Markusovszky Kórház	SZABÁLYZAT	Oldalszám: 23 Kiadás: 01 Változat: 01 Törzspéldány megőrzés: Érvényesség + 3 év

SZ-61.

Ikt. szám: 1/324-0/2017.

MARKUSOVSZKY EGYETEMI OKTATÓKÓRHÁZ

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

	Név / Beosztás:	Aláírás:	Dátum:
Készítette/módosította:	Molnárné Máté Zsanett informatikai biztonsági felelős		2017.05.01.
Ellenőrizte:	Gelencsér Mária informatikai osztályvezető		
	Dr. Káldy Zoltán minőségirányítási vezető		
Jóváhagyta:	Dr. Nagy Lajos főigazgató		

1. Informatikai Biztonsági Szabályzat

Az állami és a hivatali szervek elektronikus biztonságáról szóló 2013. évi L. Tv. 15.§ (1) bekezdés d) pontjában, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. Tv. 2. sz. mellékletében, továbbá a 246/2015. (IX.8) Korm. Rendelet 4.§ a) pontjában kapott felhatalmazása alapján a Markusovszky Egyetemi Oktatókórház (továbbiakban: Kórház) informatikai biztonsági szabályzatát (továbbiakban: IBSZ) az alábbiakban határozza meg:

a) informatikai biztonsági célokat, a szabályzat tárgyi, szervezeti, személyi és időbeni hatályát,
b) az informatikai biztonsággal kapcsolatos szerepköröket,
c) a szerepkörökhöz rendelt tevékenységeket,
d) a tevékenységekhez kapcsolódó felelősségeket,
e) az információs rendszerek alkalmazása során az adatbiztonságot,
f) az elektronikus információrendszerének helyes és biztonságos használatát,
g) az információbiztonság hivatalrendszerének belső együttműködését.

IBSZ -hez kapcsolódó és külön elkészítendő dokumentumok

- Adatvédelmi és adatkezelési szabályzat (SZ-03.)
- Informatikai Működési Rend Mentési és Archiválási melléklete (MR-43. 5. sz. melléklet)
- Katasztrófavédelmi Szabályzat (SZ-22.)

Alapfogalmak

Jelen szabályzat alkalmazásában:

1. *Adat*: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
2. *Adatfeldolgozás*: az adatkezeléshez kapcsolódó technikai feladatok elvégzése;
3. *Adatfeldolgozó*: az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelő részére adatfeldolgozást végez;
4. *Adatforgalmi munkaállomás:* adatbevitelre és adatfeldolgozásra használt munkaállomás
5. *Adatkezelés*: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy műveletek összessége, gyűjtése, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásnak megakadályozása;
6. *Adatkezelő*: az a természetes, jogi személy, jogi személyiséggel nem rendelkező gazdasági társaság vagy egyéni vállalkozó, aki vagy amely az adatkezelést végzi;
7. *Adminisztratív védelem*: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, tovább a védelemre vonatkozó oktatás;
8. *Alkalmazás:* informatikai program (szoftver), melynek feladata valamely informatikai feladat elvégzése;
9. *Bizalmasság:* az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

10. *Biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmasság, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;
11. *Biztonsági esemény kezelése:* az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló események jövőbeni előfordulásának megakadályozása érdekébe végzett tervszerű tevékenység;
12. *Biztonsági osztály:* az elektronikus információs rendszer védelmének elvárt erőssége;
13. *Biztonsági osztályba sorolás:* a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
14. *Biztonsági szint:* a Kórház felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
15. *Biztonsági szintbe sorolás:* a Kórház felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
16. *Elektronikus információs rendszer biztonsága:* az elektronikus biztonsági rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
17. *Elektronikus postafiók:* a munkahelyi feladatok korszerű és hatékony ellátása érdekében az elektronikus levelek fogadása, küldése valamint továbbítása céljából a Kórháznak és szervezeti egységeinek hivatalos, a munkavállalóknak személyhez kötött elektronikus üzenetkezelő rendszere;
18. *Felhasználó:* a Kórház olyan teljes munkaviszonnyal rendelkező munkatársa, aki munkáját számítógép használatával végzi;
19. *Fenyegetés:* olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;
20. *Fizikai védelem:* a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer; a megfigyelő rendszer; a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
21. *Globális kibertér:* a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese;
22. *Hardver:* az informatikai rendszer eszközei, fizikai elemei;
23. *Hálózati végpont:* az informatikai eszközök informatikai hálózathoz való csatlakozását szolgáló fizikai és logikai csatlakozási pont;
24. *Elektronikus információs rendszer biztonságáért felelős személy:* az informatikai biztonságért felelős és ilyen ügyekben intézkedési jogosultsággal rendelkező informatikusi végzettséggel rendelkező szakember;
25. *Informatikai biztonságpolitika:* a biztonsági célok, alapelvek és a Kórház vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására;

26. *Informatikai biztonsági stratégia:* az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere;
27. *Informatikai eszköz:* az információs tevékenységek végrehajtását, folyamatát támogató vagy megvalósító eszköz;
28. *Informatikai központ:* azon helyiségek, melyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak;
29. *Informatikai rendszer:* a hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat- illetve információ feldolgozás különböző feladatainak teljesítésére alkalmazunk.
30. *Internet:* nyílt hálózatok (számítógépek és adatátviteli kapcsolóeszközök) illesztésével létrejött világméretű számítógépes hálózat, mely a használója részére információs és kommunikációs lehetőséget kínál;
31. *Kiberbiztonság:* a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása;
32. *Kijelölt informatikus:* a Kórház által az adott munkaterület informatikai vagy speciális munkafeladat ellátására kijelölt informatikus;
33. *Kliens gép:* számítógép, munkaállomás, amelyen keresztül egy szerverről kérhetünk információt, szolgáltatásokat;
34. *Kockázat:* a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának és az ez által okozott kár nagyságának függvénye;
35. *Kockázatelemzés:* az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
36. *Kockázatkezelés:* az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;
37. *Logikai védelem:* az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal kialakított védelem;
38. *Mobil eszköz:* hordozható kiépítésű, mikroprocesszor vezérlésű, operációs rendszerrel és háttértárolóval rendelkező informatikai eszköz (pl. laptop, notebook, okostelefon);
39. *Munkaállomás:* munkavégzésre használt számítógép;
40. *Reagálás:* a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
41. *Rendelkezésre állás:* annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
42. *Sértetlenség:* az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás ellenőrizhetőségét, bizonyosságát is, illetve az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
43. *Szerver:* adatok és/vagy alkalmazások tárolására és szolgáltatására alkalmas nagyteljesítményű számítógép;
44. *Szoftver:* az informatikai rendszer olyan logikai része (alkalmazás), amely a működtetés vezérléséhez szükséges;
45. *Tűzfal:* a hálózat illetéktelen hozzáférés, behatolás elleni szűrését, védelmét biztosító eszközökből álló rendszer;
46. *User szupport tevékenység:* a felhasználók támogatása, munkaállomásaik karbantartása;
47. *VPN:* Virtuális magánhálózat.

Szabályzat célja

Az Informatikai biztonsági szabályzat célja a Kórház elektronikus információs rendszerének biztonságos működésének szabályozása, az informatikai eszközök megbízható alkalmazása, a Kórház által kezelt információvagyon sértetlenségének, bizalmasságának és rendelkezésre állásának megőrzése, az adatvédelem alkotmányos elveinek betartása, az adatbiztonság érvényesítése, a szoftverekhez való hozzáférési jogok meghatározása, az ellenőrzési mechanizmusok és felelősségi viszonyok tisztázása.

A szabályzat alapelvei

A Kórház informatikai rendszereiben biztosítani kell a kezelt személyes adatok védelmét az informatikai feldolgozás teljes életciklusában (a kezelt adat keletkezésétől, feldolgozásán, tárolásán és továbbításán keresztül), valamint az ilyen adatokat tároló, feldolgozó, továbbító rendszerek üzembiztos működését.
A Kórház informatikai rendszereiben biztosítani kell az érzékeny adatok adatbiztonságát.
A felhasználókat egyértelműen azonosító és hitelesítő mechanizmusok megvalósításával és az egyes rendszereken naplózandó események rögzítésével kell biztosítani az elektronikus információs rendszer bizalmasságát.
Az információ és a rendszerek rendelkezésre állása érdekében biztosítani kell a tárhelyek sértetlenségét, valamint olyan eljárásokat kell alkalmazni, amelyek megakadályozzák a kártékony kódok rendszerbe jutását és károkozását.
Az alkalmazott programok, hardver eszközök dokumentációjának nyilvántartásának naprakészségével kell biztosítani a Kórház elektronikus információs rendszerének hitelességét.
Az elektronikus információs rendszer bizalmasságának és sértetlenségének biztosításához mentési eljárásokat kell kidolgozni az adatokra, dokumentumtárakra, szoftverekre.
A dokumentáltság elve érdekében a rendszerek rendeltetésszerű működéséhez a szükséges ismereteket, telepítési útmutatókat, használati leírásokat az érintettek rendelkezésére kell bocsátani. Külső fejlesztő közreműködése esetén, a fejlesztést végző munkatárs készíti el.
A szükséges és elégséges ismeret elve alapján a rendszer minden felhasználónak biztosítja azokat az információkat és funkciókat, amelyhez az adott felhasználó csak azonosítás és hitelesítés után férhet hozzá.
Az információtartalom sértetlenségét biztosítani kell az adattárolás, kezelés és továbbítás folyamán, vagyis az adatokat, dokumentumokat, programokat, hardvert és szoftvereszközöket és ezek konfigurációit csak az arra jogosultak kezelhetik.
A rendszer teljes életciklusában érvényesülni kell az informatikai biztonsági szempontoknak.

Az információbiztonsági szervezet

A Kórház vezetése elkötelezett az információbiztonság kialakítása, bevezetése, működtetése, fenntartása, fejlesztése és ellenőrzése iránt.
Az informatikai biztonsági feladatok elvégzése az Informatikai Osztály felügyelete mellett történik.
A védett adatok teljes körű védelme érdekében a Kórház az adott rendszer támogatására kijelölt terület rendszergazdái (3 fő alkalmazás-üzemeltetési rendszergazda, 5 fő üzemeltetési rendszergazda) számára az adott rendszer felett teljes felügyeleti hozzáférési jogot ad, a titoktartási kötelezettség betartása mellett. Az informatikai rendszer működésével összefüggő dokumentációkba, nyilvántartásokba betekintési joggal bírnak és jelezhetik a biztonsággal kapcsolatos észrevételeiket az érintetteknek.

A Kórház vezetősége az informatika rendszerek biztonsági állapotának felmérése céljából vizsgálatot indíthat, melynek eredményéről az érintett terület vezetőjét tájékoztatja és korrekció céljából az ellenőrző vizsgálat eredményét átadja.
Az Informatikai Osztály vezetője rendkívüli incidens alkalmával a biztonságot érintő eseti döntéseket hozhat, melyről haladéktalanul tájékoztatja a Kórház vezetőjét.

Szabályzat hatálya

Tárgyi hatálya kiterjed a Kórház tulajdonában lévő valamennyi informatikai rendszerre és azok elemeire: alkalmazásokra, adatbázisokra, keletkezett, feldolgozott, tárolt és továbbított adatra, információra:

- a betegellátással összefüggő elektronikus adathordozón keletkező (aktív, archivált) adatok kezelésére és védelmére,
- a betegadatokhoz közvetlenül nem kapcsolódó, szolgálati vagy államtitok körébe tartozó gazdasági, pénzügyi vagy egyéb adatok védelmére,
- a Kórház dolgozóit érintő személyi adatok védelmére,
- a Kórházban keletkező tudományos kutatási, kutatásetikai adatok védelmére,
- az adatfeldolgozás alatt lévő, ott tárolt és a feldolgozás eredményeképpen létrejött adatok védelmére,
- a Kórház tulajdonában, kezelésében lévő valamennyi számítástechnikai berendezés, eszköz, folyamatra, valamint ezek műszaki dokumentációinak védelmére.

Szervezeti és személyi hatálya kiterjed a Kórház valamennyi szervezeti egységére, fő és részfoglalkozású munkatársára illetve az informatikai eljárásokban résztvevő más szervezetek dolgozóira. A fentieken túlmenően jelen Szabályzat szervezeti hatálya kiterjed a Kórházzal szerződéses jogviszonyban álló azon természetes és jogi személyekre, akik bármilyen módon kapcsolatba kerülnek a Kórház informatikai infrastruktúrájával, vagy bármely, az IBSZ hatálya alá tartozó, a megbízható működést vagy információ védelmet érintő eszközzel. Ezen személyek esetében a Szabályzat rendelkezéseit a velük kötött szerződésben és titoktartási nyilatkozatban kell érvényesíteni.
Időbeli hatálya a hatályba lépéstől visszavonásig érvényes.

Az IBSZ felülvizsgálatának rendje

Az IBSZ kidolgoztatása, ellenőrzése, majd karbantartásának megkövetelése a Kórház főigazgatójának feladata és hatásköre. A szabályzat alkalmazásáért és betartásáért a Kórház minden egysége és minden felhasználója felelős.
Az IBSZ tartalmát illetve kapcsolódó dokumentumainak felülvizsgálatát rendszeresen, de legalább kétévente, illetve minden olyan esetben végre kell hajtani, amikor a szabályzatban leírtakhoz képest jelentős változás történik a Kórház informatikai rendszerében. Ennek felelőse az elektronikus információs rendszer biztonságáért felelős személy.

2. Szerepkörök meghatározása

A Kórház vezetésének határozott iránymutatással, elkötelezettsége kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök egyértelmű kijelölésével és elismertetésével, aktív módon támogatnia kell az informatikai biztonságot a szervezeten belül.
Az információbiztonság elismertetése a vonatkozó szabályzatok hatályba léptetésével, és az érintettek körében végzett tudatosítás és képzés keretében valósul meg.

A Kórház vezetése jelen szabályzatban meghatározza és időszakosan felülvizsgálja az információbiztonsággal összefüggő felelősségi köröket. Az információbiztonsággal kapcsolatos felelősség megoszlik az elektronikus információs rendszer biztonságáért felelős személy, a Kórház főigazgatója, az adatvédelmi felelős és az egyes szervezetek és a felhasználók között.
Az információbiztonsági szabályzatban meghatározott biztonsági előírások végrehajtásáért és betartásáért a Kórház egyes szervezeti egységeinek vezetői vagy az általuk bizonyos részfeladatokra kijelölt munkatársai a felelősek.
Az informatikai biztonsággal kapcsolatos feladatok szerepkörhöz rendeltek az alábbiak szerint:

1) A **Kórház főigazgatója**: aki felelős az informatikai rendszerben tárolt adatok védelméért és az adatok biztonságáért. Hatáskörében jogosult a számítógépes adatvédelem és az adatbiztonság megszervezésére és ellenőrzésére.

Feladatai:

- Biztosítja a jogszabályban meghatározott követelmények teljesülését a Kórház információs rendszerére vonatkozóan.
- Elektronikus információs rendszer biztonságáért felelős személyt nevez ki, erről a hatóságok felé tájékoztatást nyújt.
- Meghatározza a Kórház elektronikus információs rendszerének felhasználóira vonatkozó szabályokat.
- Gondoskodik a felhasználók információbiztonsági ismereteinek oktatásáról.
- Kockázatelemzések, ellenőrzések és auditok lefolytatása révén meggyőződik, az információbiztonsági szempontok betartásáról.
- Biztonsági események bekövetkezésekor gondoskodik a gyors és hatékony reagálásról, az esemény kezeléséről, valamint az érintettek haladéktalan tájékoztatásáról.
- Ha külsős erőforrást vesz igénybe, akkor szerződéses kötelemként gondoskodik a törvényben foglaltak teljesüléséről. A Kórház főigazgatója ebben az esetben is felelős a meghatározott feladatokért.

2) **Elektronikus információs rendszer biztonságáért felelős személy** (továbbiakban: IBF): a főigazgató nevezi ki. Az IBF felel a Kórháznál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért:

Feladatai:

- A Kórházi szervezeti egységek munkájának ellenőrzése az adatbiztonság és a minősített adatok elektronikus kezelésének vonatkozásában. Az esetleges szabálytalanságok, biztonsági események kivizsgálása, jelentése.
- A főigazgatónak közvetlen tájékoztatást, jelentést adhat.
- Gondoskodik a Kórház elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról.
- Elvégzi vagy irányítja a fenti tevékenységek tervezését, szervezését, koordinálását és ellenőrzését.
- Előkészíti a Kórház elektronikus információs rendszereire vonatkozó Informatikai Biztonsági Szabályzatot.
- Meghatározza a rendszerek biztonsági beállításaival kapcsolatos elvárásokat, jogokat, feladatokat.
- Véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit.

- Ellenőrzi, hogy az informatikai rendszerben kialakított, aktuálisan beállított jogosultságok megegyeznek-e a jóváhagyott jogosultságokkal.
- Ellenőrzi a leselejtezésre kerülő eszközök adathordozóinak törlését.
- Bármely elektronikus információs rendszert érintő biztonsági eseményről köteles tájékoztatni a főigazgatót.
- A Kórház főigazgatójának támogatásával biztosítja az e szabályzatban meghatározott követelmények teljesülését.

3) Adatvédelmi felelős: aki felelős az adattudatos szervezeti működés kialakításáért és működtetéséért, valamint ennek keretében a személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását szolgáló intézkedések megtételéért.

Feladatai:

- Ellátja az adatfeldolgozás számítástechnikai felügyeletét.
- Tevékenyen részt vesz a védelmi eszközök alkalmazására vonatkozó döntés-előkészítésben.
- Felügyeli a számítástechnikai rendszerek üzembiztonságát, adatmentéseket készít, biztosítja azok tárolását és karbantartását.
- Gondoskodik az elektronikus információs rendszer elemeinek folytonos működésének, szerviz ellátás biztosításának felügyeletéről.
- Nyilvántartást vezet az elektronikus információs rendszer elemeiről.
- Ellenőrzi a vírusvédelem folytonos meglétét, használatát és frissítését.
- Figyelemmel kíséri az Internet, Intranet forgalmat és tartalmat.
- Vezeti és felügyeli a számítástechnikai eszközökre kötött biztosítások aktualitását.

4) Üzemeltetési rendszergazda: aki felelős a hozzátartozó szervezeti egység elektronikus információs rendszerének üzemeltetéséért és az ehhez tartozó számítástechnikai és adatvédelmi szolgáltatások biztosításáért.

Feladatai:

- Biztosítja az üzemképességet és a műszaki ellátást, gondoskodik a helyi adatok védelméről, mentéséről, tárolásáról.
- Irányítja és segíti a munkatársak számítástechnikai munkáját.
- Közreműködik a hardver és szoftver eszközök fejlesztésében.
- Elvégzi a hatáskörébe tartozó jogosultsági rendszerek kialakítását, engedélyezését és dokumentálását.

5) Alkalmazás-üzemeltetési rendszergazda: aki felelős az integrált medikai rendszerben tárolt adatok védelméért, biztonságáért és a felhasználók informatikai biztonságot elősegítő támogatásáért.

Feladata:

- A Medsol integrált medikai rendszer jogosultsági rendszerének kialakítása, jogosultsági szintek engedélyezése, dokumentálása.
- A rendszer paraméterezése az információvédelmi rendszabályok betartásával.
- A vonatkozó jogszabályi előírások betartása mellett irányítja, segíti és ellenőrzi a munkatársak számítástechnikai munkáját.

6) Felhasználó: aki felelős az elektronikus információs rendszerekben tárolt adatok védelméért és az adatok biztonságáért.

Feladatai:

- A munkavégzés során a rábízott eszközöket, szoftvereket felelősséggel az előírásoknak és utasításoknak megfelelően használja és megőrzi.
- Az IBSZ –t megismeri és betartja.
- Részt vesz az informatikai oktatásokban.
- Számítógépes munkavégzése során tiszteletben tartja a jogosultsági csoportjára vonatkozó szabályokat és korlátozásokat.
- A számítógépes rendszerekhez használt hozzáféréseit biztonságos módon kezeli és megőrzi. A hozzáférésével elkövetett visszaélésekből és károkból származó következményekért felelősséggel tartozik.
- Jelzi az informatikai biztonsághoz, illetve a számítógépes rendszerek használatához köthető észrevételeit felettesének vagy az IBF-nek.
- Informatikai segítséget kérhet, ha olyan jellegű feladatot kell ellátnia, amelyhez nincs meg a megfelelő informatikai tapasztalata.
- A munkájához szükséges eszközöket, alkalmazásokat és szolgáltatásokat a főigazgató engedélyével igényelheti.

Külső szolgáltatókkal történő kapcsolat szabályai

Külső kapcsolatnak minősül a Kórház informatikai rendszereinek bármilyen, nem a Kórház által felügyelt informatikai rendszerrel, illetve adatátviteli úton felépített kapcsolat.
Külső kapcsolat tervezése során kockázatelemzést kell végezni az Informatikai Osztálynak a kapcsolat kiépítése, a belépés módja vonatkozásában.
A külső szolgáltatók igénybevétele esetén a szolgáltatási megállapodásokban (szerződésekben) kell kitölteni a szolgáltatásra érvényes biztonsági követelményeket és szabályozást. Biztosítani kell a feladatért felelős szervezet számára a mérés és ellenőrzés feltételeit.
Az informatikai rendszerek, eszközök bevezetése, üzemeltetése során harmadik felek különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.
A szolgáltatási megállapodásokban ki kell térni a külső szolgáltató titoktartási kötelezettségére a Kórház rendszereinek üzemeltetésével, fejlesztésével kapcsolatos, illetve a rendszerekben tárolt, feldolgozott adatok, információk vonatkozásában.
Az informatikai célrendszereket érintő biztonsági követelményeket és védelmi intézkedéseket Kockázatkezelési eljárásban kell rögzíteni, míg a külső ügyfelek hozzáférését a hivatali információkhoz, rendszerekhez illetve infrastruktúrához külön szabályzatban kell rendezni.
A Kórház számítógépes hálózatait más hálózatokhoz kapcsolni csak az Informatikai Osztály vezetője és a Kórház vezetője együttes engedélyezését követően, központilag, védetten és ellenőrzött módon lehet.
Külső szolgáltatók, harmadik felek igénybe vételével, az informatikai biztonsággal kapcsolatos felelősség nem hárítható át, az a feladatért felelős szervezet első számú vezetőjét terheli.
A folyamatban lévő megállapodások (üzemeltetési, karbantartási szerződések) és az új szerződések információbiztonsági, titoktartási vonatkozásait, azok tartalmát és formáját az IBF ellenőrzi, és legalább évente felülvizsgálja.

3. Informatikai vagyontárgyak kezelésével kapcsolatos szabályok

Meg kell határozni, hogy a szervezetben ki és milyen módon viseli a felelősséget az informatikai vagyontárgyakért.

Az informatikai vagyontárgyak nyilvántartása a Logisztikai Osztály Tárgyi eszköz nyilvántartójának feladata, melyhez az adatszolgáltatást a kijelölt területek üzemeltetési rendszergazdái biztosítják a következő szempontok alapján:

- Információs rendszerek,
- Felhasználói alkalmazások,
- Rendszerszoftverek (operációs rendszerek, adatbázis-kezelők, egyéb szoftverek)
- Hardver elemek (szerverek, asztali és hordozható számítógépek, monitorok, nyomtatók, egyéb hardverelemek).

Nem követelmény, hogy az alkatrészszintű elemekről külön nyilvántartás készüljön

Munkaállomások, vékony kliensek használata:

- A Kórházban használt munkaállomásokat, vékony klienseket rendeltetésszerűen, munkavégzés céljából, a Kórház érdekeinek szem előtt tartásával, a Kórház által meghatározott módon, a felhasználó felelősségére lehet használni. A munkaállomások, vékony kliensek minden egyéb célú használata tilos.
- A felhasználó felelősséggel tartozik a munkavégzés céljából átvett munkaállomásért, vékony kliensért és köteles megőrizni annak hardver, szoftver integritását. Átvételekor aláírásával elismeri felelősségét az átvett eszközökért (*B.Sz. ny. 11-66 és B.11-67 r.sz nyomtatványon*).
- Szerzői jogokat sértő állományok elhelyezése a rendszerekben tiltott tevékenység.
- A felhasználónak tilos:
  - a számítógépre bármilyen szoftverkomponenst installálni,
  - a számítógépet fizikailag megbontani: alkatrészeket cserélni, be-, kiszerelni.
- A felhasználóknak a mindennapos munkájuk során a munkaállomás, vékony kliens használat tekintetében a következő szabályok szerint kell eljárniuk:
  - A számítógépes informatikai szolgáltatások igénybevételéhez kötelesek (a saját felhasználói nevükkel és jelszavaikkal hitelesítve magukat) a munkaköri feladataikban meghatározott tevékenységek elvégzéséhez szükséges rendszerekbe belépni.
  - Bejelentkezési jogosultsággal rendelkező felhasználóknak más felhasználó azonosítójával a Kórház hálózatára bejelentkezni tilos, kivéve akkor és csak akkor, ha erre a szervezeti egységének vezetőjétől írásbeli engedélyt kapott.
  - Abban az esetben, amikor a felhasználók munkaállomásaikat felügyelet nélkül hagyják, kötelesek a munkaállomást zárolni úgy, hogy a zárolás csak az arra jogosult által legyen feloldható.
  - Abban az esetben, ha a felhasználó a munkaterületét elhagyja, tilos felügyelet nélkül hagyni a nem felhasználónak minősülő külsős személyt, illetve köteles a helyiséget bezárni, ha más felhasználó nem tartózkodik ott.
  - A felhasználók kötelesek a központi erőforrásokkal feldolgozható anyagokat a központi hálózati erőforrások igénybevételével feldolgozni, és központi helyen (szervereken) tárolni.
  - A számítógépes munka befejeztével a felhasználóknak a munkaállomásaikat ki kell kapcsolniuk a tűzvédelmi előírásoknak megfelelően.
  - Otthoni munkavégzés és bármilyen más célból nem „minősített" osztályba tartozó adatot CD-n, pendrive -on, elektronikus levélben vagy egyéb más módon a Kórház informatikai infrastruktúrájából kijuttatni csak a szervezeti egység vezetőjének írásos engedélyével szabad.
  - Tilos minősített adatot bármilyen formában a Kórházon kívülre juttatni.

Szerverek üzemeltetésével kapcsolatos szabályok:

- A szervereknek illetéktelen behatolástól jól védettnek kell lenniük.

- A szerverek konzoljáról a munkafolyamat végén ki kell lépni.
- A nem használt szolgáltatásokat ki kell kapcsolni.
- A szerverekhez történő hozzáféréseket, illetve hozzáférési kísérleteket naplózni kell, aminek ellenőrzése az osztályvezető helyettes feladata.
- A jelentős incidenseket jelezni kell az IBF felé.

4. Pénzügyi erőforrások biztosítása

A Kórház vezetősége elkötelezett az információbiztonság menedzselése iránt. Ennek megfelelően:

- Gondoskodik a Kórház keretein belül a munkatársak megfelelő felvilágosításáról, tájékoztatásáról, oktatásáról;
- Biztosítja a szükséges anyagi, humán és technikai erőforrásokat;
- Beszerzések, beruházások alkalmával megtervezi az informatikai biztonság megvalósításához szükséges forrásokat;
- Támogatja az üzemeltető és a fejlesztő irányú törekvéseket;
- Rendelkezik tartalék eszközök biztosításáról.

Mivel a Kórházi információvagyon biztonsága nem kizárólag az annak kezelésével megbízott személyek feladata és felelőssége, ezért a vezetőség elvárja, hogy a Kórház minden dolgozója és szerződéses partnere sajátjának tekintse az információ biztonságának ügyét, azt külön utasítás nélkül támogassa feladatán és hatáskörén belül.

5. Az informatikai rendszerek védelmének irányelvei

A Kórházban védeni kell minden olyan elektronikus információs rendszert, amely magába foglalja az informatikai feldolgozó, adatátviteli, hírközlési eszközöket, valamint ezek adathordozóit, amelyek részt vesznek a védett adatok előkészítésében, létrehozásában, tárolásában, feldolgozásában és továbbításában.
Fokozott figyelmet követel meg a teljes informatikai infrastruktúra védelme, ezen belül a pénzügyi, számviteli és betegadminisztrációs rendszerek, szakmai folyamatokat támogató információs rendszerek, a személyügyi nyilvántartó rendszerek, adatátviteli rendszerek és egyéb biztonsági elemek és azok adatai.

Az elektronikus információs rendszer nyilvántartása

A Kórház az elektronikus információs rendszereiről nyilvántartást vezet, amit szükség szerint aktualizál. A nyilvántartásnak az alábbiakat kell tartalmaznia:

- általános adatok: rendszert használó neve, munkaköre, település neve, helyiség neve;
- a felhasználóhoz tartozó hardver jellemzői: eszközazonosító, eszköz típusa, gyári száma;
- központi gépekre vonatkozó jellemzők: megnevezés, konfiguráció, operációs rendszer típusa, funkciója és futó szolgáltatásai;
- szoftvernyilvántartás: operációs rendszer típusa; egyéb alkalmazás jelölése;
- licencek nyilvántartása.

A nyilvántartásban minden mozgásról egyedi sorszámmal ellátott bizonylat készül. A bizonylatot az átadás-átvételben érintett szervezeti egység munkatársa, valamint az Informatikai Osztály által a feladatban részt vevő üzemeltetési rendszergazda aláírásával hitelesíti. A bizonylat 1 példánya az osztályon marad, 1 példánya a tárgyi eszközök

nyilvántartását végző szervezeti egységhez kerül. Az elkészült bizonylatot az Informatikai Osztály kijelölt munkatársa elektronikusan archiválja.

Beszerzés

Az Informatikai Osztály kezelésében álló informatikai eszközök, illetve egyéb ehhez kapcsolódó alkatrészek beszerzését a mindenkori hatályos beszerzési és közbeszerzési szabályoknak megfelelően kell végezni.
A számítógép és a hozzákapcsolódó perifériák esetében az Informatikai Osztályra leadott igények alapján történő árajánlatkérés, megrendelés, majd beszállítást követően az eszközök bevételezését a tárgyi eszközök nyilvántartását végző szervezeti egységnek kell elvégezni a szállított eszközökről szóló szállítólevél vagy számla alapján. A bevételezést követően az eszközöket el kell látni leltári azonosítóval. Bevételezés előtt informatikai eszköz nem kerülhet osztályra.
Az alkatrésznek minősülő eszközök igényét az üzemeltetési rendszergazdák összesítik a javításra váró berendezések, a raktárkészlet és az osztályokról leadott igények alapján. Az összesített alkatrészigényből a rendelkezésre álló pénzügyi források erejéig ajánlatkérés történik.

Áthelyezés, szállítás

Az informatikai eszközök, berendezések áthelyezése csak az üzemeltetési rendszergazdák közreműködésével, felügyeletével végezhető. Az áthelyezésről köteles átadás-átvételi bizonylatot kitölteni és a felhasználóval aláíratni. (*B.Sz. ny. 11-66 és B11-67 r.sz nyomtatványon*).

A Telephelyek közötti áthelyezés estén az átadás-átvételi bizonylat mellett kötelező szállítólevelet kiállítani. A szállítólevélnek tételesen kell tartalmaznia a szállított eszköz paramétereit.

Idegen tulajdonú informatikai eszközökkel kapcsolatos eljárás

A Kórház tulajdonába kerülő vagy használat céljából a Kórházba szállított idegen informatikai eszközökről nyilvántartást kell vezetni.
A bizonylati rend szerint a tárgyi eszköznyilvántartásban IDEGEN jelöléssel kell ellátni az idegen tulajdonú eszközöket.

6. Személyi Biztonság

Munkakörök meghatározása
A munkakörre vonatkozó feladatokban, a munkaköri leírásokban rögzíteni kell az egyes munkakörhöz tartozó feladatokat és felelősségi köröket és a szükséges informatikai jogosultságokat. Minden munkakörhöz csak a munkához feltétlenül szükséges jogosultságokat szabad megadni.
A szervezet elektronikus információs rendszeréhez való hozzáférés előtt a felhasználó írásbeli nyilatkozatával igazolja, hogy a rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, és saját felelősségére betartja. (*Belépő dolgozó megismerési nyilatkozata*)
Új munkatársak felvételekor, amennyiben munkaköre szükségessé teszi, a következő informatikai környezet kialakításáról kell gondoskodni a felelős szervezeti egységnél:

Feladat	Felelős
Számítógép/Vékony kliens biztosítása	Informatikai osztályvezető
Hozzáférési jogok beállítása	Rendszergazdák
Email postafiók létrehozása	Üzemeltetési rendszergazda
Külső internet hozzáférés	Üzemeltetési rendszergazda
Informatikai biztonsági oktatás	IBF
Titoktartási nyilatkozat	Informatikai Osztály

A Kórház munkatársai számára előírható informatikai jellegű oktatások:

- Általános célú informatikai oktatás,
- Informatikai biztonsági oktatás,
- Felhasználói alkalmazások ismertetése,
- Egyéb informatikai jellegű tanfolyamok, képzések.

Munkakör megszűnése, megváltozása

Munkatársak jogállásnak megváltozása esetén fenn kell tartani a biztonsági intézkedéseket. A munkatársak kilépése, tartós távolléte vagy a munkakör változása esetére az informatikai jogosultságok, eszközök tekintetében a következő eljárást kell alkalmazni: és a megfelelő adatlapot kitölteni (*Kilépő dolgozó informatikai nyilatkozat*):

- Intézkedni kell az érintett munkatárs jogosultágainak visszavonásáról, felfüggesztéséről vagy megváltoztatásáról.
- A munkatárs kilépése, tartós távolléte esetén a munkatársnak vissza kell szolgáltatnia az informatikai vagyontárgyak nyilvántartásában a nevén szereplő vagyontárgyakat (pl: laptop). A munkakör megváltozása esetén felül kell vizsgálni, hogy a munkatárs felelősségébe tartozó vagyontárgyak közül az új munkakör esetében, mely vagyontárgyak megtartása indokolt. Egyben ellenőrizni kell a vagyontárgyak meglétét is.
- Megszűnteti vagy visszaveszi a személy egyéni hitelesítő eszközeit (pl. mágnes kártya).
- Tájékoztatja a jogviszonyt megszüntető felhasználót a rá vonatkozó, jogi úton is kikényszeríthető, a jogviszony után is fennálló kötelezettségeiről.
- Felveszi a kapcsolatot a munkahelyi vezetővel, a jogviszonyt megszüntető dolgozó hivatali postafiókjához, szerveren vagy munkaállomáson tárolt elektronikus anyagaihoz illetve a folyamatban lévő ügyek kezeléséhez történő hozzáférések más munkavállalóhoz történő kiosztása miatt.

7. Kockázatkezelési stratégia

A Kórház feladata, hogy az elektronikus információs rendszereit érintő biztonsági kockázatokra és azokkal kapcsolatos következményekre megtegye a szükséges védelmi intézkedéseket. Ehhez fel kell mérnie azokat az eshetőségeket, amelyek fenyegető tényezőként befolyásolhatják a Kórház elektronikus információs rendszereinek megbízható, folyamatos és rendeltetésszerű működését. A legfontosabb feladat, hogy a lehető legnagyobb mértékben csökkentse a veszélyeztető tényezők bekövetkezésének valószínűségét.
A kockázat azonosításával a megfelelő válaszlépések kialakíthatók és a kockázatok mérsékelhetők. A választott intézkedések kockázatkezelési hatásait szükséges felmérni, melynek eredményét össze kell vetni az adott tevékenységgel kapcsolatos, eredetileg tervezett

végeredménnyel. A hatékony folyamatba épített ellenőrzés a legjobb eszköz a kockázatok kezelésére.
A Kórház feladata, hogy csökkentse ez elektronikus információs rendszerét érintő jellemző kockázatokat (tűzeset, hacker-támadás, lopás, erőszakos behatolás, rongálás stb.), továbbá a nem várt, illetve nehezen számszerűsíthető kockázatok (földrengés, árvíz, terrortámadás) következményeit is.
A Kórház célja, hogy az üzletmenet folytonosságát befolyásoló problémák estén a szolgáltatások a lehető legrövidebb idő alatt, a lehető legkisebb költséggel visszaállíthatóak legyenek. A probléma elhárítása mellett a preventív, megelőző célú karbantartásokkal csökkenti az egyes eszközök és ezáltal a teljes infokommunikációs rendszer összeomlásának kockázatát. Helyreállítási és cselekvési tervet készít az incidensek kezelésére, amely a katasztrófa védelmi terv részét képezi.
A Kórház célja, hogy a megelőzés érdekében olyan lépéseket tegyen, amelyek csökkentik a veszélyforrásokat és az esetlegesen bekövetkezett károk mértékét minimálisra redukálják. Ehhez szervezeti szinten beazonosítja az elektronikus információbiztonsági rendszerének biztonsága ellen ható események bekövetkezési lehetőségét.
Minden a Kórház informatikai rendszerét ért incidensről az elektronikus információs rendszerek biztonságáért felelős személyt tájékoztatni kell, aki a kapott adatok alapján elvégzi a szükséges elemzéseket, és ezzel összefüggésben kezdeményezi a kockázatkezelési rend aktualizálását is.

8. Fizikai védelem

A Kórház fizikai védelmi rendje összefoglalja az elektronikus információs rendszereinek helyt adó létesítményeibe történő belépések szabályozását, illetve meghatározza a fizikai belépések ellenőrzésének rendjét.
A Kórház célul tűzi ki a Kórháznál dolgozók személyi biztonságát és egészségét, a környezeti elemektől való megóvását, valamint a teljes elektronikus információs rendszerének fizikai biztonságát és szünetmentes áramellátását, szerver szobájának kiemelt védelmét.
A Kórház létesítményeinek fokozottan védett területére illetéktelenek nem léphetnek, illetve információvagyonához semmilyen módon nem férhetnek hozzá. Továbbá biztosítja a megfelelő védelmi intézkedések és eszközök meglétét a környezeti elemek által okozható károk elhárítására (pl. tűz, por, hőség, pára stb.) is.
A Kórház informatikai rendszerek elemeinek helyt adó helyiségek közül azoknál, ahol különleges védelmet igénylő informatikai eszközök találhatók, ellenőrzött beléptetési rendet alkalmaz:

- fokozott vagy kiemelt biztonsági osztályba sorolt rendszerelemek esetére,
- hálózati szerverek működésének helyszínére,
- hálózati menedzselés helyszínére.

Megkülönböztetett gonddal kell figyelni a Kórház nyilvános területén elhelyezett hálózati aktív eszközök védelmére. A rack szekrényekhez történő illetéktelen, helyi hálózatra való felcsatlakozás beláthatatlan következményekkel járhat, ezért a szekrények zárhatóságát biztosítani kell. Figyelemmel kell követni a hálózati kábelek és csatlakozók sértetlenégét. A hálózati passzív elemek megbontását csak az Informatikai Osztály üzemeltetési rendszergazdái, vagy a Kórház által megbízott, garanciát szolgáltató cég teheti meg.
A hálózati aktív eszközök esetén fokozott figyelemmel kell védeni a rendelkezésre álló csatlakozóhelyek teljes körű kihasználását. Nem maradhat hálózati végpont kihasználatlanul, üres állapotban.
A Kórház számítógépes hálózatára számítógépet, vékony klienst, egyéb gyengeáramú berendezést kizárólag az Informatikai Osztály munkatársai csatlakoztathatnak. A nem használt végpontokat, aktív eszköz portokat inaktív állapotba kell helyezni.

Fizikai védelem irányelvei

- portaszolgálat biztosítása,
- biztonságtechnikai rendszer használata a Kórház létesítményeinek védelmére,
- folyamatos áramellátás biztosítása szünetmentes tápegységek használatával, az áramingadozások és áramkiesések idejére a kritikus információtechnikai eszközök esetén,
- „üres asztal-tiszta képernyő" politika bevezetése,
- felhívja munkavállalói figyelmét az általuk használt informatikai eszközök fizikai védelmére a jogosulatlan hozzáférésektől, sérülésektől valamint az illetéktelen beavatkozásoktól,
- oktatások alkalmával a Kórház dolgozóit tájékoztatni kell az egyéni felelősségükről a fizikai környezet megóvása kapcsán,
- Hivatali időn kívül a Kórház meghatározott létesítményeinek helyiségeit mozgásérzékelő, riasztóberendezés védi.

9. Logikai védelem

A Kórház biztosítja az elektronikus információs rendszereiben tárolt adatok védelmet az alábbi szoftverkomponensek használatával:

- felhasználó azonosítása,
- hozzáférés-engedélyezése,
- audit (naplózási tevékenység),
- tűzfalak,
- antivirus szoftver,
- behatolás jelző és megelőző rendszerek.

A szoftverhasználat korlátozásai

A Kórház tartományi hálózatába csatlakoztatott munkaállomásokon, valamint a vékony kliensek által elért terminál szerveren csak a szervezetnél rendszeresített, beszerzett és jogtiszta alkalmazások működhetnek.
A Kórház bármely informatikai rendszerére csak az informatikus telepíthet szoftvereket. Felhasználók korlátozott fiókkal rendelkeznek, így programokat nem telepíthetnek, módosíthatnak és törölhetnek. Ettől eltérni csak a szervezet vezetőjének vagy az IBF engedélyével lehet. Amennyiben a felhasználó részéről igény jelentkezik új szoftver telepítésére, a kérelmező köteles egyeztetni az IBF-el a telepítendő szoftver jogtisztaságáról és annak jogos felhasználásáról, ezt követően kell felterjeszteni a kérelmet engedélyezésre a szervezet vezetője számára.
A Kórház informatikai struktúrájában a feladatok végrehajtására kizárólag a szervezet által megvásárolt licencű kereskedelmi szoftver terméket vagy szoftvereket lehet alkalmazni. Minden illegális vagy nem a munkavégzéshez szükséges szoftvert, adatot törölni kell a rendszerből. Ezt a művelet a felhasználó tudtával és az IBF engedélyével a műszaki rendszergazdák végzik el.
Telepítés előtt vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét.
A felhasználó feladatainak ellátásához köteles a rendszeresített alkalmazásokat használni, illetve a hálózati biztonság érdekében alkalmazott programok időszakos futtatását köteles engedélyezni (vírusirtó, Windows update).
A telepített alkalmazások eredetiségét igazoló OEM matricát a felhasználó köteles megóvni.

Azonosítás és hitelesítés, hozzáférés engedélyezés

A Kórház hitelesítésre és azonosításra tudás alapú azonosítást használ jelszavak maximális használati idejét. Megvédi a hitelesítésre szolgáló jelszavak tartalmát a jogosulatlan felfedésektől és módosítástól. Megköveteli a felhasználóktól, hogy védjék jelszavaik bizalmasságát és sértetlenségét.
Az azonosítási folyamatban a felhasználó megadja azonosságát a rendszer felé az ötjegyű felhasználói azonosítója segítségével. A hitelesítés a felhasználó állítólagos azonosságának a bizonyítására szolgál. A szervezet informatikai rendszereiben legalább (tudás alapú) jelszavas hitelesítést kell alkalmazni.
A hitelesítési adatokhoz való hozzáférés korlátozása érdekében az ilyen adatokat védeni kell a jogosulatlan betekintéstől, megismeréstől, módosítástól és törléstől. Az azonosítási és hitelesítési adatok és eszközök kezelésére, az azonosítás és hitelesítés folyamatára az alábbi szabályok érvényesek:

- Az alkalmazás-üzemeltetési rendszergazdák gondoskodnak arról, hogy a Medsol, eMedsol rendszerben szereplő minden felhasználói azonosító valós felhasználóhoz tartozzon.
- Az adminisztrátori (rendszergazdai) feladatokhoz külön azonosítót kell létrehozni.
- Az alkalmazás-üzemeltetési rendszergazdáknak az azonosítási adatokat naprakészen kell tartania, az új felhasználókat be kell vezetni a Medsol, eMedsol rendszerbe; a Kórháztól eltávozott munkatársak jogait pedig visszavonni.
- A Kórház informatikai rendszereihez hozzáférő felhasználóknak egyedi módon azonosítaniuk kell magukat. Más felhasználók azonosítójának használata tilos! Ugyanez vonatkozik az egyéb alkalmazások vonatkozásában is.
- Tilos a jelszavakat másnak átadni, elmondani vagy leírni.
- A felhasználó jelszavakat az alkalmazásoknak megfelelő jelszó szabály szerint kell létrehozni.
- Amennyiben egy munkaállomáson több felhasználó is jogosult dolgozni, úgy a feladat elvégzése után, mielőtt a másik felhasználó a géphez hozzáférne, a rendszerből ki kell jelentkeznie.
- A munkaállomás elhagyásakor nem lehet a számítógépet zárolás nélkül hagyni.
- A felhasználói jelszavakat 3 havonta meg kell változtatni.

A felhasználó távollétében történő elkerülhetetlen hozzáférést az illetékes vezető kezdeményezheti a Kórház vezetőjénél. Amennyiben a hozzáférést engedélyezi, a rendszergazdák megteszik a szükséges intézkedéseket.
A felhasználói azonosítók elvesztését, elfelejtését, kompromittálódását azonnal jelezni kell a szervezet vezetőjének és az IBF-nek.
A lokális számítógépes hálózathoz külső fél csak vendég felhasználóként férhet hozzá. A szervezet területén WIFI hálózat csak indokolt esetben használható és érhető el. Engedélyezése a szervezet vezetőjének írásos jóváhagyásával történhet.
A Kórház elektronikus információs rendszerében az általános, minden munkatársát érintő, tájékoztató jellegű információkat tartalmazó mappák, fájlok eléréshez nem kér külön autentikációt. Ezek a központi gépen tárolt, közös mappákban található szabályzatok, utasítok, alkalmazás leírások, elektronikus eszköz használati útmutató, stb.
A Kórház nyilvánosan hozzáférhető rendszerként határozza meg a publikus weboldalát. Az oldal üzemeltetéséért felelős munkatársnak gondoskodni kell az azon publikált információk törvényi megfelelőségéről és valódiságáról, sértetlenségéről.

Felhasználói fiókok kezelése

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságot csak a szervezet vezetőjének külön engedélyével, indokolt esetben kaphatnak. Kivételt képeznek azok az informatikai rendszerek, ahol a zavartalan működés feltétele az admin jogosultság. Az így kapott jogot a felhasználó nem használhatja üzemeltetői feladatokra.
A munkaállomásaikon a felhasználóknak tilos megosztani hálózati szolgáltatásként mappákat, fájlokat. Amennyiben a megosztás szakmailag indokolt, a közvetlen vezető kezdeményezésére az IBF jóváhagyásával az informatikus végezheti el a feladatot. Csak azok a felhasználók kaphatnak jogot a megosztott erőforrások eléréséhez, akiknek az a munkájukhoz valóban szükséges.
A Kórház minden szobájában van hozzáférés a hálózati erőforrásokhoz, amelyek eléréséhez hálózati szintű jogosultság szükséges. Ezek a jogok az alábbi tevékenységek elvégzését teszik lehetővé:

- hálózat kezeléséhez szükséges programok,
- közös nyomtató használat,
- internet böngészés,
- elektronikus levelezés,
- adatbázisok elérése,
- programok és adatok elérése.

Rendszer- és kommunikációvédelem

A Kórház felügyeli és ellenőrzi elektronikus információs rendszerének külső határain történő, valamint a rendszer kulcsfontosságú belső határian történő kommunikációt. A zónák közötti kommunikáció csak szabályozott formában, határvédelmi rendszer beiktatásával történhet.
A Kórház információs rendszereiben ellenőrizni kell mind a belső, mind a külső hálózatra telepített szolgáltatásokat. Ennek érdekében a Kórház hálózata és bármely más szervezet hálózata közé, illetve a nyilvános hálózatok közé proxy szerver kerül telepítésre. Fontos szempont az is, hogy a hálózatok terhelésének optimális eloszlása illetve a hálózati adatbiztonság növelése érdekében minden hálózati szolgáltatás eléréséhez útvonal korlátozások kerülnek bevezetésre.
Alapvető szabályok:

- A különböző zónák (intranet – internet) közötti kommunikáció tűzfal által kontrollált.
- Amennyiben egy kommunikációs csatorna nincs külön engedélyezve, az tiltott.
- Az egyes hálózati zónák közötti kapcsolat létrehozásakor az alábbiakat kell figyelembe venni:
  - a kapcsolat megfelelő erősségű titkosítással legyen biztosítva
  - a kapcsolat megfelelő erősségű azonosítással legyen biztosítva.
- A kapcsolat megvalósításához ajánlott technológia: VPN.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, frissítéséről gondoskodni kell.

Külső elektronikus információs rendszer használata

A Kórház belső munkatársai engedélyhez kötötten használnak távoli elérést a szervezet elektronikus információs rendszereihez. A Kórházzal szerződéses jogviszonyban álló, a folyamatos üzemeltetési feladatok ellátásával megbízott külső cég kijelölt munkatársai

állandó távoli hozzáférést kapnak az általuk felügyelt rendszerhez. Ezeket a hozzáféréseket a cégnek az IBSZ betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük. VPN kulcsok kiadása az Informatikai Osztályvezető kompetenciája.

Rendszer és információsértetlenség

A Kórház Vírusvédelmi szabályzatában kerültek részletes meghatározásra a szervezetet érintő rendszer- és információsértetlenségre vonatkozó intézkedések. A Szabályzat tartalmazza a szervezet számítógépes vírusvédelmére vonatkozó előírásokat, felelősségi köröket és rögzíti az ehhez kapcsolódó feladatokat.
A Kórház az elektronikus információs rendszereiben tárolt adatok vírusvédelme, a vírusfertőzések elkerülése érdekében rendszeres vírusellenőrzést végez. Ehhez többszintű kártékony programok elleni szoftveres védelmet vezetett be, amely a klienseken és a szervereken fejti ki hatását.
A kártékony kódok felderítése, hatásuk, aktiválódásuk megelőzése, terjedésük korlátozása érdekében a munkaállomások fájlrendszerét rendszeresen ellenőrizni kell. Az ellenőrzésnek ki kell terjedni a vírus- és kémprogram eltávolító alkalmazásokra. Az ellenőrzést egyrészt a karbantartási, hibajavítási és felhasználói ellenőrzés folyamatba beépítve, másrészt ütemezett módon automatikusan kell végrehajtani.
A kártékony kódok elleni védelem fő alkalmazása az Sophos Endpoint Protection Advanced and Mail, valamint kiegészítő alkalmazása a Sophos eXploit Prevention.

Az elektronikus információs rendszer felügyelete

Az üzemeltetési rendszergazdáknak rendszeresen monitorozni kell az operációs rendszereket, a rendszer biztonsági állapotát és az eseteges biztonsági eseményeket. Az üzemeltetési rendszergazdáknak tilos:

- nem tesztelt frissítéseket telepíteni,
- olyan operációs rendszerfrissítést telepíteni, amely a tesztek során nem felelt meg az elvárásoknak,
- nem az előírások szerint végezni az üzemeltetést.

A szervezet vezetőjének gondoskodni kell a Kórház informatikai rendszerének felügyeletéről az alábbi szempontokat figyelembe véve:

- szükség szerinti monitorozás,
- váratlan események rögzítése, kivizsgálása,
- rendszeres felülvizsgálatok kezdeményezése,
- rendszerhibák okán fellépett biztonsági események elemzése,
- képzéseket rendel el az elektronikus információs rendszerben tárolt adatok, információk kezelését végző felhasználók oktatására, mind a hatályos jogszabályok, mind az informatikai biztonsággal, működéssel kapcsolatban.

10. Viselkedési szabályok az interneten

A Kórház email postafiókkal és Internet használati joggal rendelkező dolgozói csak a munkájukkal összefüggésben használhatják a Kórház által biztosított szolgáltatásokat. A belső hálózaton Internet kapcsolatot kizárólag tűzfalon keresztül lehet elérni. Nem megengedett az egyéb csatlakozási lehetőség (mobiltelefonos).

Az Internet szolgáltatás magán célú használata tilos. Az Internetforgalom szoftveresen szűrésre kerül és a felhasználó számára beállított havi kvóta erejéig vehető igénybe.
A felhasználóknak az Internet használat során az alábbi szabályokat kell betartaniuk:

- Tilos látogatni on-line játék, fogadási, csevegő, letöltő, pornográf és törvénybe ütköző tartalmakat szolgáltató oldalakat. Ezekről letölteni, ilyen tartalmakat publikálni, adatokat cserélni és tárolni!
- Az Internetről letöltött programok telepítése és futtatása nem megengedett. Igény esetén az informatikai osztályvezető, előzetes bevizsgálás után (vírusmentesség, környezetbeágyazhatóság illetve szerzői jogok tekintetében) engedélyezheti az ilyen alkalmazások letöltését és futtatását.
- Nem engedélyezett a csevegő programok használat (pl. skype, google hangouts stb.), kivéve, ha a Kórház érdekéből történik használatuk, amire a szervezet vezetője adhat dokumentált módon engedélyt.
- Tilos a Kórházzal kapcsolatosan belső információkat nyilvános oldalakra feltölteni, bármi módon közzétenni.

A belépési nyilatkozat tartalmazza a felhasználó hozzájárulását az email postafiókja, illetve az Internetes tevékenységének monitorozásához.
Az Internet-kapcsolatok üzemeltetéséért felelős vezetőnek jogában áll az Internet-hozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozásához, amiről a felhasználókat előzetesen értesíteni kell.

11. Az elektronikus információs rendszer mentései

A Kórház informatikai rendszereiben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell. Az informatikai infrastruktúrában a biztonsági mentési eljárást, annak pontos leírását valamint az ehhez tartozó feladatokat, szabályokat a Kórház Informatikai Működtetési Rendjének Mentési és Archiválási melléklete tartalmazza (*MR-43. 5.sz melléklet*).
Teljes biztonsági mentést és archiválást kell végezni a munkaállomásokon és szervereken található, elektronikus adatokról. Az adatok mentésének és archiválásának időrendjét és felelősét az adatmentési melléklet tartalmazza.

12. Cselekvési terv

A Kórház cselekvési tervet készít, ha elektronikus információs rendszerérében változás állt elő, vagy egy belső informatikai jellegű vizsgálat hiányosságokat állapít meg. Ebben dokumentálja a felfedezett gyengeségek javítására, az elektronikus információs rendszer ismert sérülékenységeinek csökkentésére vagy megszüntetésére irányuló tervezett tevékenységeket. Amennyiben elektronikus információs rendszere megfelel az előírtaknak, meghatározott gyakorisággal ellenőrzi és felülvizsgálja azt.

13. Karbantartás

Rendszeres karbantartás

A Kórház információs vagyonához tartozó számítógépeken, hordozható eszközökön, külső perifériákon, egyéb informatikai eszközökön a gyártójuk által megadott eljárásnak és időszaknak megfelelően a karbantartást kell végezni. A karbantartást csak megfelelő

szaktudással rendelkező üzemeltetési rendszergazda végezheti, évente legalább egy alkalommal.
A szerverszoba rendjéért és az ott elhelyezett informatikai eszközök karbantartásáért az osztályvezető helyettes felel. Legalább évente egyszer gondoskodni kell a légkondicionáló beltéri és kültéri egységeinek tisztításáról, illetve a szünetmentes tápegységek kalibrálásáról.
Biztosítani kell továbbá a szoftverek karbantartásával (update, upgrade) kapcsolatos frissítések szerződés szerinti végrehajtását, melynek ellenőrzése az osztályvezető helyettes feladata.
Tilos az automatikus frissítés engedélyezése a tűzfal, levelező szerver, alkalmazásrendszereken.

14. Adathordozók védelme

A Kórház gondot fordít az információs vagyonába tartozó adathordozók ellenőrzésére és fizikai védelmére az eltulajdonítástól, az illetéktelen másolástól, leolvasástól, annak érdekében, hogy az adathordozón tárolt dokumentumok, kimenő és bemenő adatok, rendszerdokumentációk ne kerüljenek illetéktelenekhez illetve rendelkezésre állásuk, sértetlenségük biztosított legyen.

Hozzáférés az adathordozókhoz

A Kórház informatikai rendszerében idegen adathordozó nem csatlakoztatható, nem használható.
A munkaállomásokon csak korlátozott módon lehet CD-t vagy DVD-t használni. Magáncélú CD vagy DVD másolás semmilyen formában és célból nem engedélyezett.
A Kórház informatikai rendszerében memóriakártya-alapú vagy külső merevlemezen adatmentést, adattárolást és továbbítást csak a szervezet által erre a feladatra kiadott eszközökön és felhatalmazással lehetséges.

Adathordozók törlése

A használatból kivont adathordozók, mint HDD, pendrive vagy más memóriát selejtezésre. megsemmisítésre az üzemeltetési rendszergazdáknak kell átadni. CD-t, DVD-t a felhasználó szervezet selejtezi. Az adathordozókat fizikailag alkalmatlanná kell tenni további használatra, ezt követően lehet lefolytatni a selejtezési eljárást és a használatból történő kivonást, melynek nyilvántartása selejtezési jegyzőkönyvben történik.
Azokat az adathordozókat, amelyek fizikailag sérültek, javíthatatlanok és adat tárolására alkalmatlanok vagy véglegesen elhasználódtak, megsemmisítéssel a használatból ki kell vonni.

Adathordozók használata

A felhasználó teljes felelősséggel tartozik az általa használt adathordozók használatáért, az információbiztonsági követelmények betartásáért.
Mobil adathordozót a szervezet informatikai rendszerébe a felhasználók nem csatlakoztathatnak, csak a szervezet vezetőjének külön engedélyével. Amennyiben a szervezet vezetője jóváhagyta a külső adathordozó használatát, a felhasználó minden alkalommal köteles vírusellenőrzést végrehajtani az eszköz használata előtt.

15. Hibajavítás

A Kórház figyelmet fordít elektronikus információs rendszereinek folyamatos hibavédelmére, mind az adatátviteli, mind az adatfeldolgozási műveletben fellépő hibák teljes kiküszöbölésére, a helyes adatok visszaállítására, a hibás és zavaros jelek kiszűrésére.
Az elektronikus információs rendszerbe bevezetésre kerülő új alkalmazások, csak tesztelés után kerülhetnek az éles rendszerbe.
Az informatikus feladata, hogy az alkalmazott szoftverekhez kiadott upgrade -eket lehetőség szerint a kiadást követően fel kell telepíteni a munkaállomásokra.

16. Naplózási eljárásrend

A Kórháznál használt informatikai rendszerekben bekövetkezett fontosabb események feltárását, az elszámoltathatóság és ellenőrizhetőség érdekében, naplózási rendszer kialakításával biztosítja. Ezáltal ellenőrizni lehet a hozzáférések jogosultságát, az illetéktelen hozzáféréseket a felelősség megállapítására.
A Kórház szerverein biztosítani kell a naplózást, a naplóállományok rendszeres mentését, elemzését.

Naplózható események

A Kórház információs rendszereiben bekövetkező események és problémák azonosítása érdekében a naplófájlok tartalmazzák a problémák megoldásához szükséges adatokat. A visszaélések felderítése érdekében a jogosult felhasználói tevékenységek és jogosulatlan tevékenységre irányuló kísérletek naplózásra kerülnek. A naplózás további célja, hogy a szerverek naplóállományainak elemzése során felszínre kerüljenek azok a biztonsági incidensek, amelyek a rendszer szempontjából problémákhoz vezethetnek.

Naplóbejegyzések tartalma

A Kórház szerverinek naplóbejegyzései az alábbi információkat rögzítik:

- Naplóbejegyzés típusa
- Az eseményt regisztráló szerver neve
- Az esemény naplózásának időpontja
- A módosítást kérő számítógép neve
- A módosítást kérő felhasználó neve
- Szolgáltatás kérés állapota
- A szolgáltatás kódja

Időbélyegek

A Kórház központi számítógépén a timestamp beállításaival készülnek az időbélyegek. A Time Szerver funkciót ellátó gépnek (APOLLÓ) az időszinkronizáció tekintetében a time.kfki.hu szervert kell alapul vennie.

Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédje a naplóbejegyzéseket és a napló-kezelő eszközöket a jogosulatlan hozzáférésektől, módosítástól, esetleges törlésektől.
A Kórház szerverén tárolt naplóinformációk adattartalmához a következő személyek kaphatnak betekintést:

- informatikai osztályvezető
- üzemeltetési rendszergazdák
- alkalmazás-üzemeltetési rendszergazdák
- informatikai biztonsági felelős

Naplóbejegyzések megőrzése

A Kórház a jogszabályi és szervezeten belüli információ megőrzési követelményeknek megfelelően a naplóbejegyzéseket 1 évig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

Naplógenerálás

A Kórház biztosítja, hogy a rendszerüzemeltetés során a levelező rendszer, web szerver, adatbázisok üzemelésével kapcsolatban olyan naplófájlok készüljenek és őrződjenek meg, amelyek segítségével a biztonsági események, felhasználói tevékenységek utólagosan is nyomon követhetők legyenek. A naplófájlok rendszeres átvizsgálásra kerülnek.
Az adatfeldolgozás és kezelés biztonságát sértő eseményeket, az esteleges rossz szándékú hozzáférési kísérleteket, illetéktelen adatfelhasználást naplózni kell.