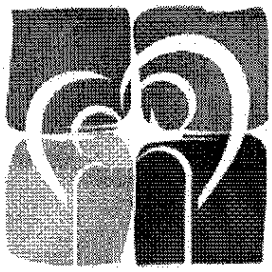

Kenézy Gyula Kórház és Rendelőintézet

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Debrecen
2014. október 1.

Tartalom

A gyógyintézetek működési rendjéről, illetve szakmai vezető testületéről szóló 43/2003. (VII. 29.) ESzCsM rendelet 9. § (2) bekezdés d) pontjában foglalt felhatalmazás alapján az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (3) bekezdésére is figyelemmel a Kenézy Gyula Kórház és Rendelőintézet (a továbbiakban: Kórház) nevében az alábbi Információbiztonsági Szabályzatot (a továbbiakban: Szabályzat) adom ki.

1. A Szabályzat célja

A Szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa a Kórház vonatkozásában az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását, valamint a jogosulatlan nyilvánosságra hozatalát.

A Szabályzat célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

A Szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig.

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

A Szabályzat alapszerkezete követi az ISO/IEC 27001:2005 szabvány „A" mellékletének („Szabályozási célok és kontrollok") szerkezetét. Ennek célja, hogy a Kórház hatékony és nemzetközi szabványon alapuló információbiztonsági irányítási rendszert alapozzon meg.

A Szabályzat a Kórház Szervezeti és Működési Szabályzata figyelembevételével készült.

2. A Szabályzat hatálya

2.1. Személyi hatálya

Jelen Szabályzat mindenkire nézve kötelező, aki használja a Kórház számítógép-hálózatát, annak berendezéseit (a továbbiakban: felhasználók). Az előbbieknek megfelelően a Szabályzat személyi hatálya kiterjed a Kórház összes munkavállalójára, aki a Kórház

számítógép-hálózatát és eszközeit használja. Ha a Kórház harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor a harmadik fél is köteles a Szabályzatban foglaltakat betartani.

2.2. Tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed:

- a védelmet élvező elektronikus adatok teljes körére, felmerülésüktől és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- a Kórház által bármely jogcímen használt valamennyi informatikai berendezésre,
- az informatikai eszközök műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

A Kórház számítógépes hálózata: részét képezik a következő típusú eszközök: passzív adatátviteli vonalak (típusuk szerint Ethernet, Token Ring, FDDI, ATM szegmensek, optikai és hagyományos összeköttetések, amelyek részben saját tulajdonúak, részben béreltek) és csatlakozók, aktív hálózati elemek (repeaterek, bridge-ek, switchek, routerek, transceiverek, modemek, terminálszerverek), továbbá minden hálózatra kötött számítógépes munkahely (PC, workstation, terminál, hálózati nyomtató) és szerver. A hálózatra nem csatlakoztatott számítástechnikai berendezések nem részei a Kórház számítógépes hálózatának. A Kórház számítógépes hálózata nyitott bármely olyan technikai megoldás befogadására, amely a meglévő szolgáltatásokat nem veszélyezteti, üzembiztonsága az elvárható szintet nyújtja.

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

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

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

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

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.

Adatvédelem: az információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény hatálya alá eső adatkör védelme.

Eszköz** (passzív és aktív hálózati elem, számítógépes munkahely, szerver) **üzemeltetője: annak a szervezeti egységnek a vezetője, amelynek használatában van az eszköz, illetve megbízás vagy szerződés alapján az üzemeltetésért felelős. Egyes eszközökhöz, eszközcsoportokhoz a főigazgató üzemeltetőt vagy üzemeltető egységet jelölhet ki.

BCP (Business Continuity Plan): üzletmenet (működés) folytonossági terv, az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik.

Biztonsági esemény: az informatikai rendszer védelmi állapotában beállt illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

DRP (Disaster Recovery Plan): katasztrófa utáni helyreállítási terv, magába foglalja az üzletmenet (működés) szempontjából kritikus adatok, hardver és szoftver működésének újraindítását természeti vagy ember által okozott katasztrófák esetén.

Felhasználó: az a személy, aki a Kórház számítógépes hálózatának valamely szolgáltatását igénybe veszi. Belső felhasználó a Kórházzal munka-, vagy megbízási jogviszonyban álló személy (a továbbiakban: felhasználó). Külső felhasználó a Kórházzal ilyen jogviszonyban nem álló személy. A külső felhasználók a Kórház publikus szolgáltatásait vehetik igénybe, egyéb szolgáltatások igénybevételére csak az üzemeltető határozott időre szóló engedélyével jogosultak. Ez utóbbi esetben rájuk is a belső felhasználókra vonatkozó szabályok érvényesek.

Incidens: a szolgáltatás standard működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.

Informatikai biztonság: az informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme — bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából — zárt, teljes körű, a kockázatokkal arányos és folyamatos.

- Teljes körű a védelem, ha a védelmi intézkedések az informatikai rendszer összes elemére, az ISO/OSI szabvány szerinti összes rétegére, valamint a végpontok közötti összes elemre kiterjednek.
- Zárt a védelem, ha az összes releváns fenyegetés figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál.

- Kockázattal arányos a védelem, ha kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékek összegével és a megvalósított védelmi intézkedések következtében a kockázatok elviselhető mértékűre mérséklődtek.
- Folyamatos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg.

Informatikai biztonságpolitika: A Kórház átfogó informatikai biztonságpolitikája minden munkatárs és választott tisztségviselő számára egységes értelmezésben azt határozza meg, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésével kapcsolatosan milyen biztonsági struktúrát és elveket kell követni, illetve milyen követelményeket szükséges teljesíteni.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése ellen. Az információvédelem az informatikai biztonság egyik alapterülete.

IT szolgáltatás: bármilyen, a Kórháznál használt vagy bevezetni szándékozott IT rendszerrel összefüggő, azzal kapcsolatos szolgáltatás.

Kockázat: a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázatot a kárnagyság és a bekövetkezés gyakoriság szorzataként definiáljuk egy megadott időtávon.

Megbízható működés: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a rendelkezésre állás és a funkcionalitás sérülése, elvesztése ellen. A megbízható működés az informatikai biztonság másik alapterülete.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

Probléma: a probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető föl. A probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

Rendelkezésre állás: annak a valószínűsége, hogy egy definiált időintervallumon belül az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.

SLA (Service Level Agreement): szolgáltatási szint megállapodás, egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (a jelen Szabályzat alkalmazása során a szolgáltatásért felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és feltételeit.

Szolgáltatásért felelős szervezeti egység: az IT és telekommunikációs szolgáltatás nyújtására alkalmas infrastruktúrával rendelkező önálló szervezeti egység, mely az adott szolgáltatás nyújtásának feltételeit a felhasználók számára nyilvánosságra hozza.

Üzletmenet-folytonosság és katasztrófa-elhárítás tervezés: az informatikai rendszer és a benne kezelt adatok, valamint a környezetüket képző összes rendszerelem csoportra vonatkozó védelmi intézkedések meghatározására irányuló tervezési tevékenység üzemzavarok és katasztrófa esetére. A védelmi intézkedések érvényesítésével az adatok védelme és/vagy visszaállíthatósága valósítható meg üzemzavar vagy katasztrófa események estén. Angol nyelvű elnevezése: Business Continuity Planning (rövidítése: BCP) és Disaster Recovery Planning (rövidítése: DRP).

4. A kötelező felülvizsgálat (revízió) időpontja és a Szabályzat változásmenedzsmentje

4.1. A Szabályzat karbantartása

A Szabályzatot az informatikában – valamint a Kórháznál – a fejlesztések során bekövetkező változások miatt időközönként, szükségszerűen aktualizálni kell.

A Szabályzat felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a szabályzatban leírtakban jelentős változás(ok) történnek.

A felülvizsgálat a belső szabályozó dokumentumok elkészítésének, módosításának helyben kialakított, külön eljárási rendje szerint történik.

4.2. A Szabályzat alkalmazásának módja

A Szabályzat megismerését az érintett munkavállalók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.

A Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni a Szabályzat előírásainak megfelelően.

5. Kapcsolódó szabályozások

A Szabályzat előírásai összhangban vannak a Kórház belső szabályozó dokumentumaival, különösen:

- az Adatvédelmi és adatkezelési Szabályzattal,
- a Számviteli politikával,
- a Szervezeti és Működési Szabályzattal,
- a munkaköri leírásokkal.

6. Információbiztonsági Politika

Az Információbiztonsági Politika célja, hogy a Kórház szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitásainak biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembe vételével meghatározható az információbiztonsági szabályozás alapján minősített adatokat kezelő informatikai rendszerek biztonsági osztályba sorolása; kidolgozhatóak a konkrét, rendszer szintű információbiztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez szükséges alapelveket és követelményeket.

6.1. Az Információbiztonsági Politika elfogadása és közzététele

Az Információbiztonsági Politikát a Szabályzat részeként kezeljük, ezért elfogadása és közzététele a Szabályzattal megegyező módon történik, azaz az üzemeltetési felelős előterjesztése alapján a főigazgató fogadja el. A jelen Szabályzat mellékletét képező

Információbiztonsági Politika (*2. sz. melléklet*) az egyes szervezeti egységeknél kifüggesztve is megtekinthető.

6.2. Az Információbiztonsági Politika rendszeres felülvizsgálata

Az Információbiztonsági Politika a Szabályzat szerves része, és azzal egy időben és azonos módon történik a felülvizsgálata:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni),
- minden olyan esetben, amikor a politikában leírtakban jelentős változás(ok) történnek.

7. A Szabályzat biztonsági fokozata

A Kórház adatai különböző biztonsági fokozatokba tartozhatnak (pl. egészségügyi adatok, személyes adatok, üzleti titkok, pénzügyi adatok, illetve a Kórház belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas) adatok.

7.1. IT rendszerek biztonsági osztályai, besorolás

Kritikus rendszerek (A)

Az intézmény működése szempontjából kritikus, az intézmény egészére kiterjedő rendszerek, amelyek szenzitív, illetve személyes adatokat tartalmaznak. Adatvédelmi szempontból kiemelt védelmet igényelnek:

- bér- és munkaügyi rendszer,
- medikai rendszerek,
- gazdasági, ügyviteli rendszer,
- dokumentumkezelési rendszer,
- központi levelező kiszolgálók,
- központi tárhely-kiszolgálók,
- intézményi autentikációs rendszerek.

Kiemelt rendszerek (B)

Az intézmény működése szempontjából kritikus rendszerek, amelyek elsősorban technikai jellegűek, a rajtuk tárolt adatok nem személyes jellegűek:

- telekommunikációs hálózat,
- technológiai (environment, middleware) rendszerek,
- kommunikációs rendszerek.

Normál rendszerek (C)

A vagy B kategóriába nem sorolt, a teljes intézmény napi működése szempontjából nem kritikus, illetőleg az intézménynek csak egyes részeire kiterjedő olyan rendszerek, amelyek

indítása/üzemeltetése során központi felülvizsgálat történik, illetőleg teljes körű dokumentáció készül:

- interaktív kiszolgáló szerverek.

Egyéb rendszerek (D)

Az előző három kategóriába nem sorolt rendszerek.

A Kórház az A és B kategóriákat egyforma szinten, kritikus rendszerként kezeli.

Információbiztonsági alapelvek:

A Kórház szervezeti egységei által kezelt adatok védelmét bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából úgy kell megvalósítani, hogy az informatikai rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint megvalósuljon a zárt szabályozási ciklus, a következők szerint:

1. A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén kell érvényesíteni, úgymint:
    - az összes információbiztonsági rendszerelem csoportra,
    - az informatikai rendszer infrastrukturális környezetére,
    - a hardver rendszerre,
    - az alap- és felhasználói szoftver rendszerre,
    - a kommunikációs és hálózati rendszerre,
    - az adathordozókra,
    - a dokumentumokra és feljegyzésekre,
    - a belső személyzetre és a külső partnerekre,
    - mind a központi, mind a végponti informatikai eszközökre és környezetükre.
2. A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedés megvalósul.
3. A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.
4. A védelem folytonossága úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket a rendszerből történő kivonásig folytonosan biztosítani kell a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel.
5. A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.

További célok és elvek:

A Kórház igyekszik a kockázatot minimalizálni, de minden munkavállalóban tudatosítja, hogy teljes körű védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállalja.

A Kórház a felelősségeket az információbiztonság területén hangsúlyozottan elhatárolja, és az egyes szervezeti szerepkörökhöz köti.

A Kórház hangsúlyozottan törekszik a törvényi és jogszabályi megfelelőségre, különös tekintettel a személyes és különleges adatok kiemelt védelmére. A Kórház az alapvető jogok biztosának ez irányú állásfoglalásait figyelembe veszi.

A Kórház megpróbálja kiegyensúlyozottan kezelni a mobilitás lehetősége és a biztonság közötti ellentmondást.

Elsődleges cél a működőképesség fenntartása, ezért az olyan felhasználókat, akik magatartásukkal más felhasználók tömegeinek munkáját veszélyeztetik, a Kórház haladéktalanul kizár a szolgáltatásból mindaddig, amíg a veszélyt okozó tevékenységüket meg nem szüntetik.

A védelem mellett a Kórház biztosítja az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.

A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatóak. Az információbiztonsági incidensek esetében a felelősség a jogosultsággal bíró személyhez kötődik. A Kórház rosszhiszemű felhasználásnak tekinti, ha a felhasználó jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani.

Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatásmonitorozó komponensek jelezzék.

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

Az adatok és információk osztályozása jelentőségük és bizalmassági fokozatuk alapján az alábbiak szerint történik:

- közlésre szánt, bárki által megismerhető adatok, közérdekű adatok
- minősített, egészségügyi, pénzügyi, számviteli, munka- és bérügyi titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek az adat védelme az érdekkörébe tartozik.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt munkavállalók előtt az adatvédelmi 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 lehetőség szerint 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 rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést, vagy annak a kísérletét a Kórház főigazgatójának jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai osztály vezetője felelős.

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

7.3. 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.

7.3.1. A védelem tárgya

A védelmi intézkedések kiterjednek:

- 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 rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.

7.3.2. 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.

7.4. A védelem felelőse

A védelem felelősei az informatikai osztály vezetője.

A jelen Szabályzatban foglaltak szakszerű végrehajtásáról a Kórház főigazgatójának kell gondoskodni.

7.4.1. Informatikai biztonság felelős feladatai

a) Informatikai osztályvezető feladatai:

- a Szabályzat kezelése, naprakészen tartása, módosítási javaslatok kidolgozása,
- javaslattétel a rendszer szűk keresztmetszeteinek felszámolására,
- a védett adatok körének meghatározása,
- az adatkezelés és adatfeldolgozás felügyeletének ellátása,
- a védelmi előírások betartásának ellenőrzése,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenység adminisztrálása,
- a szoftverek használata jogszerűségének ellenőrzése.

b) Rendszergazda feladatai:

- a saját feladatkörébe tartozó rendszer felügyelete,
- az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok készítéséért és karbantartásáért felel,
- a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról történő gondoskodás,
- védelmi eszközök működésének folyamatos ellenőrzése,
- a kórházi informatikai rendszer hardver eszközeinek karbantartásáért felel,
- a beszerzett, illetve üzemeltetett hardver és szoftver eszközök, licencek nyilvántartása,
- a folyamatos vírusvédelemről történő gondoskodás,
- a vírusfertőzés gyanúja esetén a fertőzött rendszerek vírusmentesítéséről történő gondoskodás,
- a rendszer működése és biztonsága szempontjából a lényeges paraméterek alakulásának folyamatos figyelemmel kísérése és vizsgálata,
- a rendszer adminisztrációjának ellenőrzése.

7.4.2. Az informatikai osztályvezető ellenőri feladatai

- évente egy alkalommal a Szabályzat előírásai betartásának részletes ellenőrzése,
- a védelmi eszközökkel való ellátottság rendszeres ellenőrzése,
- előzetes bejelentési kötelezettség nélkül az informatikai munkafolyamat bármely részének ellenőrzése.

7.4.3. Az informatikai osztályvezető jogai/kötelezettségei

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Kórház főigazgatójánál,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,

- betekinthet valamennyi iratba, amely az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi,
- a Kórház intézeti adatvédelmi felelőse részére éves beszámolót készít az információbiztonság megvalósulásáról, illetve az esetleges jogsértésekről, rendkívüli eseményekről.

8. Az információbiztonság szervezeti kérdései

8.1. Az információbiztonság belső szervezete

Az információbiztonsággal kapcsolatos felelősség megoszlik a főigazgató, és az Informatikai Osztály munkavállalói, az egyes szervezeti egységek és a felhasználók között. A felelősség-megosztás elveit az alábbiakban tárgyaljuk.

8.2. Vezetői elkötelezettség

Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának kialakításáért és fenntartásáért.

A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják.

A belső és külső szolgáltatói megállapodások (SLA-k) figyelése, figyelembe vétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség kinyilvánítása. Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása szintén a vezetői elkötelezettséggel összhangban zajlik.

A kórházi informatikai rendszerek Szabályzatnak való megfeleltetése a főigazgató hatásköre.

8.3. Információbiztonsági koordináció (érintett felekkel egyeztetés)

Az informatikai rendszerek Szabályzatnak való megfeleléseinek vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást a főigazgató, az üzemeltetési felelős és a minőségirányítási vezető végzi (a külső audit igények kivételével). A Szabályzatnak történő megfelelés vizsgálatát a főigazgató vagy a rendszert üzemeltető szervezeti egység vezetője kezdeményezheti. Az egyes információbiztonsági védelmi intézkedésekkel kapcsolatos döntések fórumai a gyógyító osztályok osztályértekezletei, illetve a főorvosi, főnővéri értekezletek. Ezen fórumokon történik a megtett intézkedésekre vonatkozó beszámolók előterjesztése.

8.4. Az információbiztonsági felelősségek allokációja

Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres a Szabályzatnak való megfelelőségi vizsgálata, minden negatív biztonsági esemény felelőssége az üzemeltető szervezeti egység vezetőjét terheli.

Azon rendszerek esetében, ahol megfelelőségi vizsgálat sikeres volt, illetőleg a vizsgálat során készült és elfogadott hiánylistát az üzemeltető pótolta, a negatív biztonsági események felelőssége egyedi vizsgálat alapján állapítható meg. A Szabályzat betartása esetén az üzemeltető jóhiszeműnek minősül.

A főigazgató felelőssége az információbiztonsági eseményeknek, az incidensek tanulságainak és a pozitív példáknak a megjelenítése a cég szokásos információs csatornáin.

8.5. Új információ-feldolgozó rendszerek elfogadási eljárása

Új informatikai szolgáltatás indítási kérelemhez csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján a főigazgató a szolgáltatás engedélyezése előtt javaslatot kérhet az üzemeltetési felelőstől a Szabályzat mellékleteinek aktualizálására, az új szolgáltatás Szabályzat szerinti paramétereinek megállapítására.

8.6. Bizalmassági nyilatkozatok

Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban titoktartási nyilatkozatot írnak alá a rendszerek üzemeltetői, illetve a felhasználók is abban az esetben, amennyiben erről az adott rendszer SLA-ja külön rendelkezik.

A rendszer üzemletetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.

A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott információkat védeni kell.

Minden bizalmassági kérdésben érintett szereplővel nyilatkozatot kell kitöltetni, melynek aláírásával vállalja, hogy a birtokában levő információval nem él vissza.

8.7. Kapcsolattartás hatóságokkal

A különböző törvényekben és rendeletekben előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése a főigazgató felelőssége. A Kórház jogi képviseletet nem lát el az egyének jogvitáiban a hatóságokkal szemben.

8.8. Kapcsolattartás különleges érdekközösségekkel

A főigazgató felelős a különleges érdekközösségekkel történő kapcsolattartásért.

Minden hivatalos tagsági és kapcsolattartási kérdésben a Kórház érdekeinek figyelembe vételével a főigazgató dönt.

A felhasználók egyéni tagsága az adott személy felelőssége. Egyéni tagként is köteles a kapcsolattartás során a Szabályzat rá vonatkozó előírásait betartani.

8.9. Külső felek

8.9.1. A külső felekhez, partnerekhez kapcsolódó kockázatok azonosítása

A külső felekkel, partnerekkel való kapcsolattartás szabályai:

- Személyes, különleges vagy más intézményi adatok kiadása csak a hatályos jogszabályoknak megfelelően történhet.
- Az átadott adatok védelméért a szerződő fél felelősséggel tartozik.
- Adatvédelmi és információbiztonsági kérdésekben a kapcsolattartó tanácsot kérhet a mindenkori informatikai osztályvezetőtől, valamint a Kórház intézeti adatvédelmi felelősétől.

8.9.2. Ügyfelekkel kapcsolatos információbiztonsági feladatok (jogosultságkiadás felhasználóknak)

Az A, B és C osztályú rendszerek esetében az installálási időszakon kívüli partner hozzáférést az üzemeltetők eseti kérelme alapján a főigazgató vagy az általa megbízott felelős

engedélyezheti. A kérelemnek tartalmaznia kell az ügyfél adatait, a hozzáférés indokát, módját, paramétereit és tervezett időtartamát. Engedély nélküli hozzáférés biztosítása esetén az adott informatikai rendszer nem felel meg a Szabályzatban foglaltaknak.

8.9.3. Harmadik féllel kötött megállapodások biztonsági kérdései

Minden harmadik féllel kötött megállapodásban rendelkezni kell adatvédelmi és információbiztonsági kérdésekről.

9. Az információs vagyon menedzsmentje

9.1. Felelősség az információs vagyonért

9.1.1 Információs vagyonleltár

Az információs vagyon az üzemetetési dokumentációkban leírtak alapján meghatározott.

Az intézmény A, B és C kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások paramétereinek nyilvántartását az Informatikai Osztály végzi. Az ehhez szükséges adatszolgáltatás a rendszerek üzemeltetőinek Szabályzatból fakadó kötelezettsége.

A szoftvereket és adathordozókat az Eszközök és források leltárkészítési és leltározási szabályzatában foglaltaknak megfelelően kell leltározni. Az önleltározást az osztály kijelölt leltárfelelősének negyedévente el kell végeznie, melyről jelentési kötelezettsége van az informatikai osztályvezető felé.

9.1.2. Az információs vagyon tulajdonjoga

A Kórház A, B és C kategóriájú rendszereinek intézmény-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, amely a vásárolt rendszerben található állapottól eltér) a Kórház tulajdonát képezik. Ugyanezen rendszerekben tárolt minden intézményi adat a Kórház tulajdonát képezi. Ezen adatok felhasználási joga kizárólag a Kórházat illeti meg, amely alól kivételt képeznek az egészségügyi adatok, ezzel az érintett beteg rendelkezik, ezen adatok kezelésére a Kórház adatvédelmi és adatkezelési szabályzata tartalmaz előírásokat.

9.1.3. Az információs vagyon használatának szabályai

Minden munkavállaló és üzleti partner a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását a munkavállalók esetében a felettesnél, üzleti partner esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni.

Az SLA-k rögzítik az egyes szolgáltatásokkal kapcsolatos információs vagyon, valamint jogosultságkezelési és használati szabályokat. Mindenfajta változtatás az SLA-k változtatási rendjének megfelelően végezhető.

Adatok kiadása a különböző biztonsági osztályba sorolt rendszerekből csak a főigazgató engedélyével lehetséges, kivételt ez alól az az eset képez, amikor az adatcserét, adatátadást jogszabály vagy szerződés rögzíti. Ebben az esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

9.2. Az információs vagyon osztályozása

9.2.1. Az osztályozás elvei, vezérfonala

Az információvédelem területén történő osztályozás az adatok minősítési szintjével növekvő mértékű, a bizalmasság, hitelesség és a sértetlenség sérüléséből vagy elvesztéséből származó kárszinteken alapul.

- Információvédelmi alapbiztonsági osztály:

  Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

- Információvédelmi fokozott biztonsági osztály:

  A szolgálati titok, valamint a nem minősített adatok közül a különleges adatok, nagy tömegű személyes adatok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.

- Információvédelmi kiemelt biztonsági osztály:

  Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

9.3. Az osztályba sorolt információs vagyonelemek jelölése és kezelése

Az információs vagyonelemek besorolásának, jelölésének végrehajtásáért a főigazgató felelős.

10. Emberi erőforrással kapcsolatos biztonsági kérdések

A Kórház vonatkozásában az emberi erőforrással kapcsolatos teendőket a Jogi és Humánpolitikai Igazgatóság végzi. Ezekben a kérdésekben a Munkaügyi és Bérszámfejtési Eljárási Szabályzat irányadó.

10.1. Alkalmazás előtti tennivalók (szerepek és felelősségek, alkalmazási feltételek)

Az erre vonatkozó szabályokat a Munkaügyi és Bérszámfejtési Eljárási Szabályzat tartalmazza.

10.2. Az alkalmazás során irányadó tennivalók (felelősségek menedzsmentje, információbiztonsági képzések és tréningek, fegyelmi ügyek)

Az A, B és C kategóriájú rendszerek esetében minden üzemeltető, fejlesztő vagy felhasználó csak a munkakörének ellátásához szükséges jogosultságokat birtokolhatja. (Azon fejlesztői rendszerek, amelyek személyes, különleges vagy más intézményi adatokat nem tartalmaznak, nem minősülnek kategorizált rendszernek.)

Az A és B osztályú rendszerek bizonyos szolgáltatásainak igénybevételéhez (pl. gazdasági rendszer) a főigazgató tanfolyam és/vagy vizsga teljesítését írhatja elő. A kritériumok teljesítésének költsége a Kórházat terheli.

A Szabályzat előírásainak szándékos és tudatos megsértése esetén a munkavállaló a Kórház vonatkozó előírásainak megfelelően szankcionálható.

10.3. Munkaviszony megszüntetése, szünetelése vagy munkakörváltozás (munkaviszony megszüntetésével kapcsolatos felelősség, munkavállalónak kiadott eszközök visszavétele, hozzáférési jogok megvonása)

A Kórház munkavállalóinak felhasználói azonosítóját munkaviszonyuk megszűnésével, a külső személyek – ideértve a rezidenseket is – felhasználói azonosítóját megbízatásuk lejártával haladéktalanul le kell tiltani. A megszűnt munkaviszony/egyéb jogviszony esetén a felhasználó a rendszer szolgáltatásait nem veheti igénybe és erőforrásait nem használhatja. A munkaviszony/egyéb jogviszony megszűnését az érintett szervezeti egység vezetője haladéktalanul köteles jelezni az Informatikai Osztály vezetőjének.

Amennyiben a volt munkavállaló a fenti tevékenységeket céges partnerként végzi a továbbiakban, akkor a szerződés megkötése után új, partneri hozzáférés biztosítható számára az ott részletezett szabályok alapján.

Az a munkavállaló, akinek a munkaviszonya megszűnt, a C és D kategóriájú rendszerekben, a (kizárólag) személyes adatainak elérésére szolgáló belépési kódjait az üzemeltető eseti engedélye alapján megtarthatja.

A jogviszonyukat huzamosabb ideig szüneteltető (pl.: gyermek szülése), illetve a tartósan más okból távollévő (pl.: elhúzódó gyógykezelés) munkavállalók felhasználói azonosítóját le kell tiltani (fel kell függeszteni), illetve munkába állásukkal egy időben ismét engedélyezni kell.

A munkavállalók áthelyezése kapcsán felmerülő jogosultsági változásokat (felhasználói azonosítók letiltása, vagy a jogosultságok törlése, illetve új azonosítók vagy jogosultságok létrehozása) az áthelyezéssel egy időben, haladéktalanul át kell vezetni.

11. Fizikai és környezeti biztonság

11.1. Biztonsági zónák, területek

11.1.1. Fizikai biztonsági határvédelem

A, B kategóriájú szolgáltató-rendszer kritikus fizikai komponensei (szerver, tároló alrendszer, router... stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeknek mechanikai nyitórendszerrel (biztonsági zár vagy beléptető kártyával működtethető mágneses zár) és beléptető rendszerrel kell rendelkezniük. A beléptető rendszer szükséges alapfunkciói: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépés jelzése a biztonsági személyzet felé.

A C kategóriájú rendszerek esetében minimálisan biztonsági zárral ellátott helyiséget kell biztosítani, a kulcsokról és a belépésről írásos helyiségnaplót kell vezetni.

11.2. Fizikai belépési szabályozás

Az A és B kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (géptermek, kábelrendezők) való belépési jogosultságot a főigazgató, C kategóriájú rendszer esetében az üzemeltető szervezeti egység vezetője engedélyezi a munkavállalónak vagy a partnernek a helyiségek és a végezhető tevékenységek felsorolásával.

A belépési lehetőséggel rendelkezők ezen jogosultságukat nem ruházhatják át másik munkavállalóra vagy partnerre.

Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli. Az illegálisan szerzett belépési lehetőség használata betörésnek minősül és jogi következményeket von maga után.

11.3. Irodák, szobák és egyéb létesítmények fizikai biztonsága

Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános területek használati módjával. Kitüntetett hozzáférést vagy védett adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhetőek el.

Az informatikai célú helyiségekkel kapcsolatos kérdésekben az üzemeltetési felelős a felelős a ki- és az átalakítás koordinációjáért, a szakmai a biztonsági szempontok betartásáért.

Kiemelt fontosságú helyiség a szerverszoba, mely használatának szabályait az ebben a témakörben irányadó szabályok részletezik.

11.4. Külső és környezeti károk elleni védelem

A, B és C kategóriájú szolgáltató-rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten, vagy az alatta elhelyezkedő helyiségek esetében az ár- és belvízvédelmi szabályozásnak is meg kell felelni.

Egyedi esetben a főigazgató egyéb előírásokat is megfogalmazhat.

A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, amely tűzjelzés esetén a biztonságos oltás feltételeit megteremti.

Minden fenti helyiség esetén biztosítani kell azt a gépészeti hűtési kapacitást, amely a teljes termelt hőmennyiség biztonságos elvezetését automatikusan meg tudja oldani.

Minden fenti helyiség esetén biztosítani kell azt az erősáramú ellátó kapacitást, amely a berendezések megtáplálását túlterhelésmentesen el tudja végezni. Az erősáramú ellátó rendszernek áramkör-szelektív biztosítókkal kell rendelkeznie.

11.5. Munkavégzés biztonsági zónákban

A minősített rendszereket tartalmazó helyiségekben minden olyan munkavégzés, amely az informatikai rendszereket vagy azok működését veszélyeztetheti – kizárólag előzetes egyeztetés alapján és – felügyelet mellett végezhető. Az egyeztetést a munkavégző cég és az üzemeltető szervezeti egység vezetője végzi, az üzemeltetési felelős szervezésében és lebonyolításával. A helyiség gépészeti berendezéseit veszélyeztető munkák csak az Informatikai Osztály előzetes engedélyével folytathatóak.

11.6. Nyilvános hozzáférés, szállítási és töltési területek

A minősített rendszereket tartalmazó helyiségekben minden szállítási tevékenység csak belépésre jogosult munkavállaló felügyelete mellett végezhető.

11.7. Eszközbiztonság

11.7.1. Eszközök elhelyezése, védelme

Minden minősített rendszerkomponens fizikai elhelyezésénél törekedni kell a gépterem/kábelrendező helyiség felépítési elveinek betartására (pl. rackben történő elhelyezésre, megfelelő ventillációs irányra... stb.)

Ezen irányelveket új komponens beszerzése esetén a főigazgató írhatja elő.

11.7.2. Támogató közművek (szolgáltatások)

A gépterem/kábelrendező helyiségekben üzembe állítandó új rendszerek (vagy nagyobb rendszerkonfiguráció módosítás) esetében az installálást végző szakembereknek előzetesen konzultálniuk kell a rendszergazdával az erősáram és hűtési igény biztosításáról. A szükséges gépészeti módosításokat az új rendszer üzembe állítása előtt el kell végezni.

11.7.3. Kábelbiztonság

A kiemelt rendszerek védett helyiségen kívül húzódó, összekötő komponenseit (telefon és gerinchálózati kábeleket) tartalmazó alépítmények, kábelaknák és védőcsövek az üzemeltetési felelős által felügyelt területnek minősülnek. Azokban munkát végezni, vagy a megközelíthetőségüket korlátozni csak a rendszerkomponens üzemeltetőjének előzetes engedélyével lehet.

11.7.4. Eszközkarbantartás

Minden szolgáltató rendszer üzemeltetője köteles a hardver komponensek karbantartási igényét felmérni és ezeket úgy ütemezni, hogy a rendszer élettartama karbantartási hiányosságok miatt ne rövidüljön.

A Kórház külön karbantartási tervvel rendelkezik.

A karbantartás során a felmerült biztonsági sérülékenységeket megfelelően kell kezelni, illetve úgy kell a karbantartásokat elvégezni, hogy újabb biztonsági kockázatok ne merüljenek fel. Ennek felelőse a karbantartást végrehajtó személy vagy szervezet.

11.7.5. Telephelyen kívül használt eszközök biztonsági szabályai

A telephelyekről kivitt eszközök használata során bekövetkező károkért (adatvesztés, adatszivárgás) az a személy viseli a felelősséget, aki az eszközt kivitte. A telephelyen kívüli használat során mindazon elvek és gyakorlat követendő, amelyeket a Szabályzat egyes fejezetei leírnak.

11.7.6. Eszközök biztonságos megsemmisítése vagy újrahasznosítása

A használt eszközök selejtezése a Kórház hatályos szabályainak figyelembevételével történik. Speciális eszközök selejtezése esetén az üzemeltető gondoskodik a szakszerű elhelyezésről, illetve átadás-átvételi jegyzőkönyv alapján ezt a tárolási/elszállítási feladatot átadhatja a selejtezési feladatok ellátásáért felelős szervezeti egységnek.

A, B és C kategóriás adattároló eszközök selejtezésénél gondoskodni kell az azon tárolt adatok selejtezés előtti fizikai megsemmisítéséről is.

11.7.7. Eszközök (HW, SW) kivitele telephelyről

Az eszközök ki-, illetve beszállítását szállítólevéllel kell igazolni, amelyen az eszköz(ök) egyedi azonosítóját – ha értelmezhető – fel kell tüntetni.

12. Az informatikai eszközbázist veszélyeztető helyzetek

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

12.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
  - földrengés,
  - árvíz,
  - tűz,
  - villámcsapás...stb.,
- környezeti kár:
  - légszennyezettség,
  - nagy teljesítményű elektromágneses térerő,
  - elektrosztatikus feltöltődés,
  - a levegő nedvességtartalmának emelkedése vagy csökkenése,
  - szennyeződés (pl. por),
- közüzemi szolgáltatásban bekövetkező zavarok:
  - feszültség-kimaradás,
  - feszültségingadozás,
  - elektromos zárlat,
  - csőtörés.

12.2. 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,
- gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- 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.

13. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

13.1. Tervezés és előkészítés során előforduló veszélyforrások

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

13.2. A rendszerek megvalósítása során előforduló veszélyforrások

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

13.3. A működés és fejlesztés során előforduló veszélyforrások

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

14. Az informatikai eszközök környezetének védelme

14.1. Vagyonvédelmi előírások

- A géptermek külső és belső helyiségeit biztonsági zár védi.
- A gépterembe való be- és kilépés rendje szabályozott.
- A gépterembe, szerverterembe történő illetéktelen behatolás tényét a Kórház főigazgatójának azonnal jelenteni kell.

- Az informatikai eszközöket csak a Kórház arra felhatalmazott munkavállalói használhatják.
- Az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

14.2. Adathordozók

- Az adathordozókat 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 (floppy, CD, DVD, pendrive stb.) a tárolásra kijelölt helyről kell kivenni, és oda kell vissza helyezni is.
- A munkaasztalon, jogosulatlan hozzáférés elkerülése miatt, csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek.
- Adathordozót másnak átadni csak engedéllyel és dokumentált formában szabad.
- A munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

14.3. Tűzvédelem

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

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

A Kórház géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.

A Kórház géptermeiben, szerverszobáiban elektromos, vagy más munkát csak a tűzvédelmi felelős tudtával, illetve engedélyével szabad végezni.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. Ezen adatállományok kijelölése az informatikai vezető feladata.

A Kórház egyéb területén a Tűzvédelmi Szabályzatban leírtak az irányadóak.

15. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

15.1. A számítógépek és szerverek védelme

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

- a még használható anyag mentése,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok, illetve eszközök használatával a feldolgozás folytatása.

15.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.

A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik.

A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

15.3. Az informatikai feldolgozás folyamatának védelme

15.3.1. Az adatrögzítés védelme

- Az adatbevitel hibátlan műszaki állapotú berendezésen történjen.
- Csak tesztelt adathordozóra lehet adatállományt rögzíteni.
- A bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani.
- Az adatrögzítő szoftver védelme: lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják 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 személyek férjenek hozzá).
- Az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.

  Az adatrögzítés folyamatához kapcsolódó dokumentációk:

  - adatrögzítési utasítások,
  - ellenőrző rögzítési utasítások,
  - tesztelő és törlő programok kezelési utasításai,
  - megőrzési utasítások,
  - gépkezelési leírások.

15.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

15.3.3. Adathordozók tárolása

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

15.3.4. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott őrzési kötelezettségnek megfelelően kell kialakítani.

15.3.5. Selejtezés, sokszorosítás, másolás

A selejtezést a Kórház Felesleges vagyontárgyak hasznosítási, selejtezési szabályzata alapján kell lefolytatni.

Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít.

15.3.6. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.

A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkavállalók (felhasználók) feladata.

A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.

A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák felelősek.

15.4. Szoftver védelem

15.4.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetőek legyenek a felhasználók számára.

15.4.2. Felhasználói programok védelme
Programhoz való hozzáférés, programvédelem

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

Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek, jogszabályi elvárásoknak megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni.

A számvitelről szóló 2000. évi C. törvény értelmében a Kórháznak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig meg kell őrizni.

Az egészségügyi ellátás során keletkező adatok esetében az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény tartalmazza a megőrzési időket.

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 a vezetők felelősek.

16. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

16.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.

A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftverekről biztonsági másolatot kell készíteni.

16.2. Munkaállomások

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

Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

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

A Kórház informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

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

Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

17. Kommunikáció és üzemelés menedzsment

17.1. Működési folyamatok és felelősségek

Amennyiben egy szervezeti egység szolgáltatás-indítási kérelemmel fordul a főigazgatóhoz, ezzel elismeri, hogy megfelel a Szabályzat kritériumainak. A szolgáltatás-indítási kérelem csak adathiány vagy a Szabályzatban foglaltak megsértése esetén utasítható el. Az elutasítást részletesen indokolnia kell a főigazgatónak, nem kizárva egy esetleges módosított kérelem beadását.

Minősített (A, B illetve C osztályú rendszerek) esetében a Szabályzatnak történő megfelelést a főigazgató esetileg vizsgálhatja, és az esetleges hiánypótlásra az üzemeltetőt felszólíthatja. Amennyiben a vizsgált informatikai rendszer maga is más informatikai szolgáltatásokat használ, úgy a használt szolgáltatás SLA-ja is vonatkozik rá.

Minden informatikai rendszer esetében a használatra vonatkozó igény bejelentése – hozzáférés vagy felhasználói azonosító igénylése – a szolgáltatási SLA elfogadásának szándéknyilatkozatát is jelenti. A hozzáférés megadásával az SLA a szolgáltató és az igénybevevő között életbe lép.

Az A és B osztályú rendszerek esetében az SLA-ban vállalt szolgáltatási és rendelkezésre állási paraméterek alulteljesítése miatt a Kórházat anyagi és egyéb kár érheti. Ilyen esetekben a felelősség megállapítására és a szükséges lépések megtételére (rendszer-módosítás, szabályzat-módosítás) a főigazgató eseti bizottságot nevezhet ki. Ezen bizottságnak mindig tagja az üzemeltetési felelős.

17.2. Harmadik fél által nyújtott szolgáltatások menedzsmentje

A harmadik fél által nyújtott informatikai szolgáltatások is SLA kötelezettek, a kritikus paramétereket a partnerrel kötött szolgáltatási szerződésben is rögzíteni kell. A szerződésnek ki kell terjednie az információbiztonsági és adatbiztonsági kérdésekre is.

Az SzMSz-ben meghatározott főigazgatói kompetenciák (IT szolgáltatások) esetében a Kórház egykapus ügyintézést és érdekképviseletet alkalmaz. Ezen szolgáltatók esetében az ügyfélkapcsolatra az üzemeltetési felelős, szerződéskötésre a főigazgató jogosult.

17.3. Rendszertervezés és elfogadás

Az informatikai szolgáltató rendszerek esetében a Szabályzatnak történő megfelelést már a tervezési szempontok között szerepeltetni kell. A Kórház által üzemeltetni tervezett A, B és C osztályú rendszerek esetében a Szabályzatnak történő megfelelés a szolgáltatás indításának szükséges feltétele. A Kórház informatikai rendszerei esetében a szolgáltatás megindítását a főigazgató engedélyezi a informatikai osztály vezetőjének javaslata alapján.

17.4. Védekezés vírusok és egyéb kártékony kódok ellen

Azon rendszerek esetében, ahol a kártékony és mobil kódok előfordulhatnak, a detektálásukat és elhárításukat végző komponensek installálása a szolgáltatási engedély kiadásának feltétele.

Minden olyan rendszer esetében, ahol vírusfenyegetés fennáll és lehetséges installálni vírusvédelmi rendszert, valamint a kémprogram-jelző komponenst, akkor ott az a szolgáltatás üzembe helyezésének és üzemeltetésének feltétele.

Publikus levelező rendszerek esetében az intézményen kívüli kapcsolat létesítésének feltétele a levelek informatikailag veszélyes tartalmának vizsgálati képessége illetőleg az „open relay" lehetőség kiküszöbölése.

Felhasználói tulajdonú adathordozók használata esetén az adott eszköz használata következtében okozott károkért a Kórház rendszereiben felhasználóként belépett személy a felelős (pl. vírusos USB kulcs).

17.5. Biztonsági mentések

Minden A, B és C osztályú szolgáltató rendszer üzemeltetési leírásának tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, és a mentéséért felelős személyt, a mentés tárolási rendjét, mentés külső tárolásának rendjét).

A és B osztályú rendszerek esetén külső tárolású (offsite) mentésekkel is kell rendelkezni, C és D osztályú rendszerek esetén onsite mentések is elfogadhatóak.

A mentési rendnek az alkalmazásra vonatkozó részét úgy kell megállapítani, hogy új hardware biztosítása esetén a rendszer működőképessége tetszőleges komponens meghibásodása vagy adatvesztése esetén helyreállítható legyen. Ennek érdekében az alkalmazás futó kódját legalább minden release váltás előtt és után menteni kell, a mentést minimum egy évre visszamenőleg meg kell őrizni.

Minden A, B és C osztályú rendszer esetében évente minimum egy alkalommal visszatöltési gyakorlatot (tesztelés) kell tartani, ami a mentések felhasználhatóságát ellenőrzi. A visszatöltési gyakorlat a szolgáltató rendszerrel funkcionálisan egyező tesztrendszeren is teljesíthető. A mentések meglétét és a visszatöltési gyakorlatot a főigazgató ellenőrizheti.

A Kórház által használt rendszerek mentési szabályait az e témakörben irányadó szabályok részletezik.

17.6. Hálózatbiztonság menedzsmentje

Az intézmény teljes területére kiterjedő alapinfrastruktúra (számítógépes és telefonhálózat) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását és a szükséges operatív beavatkozásokat a telekommunikációs hálózat üzemeltetésével megbízott szervezeti egység végzi. A kommunikációs hálózathoz való csatlakozás feltétele a – csatlakozás módjától és a csatlakoztatott rendszertől függő – biztonsági előírások maradéktalan betartása. Ezen előírások a csatlakozásnak, mint szolgáltatásnak az igénybevételi feltételei között tekinthetők meg (lásd a vonatkozó SLA-kat).

17.7. Médiakezelés

Az A és C osztályú rendszerek adatterületeinek mentései jogvédelem alá első intézményi és személyes adatokat tartalmazhatnak. Ezen adathordozókat olyan körültekintéssel kell tárolni és kezelni, mint magát az adatot tároló rendszert.

A mentések tárolása: az A és B osztályú rendszerek mentéseinek tárolása a főigazgató által kijelölt és jóváhagyott, védett helyiségben történik. A médiáról nyilvántartást kell vezetni.

A mentések adathordozóinak használatból való kivonása és megsemmisítése (pl. demagnetizálás) a szolgáltatást üzemeltető feladata. A média megsemmisítéséről jegyzőkönyvet kell felvenni.

17.8. Információcsere

Az intézmény A, B és C osztályú rendszerei esetében az automatikus adatcserét lehetővé tevő kapcsolatok létesítéséhez főigazgatói engedély és az érintett adatgazdák hozzájárulása szükséges. A kérelemben az alkalmazások üzemeltetőinek részletezniük kell az elérendő adatkezelési célt és az alkalmazott informatikai megoldást, különös tekintettel a jogosulatlan adatcserét kizáró biztonsági megoldásokra.

Az adatcsere környezetét, technológiai megvalósítását dokumentálnia kell az adatcserét kezdeményező alkalmazásüzemeltetőnek.

17.9. Elektronikus kereskedelem

A Kórház nem végez elektronikus kereskedelmi, vagy azzal kapcsolatos tevékenységet. Az elektronikus kereskedelmet lehetővé tévő alkalmazások esetében, a biztonsági feltételek megteremtése érdekében, a főigazgató engedélye lenne szükséges a rendszer működtetéséhez.

Az alkalmazás tervezésébe és megvalósításába be kell vonni a főigazgatót, vagy annak kijelölt képviselőjét.

17.10. Monitorozás

Az A és B osztályú rendszerek esetében az üzemeltetők felelőssége az automatikus szolgáltatásmonitorozó komponensek bevezetési lehetőségének vizsgálata és a monitorozás megvalósítása.

18. Hozzáférés szabályozás

18.1. Működési követelmények a hozzáférés szabályozása érdekében

Minden olyan informatikai rendszer esetében, ami a Kórház működéséhez szükséges, illetőleg bármilyen védett (kórházi, magán, kutatási, jogvédett... stb.) információt tartalmaz, meg kell határozni a hozzáférésre jogosultak körét és hozzáférési kísérlet esetén a jogosultságot ellenőrizni kell. Informatikai rendszerhez való, módosítást és védett adatok lekérdezését lehetővé tevő hozzáférésre kizárólag másik rendszer és természetes személy lehet jogosult. Természetes személyek egy csoportja (szervezeti egység munkavállalói stb.) közös használatú hozzáférési lehetőséget kizárólag publikus adatok lekérdezésére birtokolhatnak.

A jogosultságkezelésnek napra késznek kell lennie és dokumentálni kell.

18.2. Felhasználói hozzáférés menedzsmentje

Az adott informatikai rendszerhez történő hozzáférés módját (igénybe vételre jogosultak köre, igénylés módja, igénylés elbírálása) a rendszerben működő szolgáltatások SLA-i tartalmazzák. Az igénylés során a természetes személynek azonosítania kell magát egyedi adatával. Lehetőség szerint az informatikai rendszerek felhasználóinak azonosítása, jogosultság-elbírálása központilag, erre a célra szolgáló rendszerekkel történjen és a felhasználói adatbázis kezelése egységesen és konzisztensen valósuljon meg. Kivételt azon már meglévő és működő rendszerek képeznek, melyek nem képesek központi jogosultságkezelést megvalósítani.

A szolgáltatási SLA megszegése esetén a felhasználó az adott szolgáltatásból kizárható. Kizárás esetén a felhasználót ennek tényéről, a kizárás időtartamáról, a problémát okozó tevékenységről és a követendő magatartásról tájékoztatni kell. Ha a felhasználó tevékenysége által okozott kár csekély, akkor törekedni kell az előzetes figyelmeztetésre vagy a letiltás előtti tájékoztatásra.

Az A és B osztályú rendszerek esetében az üzemeltetési felelős a hozzáférésre jogosultak csctében is előírhat engedélyezési eljárást a hozzáférés megadásához. Az engedélyt írásban, a kért jogosultságokat feltüntetve kell a rendszergazdának eljuttatni. Minden A, B és C osztályú rendszer esetében az üzemeltetési felelős feladata, hogy a kiadott hozzáférések adatait (név, alkalmazás, jogosultsági szint, kiadás dátuma, indoka) naprakészen nyilvántartsa.

A hozzáférés indokának megszűnése esetén az üzemeltetési felelősnek a hozzáférést haladéktalanul vissza kell vonnia az SLA-ban dokumentált módon.

Az információs rendszerek illetéktelen elérésének megakadályozása érdekében megfelelő hozzáférési rendszert kell kialakítani. Hozzáférési jogosultság csak írásban igényelhető. Minden szerepkör feljogosít meghatározott fizikai, illetve logikai biztonsági tartományba (pl. szerverszoba, gépterem, archiváló helyiség, illetve adott alkalmazás, hálózati szegmens, munkahelyi állomás... stb.) történő belépésre és abban az engedélyezett fizikai, illetve logikai objektumokhoz való hozzáférésre az engedélyezett hozzáférési jogokkal.

Jelen Szabályzat kiterjed a felhasználói hozzáférés életciklusának minden egyes szakaszára, az új felhasználók kezdeti bejelentkezésétől az olyan felhasználók kijelentkezéséig, akik többé már nem igénylik (nem igényelhetik) az információs rendszerek és szolgáltatások elérését.

Hivatalos be- és kijelentkezési eljárást kell működtetni, amely alapján mindegyik több-felhasználós rendszerben és szolgáltatásnál szabályozni lehet a felhasználók hozzáférését. A felhasználói azonosítónak alkalmasnak kell lennie az informatikai rendszert használó identitásának egyedi, jellemző, ellenőrizhető hitelesítésre. A felhasználók közé sorolandók a természetes személyek, folyamatok, vagy egyéb eszközök egyaránt. Az egyedi felhasználói

azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni.

Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz és az adatokhoz való hozzáférést megfelelően szabályozza (korlátozza) és követhető, ugyanakkor a biztonsági funkciók működése során ellenőrizhető legyen a biztonsági rendszer által.

A felhasználó azonosítónak minden esetben egyedinek kell lennie, azaz semmilyen körülmények között sem adható ki különböző felhasználók részére ugyanazon azonosító.

A felhasználói azonosítók képzésére vonatkozó rendelkezéseket az Informatikai Osztály ügyrendje tartalmazza. A felhasználói azonosítók képzését a Kórházon belül egy helyen kell végrehajtani. A felhasználói azonosítók és jogosultságok rendszerében bekövetkezett mindennemű változást – az ellenőrizhetőség érdekében – naplózni kell.

Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.

A felhasználói azonosítók nem örök érvényűek. Ennek megfelelően a következő szabályokat kell alkalmazni:

- A Kórház munkavállalói, illetve külső személyek – amennyiben munkakörük, illetve beosztásuk alapján az informatikai rendszer szolgáltatásait igénybe vehetik –, munkába állásuk után haladéktalanul meg kell kapják felhasználói azonosítójukat. A szervezeti egység vezetőjének legalább 3 munkanappal a munkába lépés előtt meg kell igényelnie a felhasználói azonosítót a hozzáférési jogosultságok megjelölésével. Más azonosítója átmenetileg sem használható. A kapott felhasználói azonosítót haladéktalanul érvényesíteni kell.
- Külső személyek, akik valamilyen okból igénybe vehetik a Kórház bármelyik rendszerének szolgáltatásait, csak meghatározott időre, és korlátozott lehetőségeket biztosító (pl. egy adott projekt keretein belül érvényes) felhasználói azonosítót kaphatnak. A részükre kiadott azonosító szerkezetileg feleljen meg a szervezeten belüli munkavállalók azonosítójának, de legyen egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító külső személyé.
- Azokban a rendszerekben, amelyek regisztrálják a felhasználó utolsó bejelentkezésének időpontját, ha egy felhasználói azonosító 30 napot meghaladóan inaktívnak bizonyul (azaz a felhasználó a rendszer szolgáltatásait ez idő alatt egyszer sem vette igénybe), azonosítóját le kell tiltani és erről a munkavállaló munkahelyi vezetőjét értesíteni szükséges, megjelölve az érvénytelenítés okát.

A Jogi és Humánpolitikai Igazgatóság Humánpolitikai és Munkaügyi Osztály vezetőjének haladéktalanul kezdeményeznie kell a kilépő munkavállaló összes azonosítójának letiltását. Ennek megfelelően a kilépő dolgozók névsorát rendszeresen eljuttatja az Informatikai Osztály részére.

18.2.1. A jogosultságok kezelése

Standard jogosultságok:

- olvasási jog (betekintés),
- létrehozási jog,
- módosítási jog,
- törlési jog.

A hozzáférési jogosultság vezérlésére a szerepkör szerinti hozzáférés elvét kell alkalmazni, valamint a biztonsági adminisztrátori szerepkört elkülönítetten kell létrehozni.

A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultsági csoportokat kell kialakítani.

A Kórház informatikai rendszeréhez való hozzáférési jog megadása csak írásos kérelemre lehetséges. Az igénylések megőrzése és karbantartása az informatikai üzemeltetés feladata.

18.2.2. A felhasználói jelszavak kezelése

Az informatikai rendszerekben a felhasználók hitelesítésének alapvető módja a jelszó megadása.

A felhasználónak kötelezően nyilatkoznia kell arról, hogy felelősséget vállal személyes jelszavainak bizalmas kezeléséért.

A belépéskor kapott, illetve (pl. ha a felhasználó elfelejtette a jelszavát) az új jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes (pl. személyes) azonosítása után.

Az új jelszavak csak az adott munkanap végéig lehetnek érvényesek, megváltoztatásuk kötelező.

Telefonon történő kérésre jelszóváltoztatás nem kezdeményezhető.

A felhasználónak minden esetben vissza kell igazolnia új jelszavának átvételét ellenőrizhető úton (pl. e-mailben vagy személyesen).

A jelszónak minden felhasználó számára szabadon megváltoztathatónak kell lennie.

A felhasználói jelszavakkal kapcsolatban – amennyiben az adott rendszerben erre lehetőség van – biztosítani kell a következő követelmények teljesülését:

- a jelszó legalább 8 karakterből álljon,
- a jelszót a kisbetű (a-z), nagybetű (A-Z), szám (0-9) és jelek halmazából legalább két csoport felhasználásával kell képezni, a jelszó 12 hónapig és legalább 4 jelszóváltásig nem ismételhető,
- a jelszó maximális élettartama 3 hónap,
- a jelszó 10 sikertelen kísérlet után zárolásra kerül,
- a központi jelszó megadása utáni első bejelentkezéskor a kötelező jelszó cseréjét,
- a számítógépes rendszerekben a jelszavakat tilos nyílt formában tárolni. A jelszófájlokat megfelelő rejtjelezési védelemmel kell ellátni,
- a jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.

Automatikus bejelentkezési eljárások (pl. batch-fájlok, vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót. A felhasználói azonosítók és jelszavak nem tárolhatóak rejtjelezetlen formában. Felhasználói azonosítók, jelszavak, kriptográfiai kulcsok és az ehhez tartozó jelszavak nyomtatott formában, lezárt, lepecsételt borítékban, lemezszekrényben tárolhatóak. A lezárt borítékot a lezárónak alá kell írni, a lezárás dátumának feltüntetésével.

Biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága munkakörüknek megfelelő legyen.

Az Informatikai Osztály vezetője, az intézeti adatvédelmi felelős, a rendszergazdák - a Humánpolitikai és Munkaügyi Osztály és az alkalmazásgazdák bevonásával - a

jogosultságokat rendszeres időközönként ellenőrzi. Az általános felhasználók esetében ezt évente, míg a kiemelt jogosultsággal rendelkező felhasználók esetében legalább 3 havonta kell megtenni. Rendszeresen ellenőrizni kell azt is, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók, csoportok és eszközök rendelkezhessenek.

A munkakörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni, és az új munkakörnek megfelelően módosítani kell. A munkakörök változásáról a munkahelyi vezetők és a Humánpolitikai és Munkaügyi Osztály köteles értesíteni az Informatikai Osztályt.

18.2.3. A felhasználó feladatai

Meg kell akadályozni az illetéktelen felhasználói hozzáférést az informatikai rendszer erőforrásaihoz. A biztonság hatékonyságához nélkülözhetetlen az engedéllyel rendelkező felhasználók együttműködése.

A felhasználóknak tudomással kell bírniuk a hozzáférés hatékony ellenőrzésére alkalmas eszközök használatáról, különös tekintettel a jelszavak használatára és a felhasználó kezelésében lévő berendezések biztonságára.

A jelszavakat bizalmasan kell kezelni, azok más személyeknek nem adhatók meg, nyilvánosságra nem hozhatók.

A jelszavakat nem szabad papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a kezdeti jelszó), akkor gondoskodni kell a jelszó zárt borítékban történő, biztonságos tárolásáról. Ezektől eltérően a legmagasabb jogosultságot biztosító felhasználói azonosítók esetén a jelszavakat kötelező zárt borítékban, legalább zárható lemezszekrényben tárolni.

Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie.

A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat (pl. neveket, telefonszámokat, születési dátumokat), összefüggő szövegként ne legyen olvasható.

Legalább 3 havonta rendszeresen cserélni kell a rendszerben használt felhasználói jelszavakat, kerülve a korábban használt jelszavak ismételt vagy ciklikus használatát.

Első bejelentkezés alkalmával kötelező jelszócserét végrehajtani.

Amennyiben a munkaállomásokon a hitelesítési folyamatban a beírt jelszó olvasható (az alkalmazás nem rejti el megfelelően a jelszót), az alkalmazás üzemeltetőjének figyelmeztetése alapján, a felhasználó köteles gondoskodni arról, hogy más illetéktelen személy ne láthassa meg az általa beírt jelszót.

A biztonságos jelszóhasználat szabályait minden felhasználónak oktatni kell.

A felhasználó azonosítójával és jelszavával az informatikai rendszerben végrehajtott műveletekért személyesen felel.

A felhasználóknak gondoskodniuk kell a felügyelet nélkül hagyott eszközök megbízható védelméről. A felhasználó helyiségeiben felállított és a hosszabb időre felügyelet nélkül hagyott berendezéseknél – többek között munkaállomásoknál vagy szervereknél – külön védelemre lehet szükség az illetéktelen hozzáférés megakadályozására. Mindegyik felhasználónak és harmadik személynek meg kell ismernie a felügyelet nélkül hagyott berendezésekre vonatkozó biztonsági követelményeket és eljárásokat, valamint tájékoztatást kell kapniuk a védekezés megvalósítására vonatkozó felelősségükről.

Azokban a rendszerekben, ahol lehetőség van rá, biztosítani kell a hosszabb ideig inaktív munkaállomások rendszer által kikényszerített kijelentkezését, vagy a berendezés blokkolását (lock), például a PC-s munkaállomásoknál alkalmazni kell a jelszóval kombinált képernyővédő funkciót. (A munkaállomáshoz történő visszatéréskor a képernyővédő funkció feloldása csak sikeres jelszó megadás után legyen lehetséges.)

Megfelelő védelmi eszközzel, vagy beépített védelemmel nem rendelkező operációs rendszerek nem használhatók.

A napi munkavégzés befejezését követően a munkaállomások kikapcsolása kötelező.

18.3. Felhasználói felelősségek

A szolgáltatás felhasználója teljes felelősséggel tartozik az adott szolgáltatás SLA-jában általa vállalt kötelezettségek betartásáért, beleértve a korlátos erőforrások pazarlása miatt az üzemeltetőnél keletkező többletköltségeket is.

Az A osztályú rendszerek felhasználója munkaköri felelősség keretében kezelheti az intézményi adatokat, azok bizalmas kezelése munkaköri kötelessége. Az intézményi rendszert köteles csak a munkakörének megfelelően, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használni.

A Kórház informatikai eszközei alapvetően csak a Kórház küldetésének teljesítése, valamint a munkahelyi vezető jóváhagyásával végzett tudományos kutatás, illetve e célból történő kapcsolattartás céljára használhatók. Minden egyéb tevékenység személyes használatnak tekintendő.

Eszközök kezelése, használata

(1) Az eszközök kezelése, használata során minden felhasználónak gondosan be kell tartani az alábbiakat:

a) Minden olyan előírást, mely az eszközök kezelési útmutatójában szerepel.

b) Ha egy eszközre nincs ilyen, akkor az intézmény által kiadott kezelési útmutatóban leírtakat.

c) Minden eszközt csak a kezelési útmutatóban leírtak szerint lehet használni.

d) A szoftverek, dokumentumok használata, létrehozása során a szerzői jogokra vonatkozó jogszabályokat.

e) A munka és tűzvédelmi előírásokat, szabályokat.

f) Tilos az eszközök közelében enni, inni, dohányozni.

g) Tilos az eszközöket és azok részeit áthelyezni, burkolatukat, csatlakozásaikat megbontani.

h) Tilos a számítógépekre szoftvert telepíteni, illetve engedély nélkül letörölni.

i) A felhasználók kötelesek minden meghibásodást jelenteni. A hibabejelentés, jellegéből adódóan a Hibajelentő űrlapon, vagy telefonon, vagy elektronikus úton történik.

j) A felhasználóknak tilos az eszközök elektromos csatlakozásait megbontani. Elektromos meghibásodás, pl. zárlat gyanúja esetén az eszközt áramtalanítani kell. Ha a meghibásodás a rendelő elektromos hálózatában keletkezik, úgy az egész rendelőt áramtalanítani kell a főkapcsolóval.

(2) Az eszközök használatát az arra kijelölt személy (rendszergazda) ismerteti. Az ő feladata az eszközök kezelésének bemutatása, az ahhoz kapcsolódó speciális tudnivalók ismertetése is. Mindenki csak azokat az eszközöket használhatja, melyekre engedélyt kapott, és kezelésükre ki lett oktatva. A használható eszközök körének meghatározása a felhasználói jogosultság kiadásával párhuzamosan történik.

(3) A felhasználók jogosultak a nyomtatókba papírt tölteni. Nyomtatóhiba esetén az Informatikai Osztály jogosult engedélyezni a felhasználónak a hiba elhárítását.

(4) Az Informatikai Osztály köteles folyamatosan megfigyelni a rendszert, és az illegális használat felmerülése esetén köteles a helyzetet kivizsgálni, és az esetet jelenteni az ügyvezetésnek és az illetékes munkahelyi vezetőnek. Amennyiben az illegális használat bebizonyosodik, a felhasználó köteles az okozott kárt és költséget megtéríteni.

(5) Minden esetben, amikor a hibaelhárítást az Informatikai Osztály felügyeletével a felhasználó végzi, a teljes felelősséget az Informatikai Osztály viseli. A felhasználó köteles együttműködni az Informatikai Osztállyal a hiba elhárításában.

(6) A hordozható (notesz) gépek esetén

a) a biztonsági beállításokat csak az Informatikai Osztály változtathatja.

b) amennyiben egy hordozható gép hosszabb ideig nem volt a Kórház hálózatára csatlakoztatva, a felhasználó köteles a csatlakoztatás előtt az Informatikai Osztály részére biztonsági ellenőrzés céljából átadni.

c) a hordozható gépek szoftverbiztonságáért az Informatikai Osztály felelős. A felhasználó számára a biztonsági beállítások megváltoztatása tilos.

d) a hordozható gépeket kétszintű jelszóval kell védeni (bekapcsolási jelszó és az operációs rendszer jelszava).

e) tilos a hordozható gépeken olyan adatok tárolása, mely az információs önrendelkezési jogról és az információ szabadságról szóló törvény alapján személyes adatnak vagy különleges adatnak minősül.

18.3.1. Személyes használat

A felhasználók jogosultak személyes célokra is használni az informatikai eszközöket, ugyanakkor a személyes célból történő használat semmilyen módon nem zavarhatja a Kórház küldetésének teljesülését. A személyes használat során kifejezetten tilos jogsértő tevékenységet folytatni. A személyes használat engedélyezése vagy korlátozása az érintett szervezeti egység vezetőjének hatáskörébe tartozik. Az Informatikai Osztály és a szervezeti egység vezetői kötelesek együttműködni a túlzott, illetéktelen vagy jogsértő használat (a továbbiakban: illegális használat) felderítésében és esetleges korlátozásában.

18.3.2. Eszközök mozgatása és az eszközök összekötése

Az eszközök megbontását csak az Informatikai Osztály végezheti.

Az eszközök mozgatása és az eszközök összeköttetésének megváltoztatása kizárólag az Informatikai Osztály feladata. E szabály alól kivétel a 24 órában üzemelő területeken hiba esetén üzembe helyezett tartalék eszköz mozgatása és összekötése. Az eszközök mozgatását, illetve az eszközök összeköttetésének megváltoztatását indokolt esetben – az Informatikai Osztály engedélyével és felelősségével – a felhasználó is végezheti.

Kivételek:

A eszközök mozgatásának és az összeköttetés megváltoztatásának tilalma nem vonatkozik

(1) a kifejezetten hordozható eszközökre, mint pl. a noteszgépek vagy a műtéti monitorok.

(2) a 24 órában üzemelő területeken hiba esetén üzembe helyezett tartalék eszköz mozgatására és összekötésére. Ez esetben az Informatikai Osztályt a következő munkanapon értesíteni kell a cseréről.

(3) a kórház telephelyein található rendelőkben elhelyezett tartalékeszközök hiba esetén történő üzembe helyezésére. A cserét az Informatikai Osztály előzetes engedélyével lehet végrehajtani.

(4) a magánhasználatú, illetve magántulajdonú eszközökre.

18.3.4. Szoftver

A szoftver telepítése az Informatikai Osztály felelőssége.

A felhasználók számára tilos mindenfélc szoftver telepítése. Véletlen szoftvertelepítés esetén a felhasználó köteles az Informatikai Osztályt haladéktalanul értesíteni.

A munkaállomások automatikus, illetve központi szoftvertelepítési beállítását megváltoztatni, vagy az ilyen szoftvertelepítést akadályozni tilos.

18.3.5. Adathordozók

A felhasználók jogosultak külső adattárolók (pendrive, külső merevlemez, floppy) használatára. Külső adattároló(k) használata esetén a felhasználó teljes és korlátlan felelősséggel tartozik a külső adattárolón tárolt adatok védelméért, illetve a vírusmentességért.

18.3.6. A 24 órában működő területek

A Kórház a 24 órában üzemelő területeken tartalék eszközökkel biztosítja a folyamatos üzemmenetet. A csereeszközzel ellátott, 24 órában működő területek – a fentiekkel összhangban – kifejezetten felhatalmazást kapnak a meghibásodott eszközök cseréjére. A cserét jelenteni kell az Informatikai Osztálynál. A meghibásodott eszközök javításáról, illetve cseréjéről az Informatikai Osztály köteles haladéktalanul gondoskodni.

18.4. Hálózati hozzáférés

A számítógépes hálózatra történő fizikai csatlakozás csak az üzemeltető által elfogadott igénylés után, az abban megadott paraméterekkel lehetséges. A jogosulatlan csatlakozást az üzemeltető a rendszer integritásának védelmében azonnal megszüntetheti. A csatlakozási lehetőségeket és az igénylés módját a hálózati szolgáltatások SLA-i tartalmazzák.

A hálózati szolgáltatások SLA-iban szereplő feltételrendszer az üzembiztonság, nyomon követhetőség és központi kezelhetőség szempontjai szerint van kialakítva, ezért az SLA be nem tartása a rendszer egészét, a többi felhasználó szolgáltatási környezetét veszélyezteti. Emiatt az SLA-t megszegő felhasználó a hálózati szolgáltatásokból utólagos figyelmeztetés mellett is kizárható.

A Kórház hálózatára kizárólag annak eszközei csatlakoztathatóak. E témakörbe beleértendők a saját tulajdonú noteszgépek, intelligens telefonok, kézi számítógépek (PDA-k)... stb. is.

Nem a Kórház tulajdonában lévő eszköz hálózatra csatlakoztatása kizárólag az Informatikai Osztály vezetőjének írásos engedélyével történhet. Az informatikai vezető az engedély kiadása előtt köteles meggyőződni arról, hogy az adott eszköz semmilyen módon nem fogja veszélyeztetni a Kórház informatikai rendszerét.

Az internet bármely komponenséhez történő hozzáférés esetén a felhasználó köteles a Kórház internetszolgáltatójának szabályzatát is betartani, valamint az internetközösség etikai irányelveit, mások vallási, politikai és erkölcsi nézeteit tiszteletben tartani.

18.5. Az internet használata

Az internetkapcsolat célja az elektronikus levelezés lebonyolítása, az interneten fellelhető információ elérhetővé tétele, valamint a Kórház weboldalain az intézménnyel kapcsolatos információk közzététele. Megengedett a hálózatnak a Kórház alaptevékenységéhez kapcsolódó adminisztratív és információs feladatokkal összefüggő célokra történő használata. Korlátozott mértékben megengedett a hálózat magáncélra (pl. magánjellegű levelezés) történő felhasználása, ha ez nem jelent üzleti célú felhasználást és az internet használatát nem veszélyezteti vagy akadályozza. A Kórház internethálózata ezen belül minden olyan tevékenységre használható, amely az alábbiakban tételesen nincs megtiltva.

A felhasználóknak tisztában kell lennie, hogy az informatikai eszközök, az internet, illetve a Kórház elektronikus levelezési rendszerének helytelen használata közvetlen hatással lehet a Kórházra és munkavállalóira.

Minden felhasználó saját maga felel a bejelentkezési kódjával kezdeményezett adatforgalomért, függetlenül attól, hogy ki használta az adott gépet.

Tételesen tiltott tevékenységek az internethálózaton:

- a hatályos magyar törvényekbe ütköző cselekmények, ideértve a következőket, de nem korlátozva ezekre: betegadatok külvilág felé továbbítása, a szerzői jogok megsértése; szoftver illetve egyéb szerzői jogi védelem alá tartozó alkotás szándékos és tudatos, illegális terjesztése.
- jogosulatlanul megszerzett, illetve szerzői jogokat sértő adatoknak, anyagoknak a Kórház számítógépein történő tárolása, a Kórház hálózatán való továbbítása.
- a hálózaton terjesztett anyagok nem lehetnek ellentétesek a Kórház szellemiségével, nem lehetnek szexuális, erőszakos, vagy trágár tartalmúak, nem kelthetnek megbotránkozást, faji, vallási vagy politikai ellentéteket nem szíthatnak, törvényellenes cselekmény elkövetésére senkit nem bátoríthatnak, bárkinek a magánéletét vagy nyugalmát indokolatlanul nem zavarhatják, és nem lehetnek becsmérlőek vagy megalázóak.
- forgalom szempontjából tilos bárminemű olyan szoftver használata, amely az adott asztali számítógépet szerverként használja, és ezáltal tartalmat szolgáltat a külvilág felé (különböző filecserélő rendszerek használata, torrentek seed-elése, DC++ szerverek fenntartása vagy használata... stb.) Szigorúan tilos publikus FTP szerver üzemeltetése.
- spam (kéretlen reklám-anyagok) küldése szigorúan tilos.

Tilos továbbá:

- profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
- a hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység,
- a hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység (pl. levélbombák, elektronikus játékok, zenefájlok, mozgóképek letöltése),
- a hálózat biztonságát veszélyeztető információk, programok terjesztése,
- a hálózati erőforrások magáncélra való túlzott mértékű használata.

18.5.1. A használat korlátozása

Az Informatikai Osztály köteles folyamatosan megfigyelni az internet használatát, és az illegális használat felmerülése esetén köteles a helyzetet kivizsgálni, és az esetet jelenteni a főigazgatónak, valamint az illetékes szervezeti egység vezetőjének. Amennyiben az illegális használat bebizonyosodik, a felhasználó köteles az okozott kárt és költséget megtéríteni.

Az Informatikai Osztály a forgalmi statisztikák, illetve a tartalom alapján javaslatot tehet bizonyos weboldalak hozzáférésének korlátozására, amennyiben az adott oldal látogatása a Kórház számára működési problémát jelenthet. A hozzáférés általános korlátozásának elrendelése a főigazgató hatásköre.

Az általános hozzáférési korlátozás, illetve a II. pontban megfogalmazott tilalmak alól felmentést a főigazgató adhat.

18.5.2. A felhasználók kötelessége

Az interneten elérhető szolgáltatások (publikus e-mail szolgáltatások, chat roomok, newsgroup-ok, fórumok, üzenet falak, vásárlások... stb.), a Kórház által biztosított levelezési cím használata csak akkor engedélyezett, amikor a tevékenység kifejezetten a Kórház nevében és érdekében történik. A Kórház által biztosított levelezési címet magán célú tevékenységek esetében kerülni kell. Amennyiben ezen e-mail cím kerül használatra, minden esetben jelezni kell, hogy ez saját vélemény, független a Kórháztól.

A Kórház nevében és érdekében, illetve bármilyen kórházi tevékenységgel összefüggésben kizárólag a Kórház által biztosított levelezési cím (...@kenezykorhaz.hu) használata megengedett, magán elektronikus levelezési cím használata tilos. Nem megengedett továbbá magán célú levelezésekben a Kórházban használatos hivatalos és a Kórházra utaló hivatalos elemek használata.

18.5.3. Az internet használati szabályok megsértésének szankcionálása

A használati szabályok szándékos és durva megsértésének szankcionálása az internet hálózati szolgáltatásokból való ideiglenes vagy végleges kizárás. Ha a használati szabályok megsértése kismértékű, vagy nem tekinthető szándékosnak, akkor az elkövetőt figyelmeztetni és a Szabályzatról tájékoztatni kell. A figyelmeztetés utáni ismételt elkövetést szándékosnak kell tekinteni. Szükség esetén a Kórház jogi felelősségre vonást kezdeményez.

A Szabályzatban foglaltak megszegése az adott számítógép/személy kombináció internet-elérésének tiltását eredményezi.

18.6. Operációs rendszer hozzáférés

Az SLA köteles operációs rendszerekben a felhasználók kizárólag egyértelmű azonosítás után végezhetnek munkát. A hozzáférés tényét, időtartamát és forrását a rendszernek visszakereshető módon naplóznia kell az SLA-ban meghatározottak szerint, illetve minimum 1 hónapig.

18.7. Alkalmazásokhoz és információkhoz való hozzáférés szabályozása

Az intézményi adatokhoz való hozzáférést lehetővé tevő alkalmazások jogosultsági köreit olyan módon kell kialakítani, hogy a munkavállalók csak a munkakörükkel kapcsolatos adatokat láthassák, illetve kezelhessék. Az intézményi adatokhoz történő hozzáférést, ezen adatok módosítását alkalmazás szinten is – visszakereshető módon – naplózni kell minimum 1 hónapra visszamenőleg.

Minden A és C osztályú rendszer esetén a személyes adatokat kizárólag az adatot birtokló természetes személy, mint felhasználó láthatja. Ez alól csak a rendszer üzemeltetését ellátó és a mentéseket készítő üzemeltetői azonosítók jelentenek kivételt. A felhasználónak ezen adatok publikálásához tevőlegesen meg kell változtatnia a publikálandó adatok jogosultságát.

18.8. Mobil számítógép használat és telefonos munkavégzés

Az A osztályú rendszerekhez történő tetszőleges, illetőleg a B osztályú rendszerekhez történő menedzsment hozzáférés kizárólag az intézményi belső hálózatból (intranet) lehetséges. A C osztályú rendszerek menedzsment hozzáférése megfelelő titkosítással bíró adatkapcsolattal külső hálózatból is megengedett. Minden egyéb hozzáférési kísérlet incidensnek minősül és informatikai megoldásokkal is akadályozható az üzemeltetők részéről.

Speciális hálózati szolgáltatásokkal (pl. VPN) az intranet az intézmény fizikai hálózatán kívülre is meghosszabbítható, ezáltal a munkahelyen kívüli munkavégzés lehetséges. Ezen megoldások (a hálózati SLA megsértésével járó) önerős megvalósítása nem megengedett, kizárólag a Kórház ilyen tartalmú szolgáltatásai vehetőek igénybe. Az intranet védelmi szintjének megsértése a hálózati hozzáférés nem megfelelő használatával (pl. saját átjáró, külső hálózati kapcsolat… stb.), felhasználó általi létesítésével súlyos SLA sértésnek minősül.

Hordozható informatikai eszközön értünk minden olyan informatikai eszközt, melyet

- célja, mérete, súlya… stb. alapján eleve helyhez nem kötött működésűnek terveztek, és
- olyan operációs rendszerrel rendelkezik, amelyik alkalmas több – azonos típusú – fájl kezelésére, és
- rendelkezik, vagy bővíthető olyan programokkal, melyek lehetővé teszik a file-ok megtekintését és manipulálását.

Ilyenek különösen a noteszgépek (notebook, laptop), intelligens telefonok és a kézi számítógépek (PDA, PIM, Palmtop), de nem tartoznak ide a csak adattárolásra szolgáló eszközök, mint a pendrive-ok vagy a külső merevlemezek. Az eszközöket fokozott gondossággal kell kezelni. E tekintetben tilos:

- nyilvános vagy idegenek által könnyen elérhető helyen őrizetlenül hagyni őket (pl. rendelő, iroda, nyilvános helyek… stb.).
- gépkocsiban látható helyen hagyni.
- a használati utasításban meghatározott káros hatásoknak kitenni.

A hordozható eszközök nem a Kórház tulajdonában lévő eszközökhöz is csatlakoztathatóak (pl. otthoni nyomtató), de ez esetben a szakszerűtlen használatból eredő károkért a felhasználó felelős.

Idegen hálózatra csatlakozás előtt a felhasználó köteles meggyőződni arról, hogy az illető hálózat kellően védett-e, és nem áll fenn informatikai támadás (vírus, hacker... stb.) veszélye.

A merevlemezzel rendelkező eszközök mozgatását lehetőség szerint kikapcsolt vagy hibernált állapotban szabad végezni (amikor a merevlemez már megállt).

Nem a Kórház tulajdonában álló hordozható eszközzel csak az Informatikai Osztály vezetőjének írásos engedélyével szabad a Kórház hálózatára csatlakozni. Az Informatikai Osztály vezetője az engedély kiadása előtt köteles meggyőződni arról, hogy az eszköz semmilyen kockázatot nem jelent a Kórház informatikai rendszere számára. A már kiadott engedéllyel rendelkező, nem a Kórház tulajdonában álló gépek esetén az Informatikai Osztály vezetője jogosult és köteles a megítélése szerint szükséges szoftverek használatát elrendelni, illetve a kockázatosnak minősített szoftverek használatát megtiltani.

Ha az Informatikai Osztály illetéktelen behatolást (csatlakozást) észlel, köteles mielőbb megakadályozni a behatolást, és az esetet jelenteni a vezetőségnek.

19. Információs rendszerek beszerzése, fejlesztése és karbantartása

19.1. Információs rendszerek biztonsági követelményei

Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni, és a szolgáltatás indítási kérelemhez mellékelni kell.

A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatóak olyan irányba, hogy a rendszer biztonsági szintje csökkenjen.

19.2. Alkalmazások helyes használata

Az A osztályú alkalmazásokhoz kizárólag azon felhasználók férhetnek hozzá, akiknek az intézményi szerepük ezt megkívánja, és legfeljebb olyan jogosultsággal rendelkeznek, amit a munkakörük maradéktalan ellátása megkíván. Nevesítve:

- a rendszer üzemeltetői (üzemeltetői jogosultsággal),
- a rendszer felhasználói (a munkakörükhöz, szerepükhöz szükséges lekérdező és módosító jogosultságokkal).

A rendszer fejlesztői a szolgáltató alkalmazáson nem rendelkezhetnek üzemeltetői jogosultságokkal, mivel ez az ő munkakörük ellátáshoz nem szükséges (éles üzemű szolgáltató rendszerben fejlesztés nem történhet).

19.3. Kriptográfiai szabályozások

Az A és B osztályú rendszerekbe történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (pl. SSH, SSL, VPN) engedélyezett, kivéve azon bejelentkezési területeket, ahol a felhasználó munkahelye és a szolgáltató rendszer közötti csatorna külső fél általi lehallgatása technikailag nem lehetséges (pl. fizikai védelem miatt).

A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.

Egyéb kriptográfiai szabályozások az adott szolgáltatás SLA-jában találhatóak.

19.4. Rendszer fájlok biztonsága

A szolgáltató rendszerek működését biztosító rendszer fájlokhoz a felhasználók csak olyan mértékben férhetnek hozzá, amit a szolgáltatás használata megkövetel. A szolgáltatás szempontjából kritikus rendszer fájlok felhasználók általi módosítása csak az üzembiztonságot ellenőrző köztes felületen keresztül lehetséges.

A rendszer fájlok védelme, az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosítása az üzemeltető rendszergazdák munkaköri kötelessége.

20. Fejlesztési és támogatási folyamatok biztonsága

Minden alkalmazás fejlesztési tevékenységét a szolgáltató alkalmazás-példányától és annak adatbázisától elkülönülten kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is C osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatóak ki.

Intézményi fejlesztésű, vagy vásárolt szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek az SLA-ban rögzített minden paraméterre és funkcióra, valamint a tipikus felhasználási mintákra kell kiterjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.

Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás-verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.

Szolgáltató üzemben működő alkalmazáson csak sikeres tesztelési jegyzőkönyv birtokában és az üzemeltető üzemeltetési felelős engedélyével végezhető változtatás (külső munkavégző cég esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt, amely esetében a dokumentálást utólag kell elvégezni.

20.1.Műszaki sérülékenység menedzsment

Az adott alkalmazás üzemeltetőjének felelőssége a publikált technikai sérülékenységek elleni védekezés megvalósítása. A publikált sérülékenységek elleni védekező intézkedés (pl. patch-ek és fixek letöltése) az észlelést követő első munkanapon végrehajtandó.

21. Információbiztonsági események menedzsmentje

21.1. Biztonsági események és gyengeségek jelentése

Minden szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználóknak, és a bejelentés módját az SLA-ban közzétenni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatoknak a védelmében kötelesek lehetőség szerint rövid reakcióidővel elbírálni és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. A üzemeltetési felelős köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről.

Biztonsági esemény, vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amelyek az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, log file részlet... stb.)

A szolgáltatások felhasználása közben tapasztalt biztonsági gyengeségek jelentése – a rendszer működőképességének fenntarthatósága érdekében – minden felhasználónak kötelessége. Ennek elmulasztása, vagy a gyengeség kihasználása biztonsági eseménynek minősül.

21.2. Információbiztonsági események és fejlesztések menedzsmentje

Az informatikai szolgáltató rendszerek esetében egyenszilárdságú biztonsági megoldásokat kell kialakítani. Rendszerenként egységes tervezés és megvalósítás alapján kell a biztonsági megoldásokat kezelni. Amennyiben egy informatikai rendszer egy másik szolgáltatását igénybe veszi, akkor a szolgáltatási SLA biztonsági követelményei az igénybevevő rendszer egészére vonatkoznak.

A megvalósítandó, vagy üzemben álló szolgáltató rendszer rendszertervének az alkalmazott és a felhasználók számára előírt biztonsági megoldásokat is tartalmaznia kell. Amennyiben ezek a változó követelmények miatt nem bizonyulnak elegendőnek, a rendszer fejlesztési tervében szerepeltetni kell az új biztonsági rendszer tervezett megoldásait.

22. Működés-folytonosság biztosítása

22.1. A működés-folytonosság információbiztonsági vetülete

Az intézmény működése szempontjából kritikus, A és B osztályú rendszerek működés-folytonosságának biztosítása az üzemeltető és az üzemeltetési felelős feladata. Ez kiterjed az SLA-k feltételrendszerének körültekintő meghatározására, a felelős incidenskezelésre, a szükséges funkcionális és biztonsági javítások telepítésére, a Szabályzat betartására, valamint a rendszer fejlesztési tervcinek erőforrás-kalkuláción alapuló körültekintő elkészítésére.

A működésfolytonosság biztosításának részleteit az e témakörben irányadó szabályok részletezik.

23. Megfelelőség

23.1. Jogszabályi megfelelőség

A főigazgató felel a nyújtott szolgáltatások jogszabálynak történő megfeleléséért.

A főigazgató értelemszerűen nem felel a felhasználók által elkövetett jogsértésekért (pl. jogosulatlan adatkezelés, szerzői jogokkal való visszaélés... stb.), és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban kiadhatja.

Az információbiztonság témakörében érvényes legfontosabb jogszabályok jegyzékét az 1. sz. melléklet tartalmazza.

23.2. Megfelelés biztonsági politikának, szabványoknak és műszaki előírásoknak

A főigazgató felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.

Az információbiztonság témakörében érvényes legfontosabb szabványoknak és műszaki leírásoknak a jegyzékét az 1. sz. melléklet tartalmazza.

23.3. Információs rendszerek felülvizsgálatával kapcsolatos megfontolások

A Szabályzattal összhangban a főigazgató felelős azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább

évente megtörténjen, és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra az A osztályú rendszerek esetében.

Súlyos SLA sértés esetén a főigazgató külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.

A felülvizsgálatok eredményei alapján a főigazgató rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön.

A munkafolyamatba épített ellenőrzés során a Szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

24. Záró rendelkezések

A Szabályzat 2014. október 1. napján lép hatályba.

A Szabályzatban érintett munkavállalók munkaköri leírásába be kell építeni a Szabályzatban előírt feladatokat.

Debrecen, 2014. október 1.

Kenézy Gyula Kórház és Rendelőintézet
4031 Debrecen, Bartók Béla út 2-26.

Dr. Lampé Zsolt Tibor
főigazgató

25. Mellékletek

1. sz. melléklet

A LEGFONTOSABB INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS JOGSZABÁLYOK, SZABVÁNYOK, ELŐÍRÁSOK, AJÁNLÁSOK

Az alábbi lista értelemszerűen nem teljes körű, de tartalmazza a napi működéssel kapcsolatos leginkább releváns jogszabályokat, szabványokat, előírásokat és ajánlásokat:

Jogszabályok

- 2011. évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról
- 2012. évi I. tv. a Munka Törvénykönyvéről
- 1978. évi IV. tv. a Büntető Törvénykönyvről
- 2009. évi CLV. tv. a minősített adat védelméről
- 1996. évi LVII. tv a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
- 1995. évi LXVI. tv. a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
- 1999. évi LXXVI. tv. a szerzői jogról
- 2001. évi XXXV. tv. az elektronikus aláírásról

Biztonságtechnikai, tűzvédelemi szabványok, előírások

- MSZ 595/1-9 Építmények tűzvédelme.
- MSZ EN 3/1-5 Tűzoltó készülékek.
- MSZ 9785/1-2 Tűzjelző berendezés.
- MSZ IEC 839-1 Riasztórendszerek.
- MSZ 274 Villámvédelem.
- MSZ EN 60950 Adatfeldolgozó berendezések és irodagépek biztonsági előírásai.

Egyéb szabványok, ajánlások

- MSZ EN 60950 Adatfeldolgozó berendezések és irodagépek biztonsági előírásai.
- A MeH ITB 12. ajánlása az informatikai rendszerek fizikai, logikai és adminisztratív védelmi követelményeiről és az ezek alapján foganatosítandó védelmi intézkedésekről
- ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az informatikai rendszerek biztonságának funkcionális és minősítési követelményeire
- TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), az Egyesült Államok Védelmi Minisztériuma által kiadott információ biztonsági ajánlás
- MeH ITB 8. ajánlásán alapuló kockázatkezelési módszertan
- TCSEC = Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), az Egyesült Államok Védelmi Minisztériuma által kiadott információ biztonsági ajánlás
- ISO/OSI 7498-2 szabvány a nyílt rendszerek biztonsági architektúrájára vonatkozik. Magyar megfelelője: MSZ OSI 7498-1

2. sz. melléklet

INFORMÁCIÓBIZTONSÁGI POLITIKA

A Kenézy Gyula Kórház és Rendelőintézet információbiztonsági stratégiáját meghatározza, hogy tevékenységünkből adódóan nagy mennyiségű ügyfél adatot kezelünk. Ezek

- személyes adatokat tartalmaznak, melyre jogszabályi előírások vonatkoznak,
- együttesen nagyobb értéket és kockázatot képviselnek, mint az egyedi adatok összesen,
- sértetlenségük és bizalmasságuk befolyásolják ügyfeleinknek saját vevőik felé történő teljesítését, megbízhatóságát.

Ennek megfelelően tevékenységünk biztonsága igen erős vevői elvárás. Információbiztonsági stratégiánkban elsődleges szempont ügyfeleink adatainak védelme a bizalmasság és a sértetlenség szempontjából.

Cégünk működésével kapcsolatos szakmai elvárások nagyfokú rugalmasságot követelnek a support tevékenység, illetve saját belső működésünket illetően. Ezeken a területen az információk rendelkezésre állását tekintjük alapvető szempontnak. Ennek érdekében szervezetünkön belül nyitottságot biztosítunk, munkatársaink részére elérhetővé tesszük a munkájukhoz szükséges információkat. Ez a bizalmi alapon való működési mód másrészt azt igényli, hogy az információbiztonsági elveket tudatosítsuk és azokat minden munkatársunk kötelező érvénnyel betartsa. Különös hangsúlyt fektetünk dolgozóink képzésére, valamint az új munkatársak bevezetésére a napi és az ügyfelekkel való munkába fokozott ellenőrzés, felügyelet mellett.

A jól működő, MSZ ISO/IEC 27001:2006 információbiztonsági szabvány követelményeinek is megfelelő rendszer érdekében:

- Olyan összetett védelmi rendszert alakítunk ki, mely segítségével kellő biztonsággal, ugyanakkor rugalmassággal tudjuk kezelni a ránk bízott, és saját információkat. A védelmi rendszer mind technikai szintű, mind szabályozás szintű elemeket tartalmaz.
- Figyelemmel kísérjük a jogszabályi környezet változásait, hogy mindenkor megfeleljünk ezen előírásoknak.
- Figyelemmel kísérjük a technikai fejlődésből adódó lehetséges újabb kockázatokat, és védelmi rendszereket.
- Rendszerünket ezeknek megfelelően folyamatosan felügyeljük, értékeljük, és fejlesztjük.
- Minden munkatársunkban tudatosítjuk az információbiztonság fontosságát, a lehetséges kockázatokat, és a védelmi intézkedéseket.

Debrecen, 2013. április 1.

Dr. Lampé Zsolt Tibor
főigazgató