó eseményt a rögzített adatokkal járó eseménnyé minősíthet	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	
Fekvő eseményt járó eseményre minősíthet: Fekvő eseményt a rögzített adatokkal járó eseménnyé minősíthet	NEM	NEM	NEM	NEM	NEM	IGEN	NEM	NEM	

Más munkahely kéréseit láthatja: Láthassa-e azon vizsgálatkérések részleteit, amelyet más munkahelyek kérnek	*IGEN*	*IGEN*	*IGEN*	*NEM*	*IGEN*	*NEM*	*NEM*	*NEM*
Jelentéskészítési jog: Elérhesse-e a felhasználó a rendszergazdai felületen a jelentéskészítési funkciókat	*NEM*	*NEM*	*NEM*	*IGEN*	*NEM*	*NEM*	*IGEN*	*IGEN*
Fekvő javító rekordot kezelhet: Javító-rekord bejegyzést készíthessen-e az adatlapon	*NEM*	*NEM*	*NEM*	*IGEN*	*NEM*	*NEM*	*IGEN*	*NEM*
Laborkérést nem adhat fel, meglévő kérést nem törölhet-módosíthat: A labor-funkciót használhassa-e, feladott kéréseket módosíthasson, törölhessen-e	*NEM*	*NEM*	*NEM*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*NEM*
Röntgenkérést NEM adhat fel: A röntgen-funkció esetében kéréseket adhasson-e fel	*NEM*	*NEM*	*NEM*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*IGEN*
Konzíliumkérést NEM adhat fel: Konzílium-kéréseket adhasson-e fel	*NEM*	*NEM*	*NEM*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*IGEN*
Labor csoportot NEM törölhet: A kész labor csoportok közül törölhessen-e a felhasználó	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*NEM*
Labor munkalistára kérést nem tehet: A laborfelület használata során a munkalista funkciót használhassa-e	*NEM*	*NEM*	*NEM*	*IGEN*	*IGEN*	*IGEN*	*IGEN*	*NEM*
Paciens logot olvashat: A rendszergazdai felületen a naplózási bejegyzéseket olvashassa-e	*NEM*	*NEM*	*NEM*	*NEM*	*NEM*	*NEM*	*NEM*	*NEM*
Fekvő: első két BNO-t 1-es és 3-as típusra minősítheti: Fekvő kódolás során az első két diagnózist átminősítheti-e 1-esről 3-asra, és fordítva	*NEM*	*NEM*	*NEM*	*IGEN*	*NEM*	*NEM*	*IGEN*	*NEM*
Születési dátumok alapján javító rekordok képzési lehetősége: Születési dátumok alapján javító rekordok képzési lehetősége	*NEM*	*NEM*	*NEM*	*NEM*	*NEM*	*IGEN*	*NEM*	*NEM*

informatikán egyéni jog

CT-EcoSTAT jogosultsági szintek

1. Rendszergazdák

A program Védelem és Paraméterkezelő moduljához való hozzáférés.

Funkciók:

- Felhasználó felvétele, letiltása
- Jelszómódosítás
- Felhasználó-program modul összerendelés
- Felhasználó menüengedélyek korlátozása adott modulon belül

Felelős: informatikai osztályvezető

2. Felhasználók

A rendszergazda által az adott program modulhoz való hozzáféréssel rendelkezik, az engedélyezett menüpontokat használhatja, a jogok kérését a jogosultságkérő lap kitöltésével az adott osztály osztályvezetője teszi meg, amelyek az alábbiak:

Pénzügy

- Pénzügy modul
- Főkönyv modul
- Készlet modul
- Leltár modul
- Rendelés és Kötváll modul
- Cashflow modul

Felelős: pénzügyi osztályvezető

Kontrolling

- Főköny modul
- Medkontroll modul
- Kötváll modul
- Pénzügy modul
- Cashflow modul

Felelős: kontrolling és finanszírozási osztályvezető

Anyaggazdálkodás

- Intézeti elbírálás modul
- Osztályos igénylés modul
- Készlet modul

- Rendelés modul
- Műtéti anyagfelhasználás
- Tárgyi modul

Felelős: anyaggazdálkodási osztályvezető

Kórházüzemeltetés

- Munkalap modul
- Munkalapigénylés modul
- Készlet modul

Felelős: kórházüzemeltetési osztályvezető

Beszerzői keretgazdák

- Rendelés-Szerződés modul

Felelős: anyaggazdálkodási osztályvezető

Felhasználói keretgazdák

- Osztályos igénylés modul

Felelős: intézeti főnővér

Főnővérek

- Beteglétszám modul
- Munkalapigénylés modul

Felelős: intézeti főnővér

Élelmezés

- Élelmezés modul

Felelős: vezető dietetikus

Informatikai katasztrófaterv

1. Bevezetés

Az informatikai rendszerek mindenkori működését figyelembe véve készítettük el az informatikai katasztrófatervet, amely a rendkívüli események kezeléséhez nyújt forgatókönyvet. A katasztrófatervet úgy alakítottuk ki, hogy az újonnan bevezetésre kerülő technikai megoldások beépíthetők legyenek a tervbe.

A Katasztrófaterv-eljárás vagy tevékenység-lépések sorozata annak biztosítására, hogy a szervezet kritikus információ-feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal katasztrófa után. A számítógép-katasztrófa egy olyan esemény, amely az adatfeldolgozó képesség elvesztését okozza hosszabb időre.

Jelen *informatikai katasztrófaterv* kizárólag a kórház informatikai katasztrófahelyzeteinek kezelésére vonatkozik.

2. Kapcsolódó szabályzat

Az informatikai katasztrófatervet az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni.

- Informatikai Biztonsági Szabályzat
- Tűzvédelmi szabályzat

3. Katasztrófahelyzet

3.1 Katasztrófahelyzet meghatározása

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.

Az informatikai biztonsági szabályzatban leírtak szerint a következő vészhelyzeteket kell meghatározni.

- Az informatikai eszközparkot veszélyeztető helyzetek
  - Környezeti infrastruktúra okozta ártalmak
  - Emberi tényezőre visszavezethető veszélyek
- Az adatok tartalmát, a feldolgozás folyamatát érintő veszélyek

3.2 Szereplők, felelősségek, hatáskörök

Meg kell határozni a rendkívüli helyzetek elrendeléséért, azok kezeléséért felelősök személyét és teendőit. Ezen hatáskörök meghatározása az intézményi vezető hatáskörébe tartozik.

3.3 Mentési terv

A mentési terv azon lépések sorozata, amelyeket azért hajtanak végre a katasztrófát megelőzően (a normál üzem során), hogy lehetővé tegyék a szervezet számára a reagálást a katasztrófára. A mentési terv biztosít elmentett eszközöket a helyreállításhoz. Így például a számítógép tükrözés és az optikai tároló sokkal könnyebbé teheti nagy tömegű papíralapú dokumentumok helyreállítását.

A folytonosság biztosítása érdekében szükséges, hogy rendszerenként illetve folyamatonként meghatározzuk azokat a megelőző intézkedéseket, tartalékmegoldásokat, amelyek segítségével a szolgáltatások folyamatossága katasztrófahelyzetben is biztosítható.

Az informatikai eszközök védelme

- *Vagyonvédelmi előírások*
  - 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.

- *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.

➢ *Tűzvédelem*

A gépterem illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A tűzvédelem feladatait, sajátos előírásokat a gépteremre *(informatikai szobára)* vonatkozóan az intézmény Tűzvédelmi szabályzata tartalmazza.

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

Az intézmény azon helyiségeiben, ahol informatikai eszközöket használnak vagy tárolnak, a bejárat előtt min. 1-1 db 2-5 kg-os poroltó tűzoltó készüléket kell elhelyezni.

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

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 osztályvezető feladata.

➢ *Hardvervédelem*

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.

➢ *Szoftvervédelem*

- **Rendszerprogram 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.

- **Felhasználói program 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:

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

  A program dokumentáció a rendszerdokumentációnak része.

  Programok megőrzése, nyilvántartása

  - o a programokról naprakész nyilvántartást kell vezetni,
  - o 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 osztályvezető felelős.

Programok fizikai védelme

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

4. Helyreállítási terv

3.4.1 Észlelés, intézkedések, jelentési kötelezettségek

A **helyreállítási terv** eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák az informatikai rendszert a tartalék központban vagy helyreállítsák az adatfeldolgozó központot.

Meghatározzuk, hogy a helyzeteket követően melyek azok az intézkedések, amelyeket a károk elhárítása, vagy a károk csökkentése érdekében szükséges megtenni.

3.4.2 A katasztrófa helyzetet követő intézkedések

Szakemberekkel közösen ki kell dolgozni és rögzíteni kell azokat az intézkedéseket és eljárásokat, amelyeket a rendkívüli helyzetek bekövetkeztétől annak elhárulásáig alkalmazni kell.

A katasztrófa bekövetkezte utáni helyreállítási terv hat szakaszból áll:

1. Azonnali reakció

Válasz a katasztrófa-helyzetre, a veszteségek számbavétele, a megfelelő emberek értesítése és a katasztrófa-állapot megállapítása.

2. Környezeti helyreállítás

Az adatfeldolgozó rendszer helyreállítása: operációs rendszer, program termékek és a távközlési hálózat.

3. Funkcionális helyreállítás

Az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakció naplóval.

4. Helyreállítás

Az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.

5. Áttelepülés

Az informatikai rendszer kiépítése a hidegtartalék létesítményben, ha a melegtartalék létesítmények használata időben korlátozott.

6. Normalizáció

Az új állandó informatikai rendszer kiépítése és arra az üzemelő rendszer áttelepítése.

3.5 Tesztelési terv

A teszt terv azokat a tevékenységeket tartalmazza, amelyek a Katasztrófaterv működőképességét ellenőrzik és biztosítják.

A katasztrófaterv megfelelősségének igazolásaképpen tesztelni kell a tervet. Elkészítjük a teszteléshez szükséges terveket és szakértői rendelkezésre állást biztosítunk a tesztek elvégzéséhez.

3.6 Karbantartási (üzemben tartási) terv

A karbantartási tervet használják a Katasztrófaterv aktuális állapotban tartására a szervezet változása esetén.

Az intézmény éves belső ellenőrzési ütemtervében rögzíti az ellenőrzés módját.

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.

A katasztrófaterv felülvizsgálata:

Rendszeres időközönként szükséges a tervek felülvizsgálata. Ilyenkor adódik alkalom az alkalmazott új technikai megoldások beépítésére, illetve a tervek aktualizálására.

MÓDOSÍTÁSOK JEGYZÉKE

Módosította Aláírás/dátum	Változat száma	Módosított oldalszám	Ellenőrizte	Jóváhagyta	Kibocsátás időpontja
2016. október 25. Dr. Roland	1.	17, 18, 35, 40	2016. 10. 25.	2016.10.25	2016.10.25.
A nabálgzat átdolgozási megtörtént módosítást nem igényel.		1 sz. melléklet/5,6 o. 3. sz. melléklet/3. o.			
2017. március 30. Dr. Roland		5/C. sz. mell./1. o.			
A nabálgzat aktualizálása a dongó település vonatkozásában megtörtént. 2017. október 20. Dr. Roland	2.	13 26 28 29 30, 31, 32, 35	2017. okt. 20.		2017. 10. 20.
	1. sz. melléklet/1. o 1 sz. melléklet/15. o. 2. sz melléklet/5. o. 5. sz melléklet/3. o.				
A nabálgzat ativizsgálása megtörtént, módosítást nem igényel. 2018. március 4. Dr. Roland			2018. március 4.		
Átdolgozás megtörtént, módosítást nem igényel. 2019. március 28. Dr. Roland			2019.03.28		2019.03.28.
Átdolgozás megtörtént, módosítást nem igényel. 2020. március 30. Dr. R.			2020.03.30		2020.03.30

Megismerési nyilatkozat

Az Informatikai Adatvédelmi és Adathozzáférési Szabályzatot, és annak mellékleteit megismertem, tudomásul vettem, és munkavégzésem során a benne foglaltakat betartom.

Név	Beosztás	Dátum	Aláírás
MITRU ROLAND	INFORM. OSZT. VEZ.	2015. II. 2.	Mitru Roland
Rein Zsolt	Rendőr-őrnagy	2015. XII. 05.	
Vidumi József	Rendőr-őrnagy	2019. III. 28.	Vidumi József