MARGIT KÓRHÁZ
9300 Csorna, Soproni u.64. GH-1/2010

Szabályzat az informatikai üzletmenet-folytonosságának biztosításáról és a katasztrófavédelemi és elhárítási szabályozásáról

Érvényes: 2010. augusztus 1-től-.visszavonásig

Készítette: .....

Ellenjegyezte: MARGIT KÓRHÁZ igazgató főorvos CSORNA

Dr.Boga Attila
Mb. igazgató főorvos

1. Általános rendelkezések

1.1. A szabályozás célja

Az informatikai üzletmenet-folytonosság célja az informatikai rendszer komponenseinek megbízható üzemelését és a rendszeren belüli lehető leggyorsabb hibaelhárítása annak érdekében, hogy minden biztonsági komponensből, vészhelyzetből adódó teljes vagy részleges üzletmenet veszélyeztetettség ne okozzon a kórház működésében nagymértékű korlátozást, estelegesen teljes kiesést. Ennek előfeltétele, hogy a megengedett tűrési időn belül az előzetes vagy azonnali intézkedések hatására a teljes informatikai rendszer vagy annak komponensei, visszanyerjék az alapfeladatuk ellátásához szükséges funkcionalitást.

1.2. A szabályozás hatóköre

Az informatikai üzletmenet-folytonosság kiterjed a számítástechnikai eszközökre, az informatikai rendszer részeire és az azokhoz tartozó környezeti infrastruktúrára, a hardverre, az adathordozókra, a dokumentumokra, a szoftverekre, az adatokra, az elektronikus kommunikációra és a felhasználókra.

1.3. A szabályozás tartalma

A szabályzat olyan előírások és szabványok betartását, betartatását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

1.4. A személyi felelősség

Az informatikai rendszer biztonságának megőrzése minden felhasználónak a feladata. Az informatikai rendszer minden fontos alkalmazásához, eleméhez személyi felelőst (továbbiakban rendszergazda) kell kijelölni. Azon alkalmazásokhoz, melyek kezelője nem informatikus, az informatikusok közül is ki kell jelölni egy rendszergazdát.

2. Megelőző intézkedések, tevékenységek

Az informatikai rendszer biztonságos üzemeltetése érdekében megelőző intézkedéseket kell tenni, melyek segítségével megelőzhetőek vagy jelentős mértékben csökkenthetőek a rendszerben a nem tervezett kiesések.
Ezek az intézkedések az alábbiak:

- a rendszer naplózásra képes elemeinek folyamatos figyelemmel kísérése, a naplófájlok folyamatos elemzése, kiértékelése és a szükséges szakmai intézkedések megtétele;
- a rendszernaplózás számára elengedhetetlenül fontos rendszeridő és dátum beállítása. Azokon az eszközökön, amelyeken lehetséges (szerverek és ezek alapján a munkaállomások) automatikus frissítési szolgáltatásaként kell a rendszeridőt és dátumot beállítani, de mindenképpen naponta egyszer ellenőrizni kell ezek helyes működését.
- a rendszer kapacitásának, teljesítményének folyamatos ellenőrzése, majd igény esetén a szükséges utasítások, intézkedések megtétele;
- a rendszer működéséhez szükséges megelőző karbantartási munkák elvégzése;
- hibák vagy zavaró események észlelése esetén a rendszergazdának jelenteni kell ezt telefonon, személyesen vagy e-mailben, aki majd megteszi a szükséges intézkedéseket a megfelelő és szakszerű hibaelhárítás érdekében;
- a kórháznál alkalmazott kacsolódó szabályok és utasítások folyamatos betartatása és ezek ellenőrzése beleértve az egyes összetevők felhasználói és üzemeltetési dokumentációit;
- az informatikai rendszer elemeinek állapotát, életkorát folyamatosan figyelni kell és az előírások és a lehetőségek függvényében folyamatosan fejleszteni kell a rendszert a hatékonyság növelése érdekében az informatikai stratégia figyelembe vételével;
- a rendszer működésével kapcsolatos környezeti tényezők (pl. hőmérséklet, elektromos hálózat, levegőtisztaság, stb.) folyamatos figyelemmel kísérése és szükség esetén a megfelelő beavatkozás megtétele;
- az üzletmenet-folytonosság szempontjából az egyes kockázati tényezők figyelembe vételével megelőző, helyreállítási megoldásokat, elemzéseket

kell készíteni. Fel kell becsülni a lehetséges károkozás mértékét és a megelőzéshez szükséges és a védelmi intézkedések betartása miatt szükséges költségeket, majd szükség esetén el kell kezdeni a konkrét intézkedési feladatok kidolgozását;

- a felhasználókat a képzési tervnek megfelelően oktatásban kell részesíteni. A rendszergazdának rendszeresen informatikai biztonsági oktatást kell tartani.

A megelőző tevékenységgel kapcsolatban nagyon fontos tényező az előírt időszakos tevékenységek pontos betartása, illetve valamely nem várt esemény(ek), kockázati tényező(k) mielőbbi gyors jelzése és a prioritásoknak megfelelő, szakszerű ellátása.

3. Hibaelhárítás

Gondosan, megfelelően végrehajtott megelőző intézkedések betartása esetén is előfordulhatnak hibák, zavaró események. Ezeket az észrevételeket, hibajelenségeket, zavaró eseményeket a kórházban dolgozó felhasználók kötelesek jelenteni a rendszergazdának telefonon, e-mailben vagy élőszóban. A rendszergazda köteles ezen események elhárítását mihamarabb, a fontossági sorrend betartásával megkezdeni vagy a szükséges intézkedéseket megtenni és az adott szolgáltatást a normál működés biztosításával helyreállítani. Fontos, hogy a rendszergazda a mihamarabb történő beavatkozással és a normál szolgáltatások gyors helyreállításával a minimálisra csökkentse a felhasználók által érzékelt lehetséges hatásokat. A rendszergazda a probléma megoldása során azonosítja, megállapítja, majd megoldja vagy külső szakembert vesz igénybe, az érvényben levő egyéb szabályok, előírások és szerződések alapján. Fontos, hogy azon problémák megoldására, melyek jelentős károkat, esetleg katasztrófahelyzetet okozhatnak, nagy prioritást kell rendelni. A problémák megoldásának folyamatait a hibák jellege, míg a sürgősségüket a rendelkezésre állási szintjük határozza meg.

A hibaelhárítási folyamat zárásaként a felhasználóknak lehetővé kell tenni az események visszacsatolását.

4. Katasztrófavédelmi és elhárítási szabályozás

A legnagyobb gondoskodás és körültekintés ellenére is előfordulhatnak olyan helyzetek, mely az informatikai, de akár az egész kórházi rendszer működése szempontjából is katasztrófa helyezetnek minősül. Ilyen esetben a szabályzatok és az erőforrások figyelembe vételével törekedni kell a rendszer működésének mielőbbi csökkentett, majd normál szintre történő visszaállításával. Az adatvesztés miatti katasztrófahelyzetet az alábbi szabályok betartásával kell biztosítani.

A rendszergazda a kórház szerverén tárolt adatainak, valamint műszaki meghibásodás esetén e rendszer gyors helyreállításának érdekében köteles a megfelelő adatmentésekről gondoskodni.

Az adatmentések technikai megvalósításának menetét, időzítését és egyéb paramétereit a rendszergazda által kötelezően elkészítendő mentési terv tartalmazza. E terv olyan részletezettségű kell legyen, hogy a rendszergazda távollétében, az őt helyettesítő személy is el tudja a mentést végezni.

Külön adathordozón köteles az adatokat lementeni, külön a rendszer helyreállításhoz szükséges állományokat és külön a rendszer naplózását.

Az adatok mentésénél a legutolsó mentést megelőző legalább öt visszamenőleges példányt köteles megőrizni biztonságos helyen.

A rendszer helyreállító állományokból elegendő a legutolsó működő állapotra vonatkozó adathordozót megőrizni. Amennyiben a rendszert érintő nagyobb szoftverváltoztatás kerül végrehajtásra, úgy a mentési tervben megjelölt mentési időszakon kívül soron kívül köteles a változtatások megkezdése előtt teljes mentést végezni az adatokról, a rendszerről és a naplózási állományokról.

A naplózási állományok mentéseit visszamenőleg egy évre köteles tárolni a rendszergazda.

A mentési tervben a kiemelten fontos adatok mentésére külön ki kell térni. Ezeket különös figyelemmel, gyakoribb mentési időközzel és legalább duplikált mentési technológiával kell végrehajtani. A duplikált mentés lehetőleg eltérő adattárolási eljáráson alapuljon (pl. egyik mentés mágneses adathordozóra

(szalagos egység, mobile rack, stb.) a másik mentés optikai adathordozóra (CD, DVD, stb.) történjen).
Az ilyen adatokat a rendszergazda jelöli ki az osztályvezetőkkel történő konzultációt követően.

A rendszergazda csak a szerveren, illetve a mentési tervben meghatározott adathordozókon tárolt adatok mentésért felel, a felhasználók hibájából és nem a kijelölt helyeken tárolt adatok elveszetésért nem vonható felelősségre.

Az egyéb katasztrófa helyzetekkel kapcsolatos szabályozást más szabályzatok rendelkezései szerint kell végrehajtani.

5. Mentési terv

5.1. Napi mentések
A kórház adatállományairól napi rendszerességgel kell mentést készíteni. Az adatállományok a MEDWORKS integrált informatikai rendszerből és a COMPUTREND pénzügyi-számviteli rendszeréből történik. A két szerverről a nap végén elkészült mentéseket kell kimásolni külső adathordozóra. A napi mentések helye az informatika számítógépében található merevlemezre történik. A napi mentéseket legalább egy hétig meg kell őrizni.

5.2. Heti mentések
A pénzügyi-számvitel rendszer adatállományáról heti rendszerességgel kell az adatokat külső adathordozóra (DVD) írni. Ezeket az archivált adatokat legalább fél évig meg kell őrizni.

5.3. Havi mentések
A MEDWORKS integrált informatikai rendszerből havonta egyszer, a hónap végén kell archivált mentést készíteni, amelyet külső adathordozóra (DVD) kell írni. Ezeket az adatokat legalább fél évig meg kell őrizni.

5.4. Mentések ellenőrzése
Minden heti, illetve havi mentés után fizikai ellenőrzést kell végezni a mentett állományokon. A fizikai ellenőrzést a mentést végző rendszergazda végzi el.

5.5. Mentések tárolása
A napi mentéseket az informatikán, külső adathordozón tároljuk. A heti és havi mentéseket két különböző helyen tároljuk. Az egyik a kórház területén, az informatikán található. Itt minden mentést meg kell őrizni.
A mentések külső tárolása az Erdős 2002. Bt. telephelyén (Csorna, Szent István tér 22.), elzárt trezorban történik. Itt az utolsó 6 hónap mentéseit kell megőrizni.

6. Záró rendelkezések

Az itt nem szabályozott kérdésekre a szabályzat 1.5 pontjában tételesen felsorolt szabályzatok rendelkezése az irányadó.

A szabályzat az aláírást követően, 2010. augusztus 1. napjától hatályos.

Csorna, 2010. augusztus 1.