Iktatószám: 588./2018.Kp.

Informatikai Biztonsági Szabályzat

Hatályos: 2019. január 01-jétől

Iktatószám: 588./2019.Kp.

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

HATÁLYOS: 2019. JANUÁR 01-JÉTŐL

		Dátum	Aláírás
Készítette:	Karis István informatikus	2018.12.21	
Ellenőrizte:	Bátori József IFO osztályvezető	2018.12.21.	
Jóváhagyta:	dr. Göböl Zsolt főigazgató	2018.12.21.	

SZENT RÓKUS KÓRHÁZ ÉS INTÉZMÉNYEI
1085 Bp. Gyulai Pál u.2.
főigazgató

Módosítások jegyzéke

Kiadás dátuma	**Kiadás módosítás oka, változás tartalma**	**Módosított terület**
2018. 12. 21.	1. kiadás	

Tartalom

1 Szabályozás célja

1.1. Az szabályzat alapvető célja, hogy az informatikai rendszer működtetése, üzemeltetése során biztosítsa az adatvédelem elveinek, az információbiztonság követelményeinek érvényesülését, meghatározza a Kórház felelősségi körébe tartozó információs rendszerek védelmének felelőseire, feladataira vonatkozó alapvető szabályokat.

1.2. A szabályzat célja továbbá, hogy a informatikai szolgáltatás területén biztosítsa:

a) az informatikára vonatkozó törvényi előírások érvényesítését,
b) a folyamatos informatikai üzembiztonság fenntartását,
c) az informatikai vagyon védelmét és megőrzését,
d) az informatikai hálózat integritásának védelmét,
e) vagyon- és tűzvédelmet,
f) a személyiség jogok védelmét, titokvédelmet,
g) a hozzáférési jogosultsági rendszer kialakítását, dokumentálását,
h) az adatfeldolgozások során az illetéktelen hozzáférésből eredő károk megelőzését,
i) az adatállományok épségének megőrzését, biztonságos mentését,
j) az alkalmazott szoftverek sértetlenségét, megbízható működését,
k) a keletkezett és felhasznált írásos dokumentumok megfelelő kezelését,
l) a szervezeti egységek irányító munkatársainak az informatikai biztonság tekintetében végzett feladatait, és felelősségét.

2 A szabályozás személyi és tárgyi és területi hatálya

2.1 A szabályzat személyi hatálya kiterjed:

a) a Szent Rókus Kórház és Intézményei valamennyi közalkalmazotti jogviszonyban álló munkavállalójára és az intézményben szerződés alapján tevékenységet végzőkre,
b) a Kórház elektronikus információs rendszerével, szolgáltatásaival szerződéses vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban együtt: harmadik személy vagy szerződött partner) a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján.

2.2 A szabályzat tárgyi hatálya kiterjed:

a) a Kórház tulajdonában, kezelésében lévő valamennyi elektronikus információs rendszerre és általuk keletkeztetett, feldolgozott, tárolt, továbbított valamennyi adatra és információra (függetlenül azok megjelenési formájától),
b) a Kórház szervezeti egységeinél az informatikai folyamatokban használt valamennyi dokumentációra,
c) a Kórház szervezeti egységeinél ideiglenesen használt, más szervezetek tulajdonát képező informatikai berendezésekre.

2.3 Területi hatály kiterjed a Kórház valamennyi épületére és telephelyére, távmunka esetén a távoli kapcsolódási végpont fizikai területére. Utóbbi esetben a távmunkát végző tartozik felelősséggel az adatvédelem, információbiztonság megteremtéséért.

2.4 Az IBSZ további hatálya

a) idegen vagy vegyes tulajdonú, illetve kezelésű eszközök, rendszerek használata során figyelembe kell venni a társszervezet ide vonatkozó rendelkezéseit és előírásait, illetve a megkötött és az érvényes megállapodásokat (pl.: a szakmai ellátásban a kórház területén közreműködő szervezetek eszközei, bérelt eszközök, informatikai infrastruktúra elemek, stb.);
b) az IBSZ azokat a szabályokat is tartalmazza, amelyeket alkalmazni kell az informatikai rendszerek fejlesztése, telepítése és üzemeltetése során, a kívánt biztonsági szint elérése és fenntartása érdekében.

3 Szabályozáshoz kapcsolódó fogalom-meghatározások

adat: az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre vagy feldolgozásra. Tények, fogalmak vagy utasítások formalizált ábrázolása, amely alkalmas az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra. A számítástechnikában adat a számítógépes állományok meghatározott része (minden, ami nem program) és mindaz, amivel a számítógépek a kommunikációjuk során foglalkoznak (kimenő és bemenő adat);

adatfeldolgozó: az a természetes vagy jogi személy, valamint jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi;

adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;

adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen az adatok 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 rögzítése;

adatkezelő: az a természetes vagy jogi személy, valamint 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 adatfeldolgozóval végrehajtatja;

adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás, a keletkező dokumentumok nyilvántartása;

adatállomány: az elektronikus információs rendszerben logikailag összetartozó, együtt kezelt adatok;

adatátvitel: az adatok elektronikus információs rendszerek, rendszerelemek közötti továbbítása;

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele; adatvédelem: az adatkezelés során érintett természetes személyek jogainak és érdekeinek védelmére és az adatkezelés során felmerülő eljárásokra vonatkozó szabályozások és eljárások;

alkalmazás: informatikai program (szoftver), melynek feladata valamely informatikai feladat elvégzése;

alkalmazásfelelős: az alkalmazásokban meghatározott adminisztrátori funkciók (jogosultság beállítás, alkalmazás működési paramétereinek beállítása, adatszótárak kezelése stb.) használatára jogosult személy, akit az adatgazda jelöl ki;

backdoor (hátsóajtó) program: olyan, a felhasználó számára általában nem látható elem, amely telepítése után teljes kontrollt adhat a számítógép felett egy vagy több távoli személynek; behatolás: védett rendszerbe jogosulatlan belépés a védelem megkerülésével vagy védelmi hiba kihasználásával;

bejelentkezés: a felhasználó által kezdeményezett olyan logikai kapcsolat, amelynek eredményeképpen az elektronikus információs rendszer funkcióinak használata lehetővé válik; 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, rendelkezhetnek a felhasználásáról;

biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese;

biztonsági policy: csoportházirend, biztonsági beállítások összessége, mely meghatározza a rendszer működésének körülményeit;

biztonsági mechanizmus: valamely biztonsági követelmény(eke)t megvalósító eljárás, módszer vagy megoldási elv, amely lehet számítástechnikai műszaki tartalmú is;

cégkapu: a Központi Elektronikus Szolgáltató Rendszer (központi rendszer, KR) része. Kormány által kötelezően nyújtott azonosítási és biztonságos kézbesítési szabályozott elektronikus ügyintézési szolgáltatás. A cégkapun keresztül az igénybevevő szervezetek hitelesen tudnak fogadni elektronikus üzeneteket, illetve a hivatalok elektronikus üzenetei a hitelesen azonosított ügyfelekhez (állampolgár) vagy csatlakozott hivatalhoz eljuttathatók;

EIRF: Elektronikus Információs Rendszer biztonságáért Felelős személy

elektronikus aláírás: az elektronikus információs rendszerben kezelt adathoz csatolt, kódolással előállított jelsorozat, amely az adat, illetve az eljáró személy azonosságának, hitelességének és sértetlenségének bizonyítására használható;

elektronikus információs rendszer: az adatgazda által, adott cél érdekében az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

elektronikus postafiók: a munkahelyi feladatok korszerű és hatékony ellátása érdekében az elektronikus levelek fogadása, küldése valamint továbbítása céljából a Kórháznak és a szervezeti egységeknek hivatalos, a kormánytisztviselőknek, állami tisztviselőknek, ügykezelőknek és munkavállalóknak személyhez kötött elektronikus üzenetkezelő rendszere;

elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes, ideértve az elektronikus küldeményt és az elektronikus levelet is;

elektronikus küldemény: a Biztonságos Elektronikus Dokumentumtovábbító Szolgáltatás útján küldött, illetve érkezett elektronikus űrlap(ok) és az azokhoz csatolt egyéb elektronikus dokumentum(ok) és hivatalos iratok;

elektronikus levél: a központi rendszeren kívüli számítógépes hálózaton keresztül, egyedi levelezési címek között levelezőprogram segítségével küldhető és fogadható adategyüttes. Lehetnek hivatalos és magánjellegűek;

érzékeny adat: olyan adat, amely az információbiztonság szempontjából a sérülékenység és a fenyegetettség ténye alá esik (pl. a felhasználás folyamatainak leírása, az eljárás, az adatszerkezetek vagy az engedélyezési folyamatok);

felhasználó: az a Szent Rókus Kórház és Intézményeivel bármilyen jogviszonyban álló munkatárs, vagy külső személy, aki a munkavégzés során használja a Szent Rókus Kórház és Intézményei által rendelkezésére bocsátott informatikai eszközöket;

felhasználói leírás: tartalmazza az alkalmazás (szoftver) használatához, működtetéséhez, kezeléséhez, felhasználásához szükséges feltételeket és ismereteket;

felhasználói rendszer: olyan alkalmazás, amelyet a felhasználó saját speciális céljai elérése érdekében vezet be, és amely a hardver- és az üzemi rendszer, rendszerprogramok funkcióit használja;

felhő (cloud computing): A szolgáltatás azt jelenti, hogy olyan programokkal, fájlokkal dolgozunk, melyek fizikailag nem a saját munkaállomásunkon, hanem egy ismeretlen helyen vannak, valahol a „felhőben". Ezeket a szolgáltatásokat a felhasználók hálózaton keresztül érhetik el, publikus felhő esetében az interneten keresztül, privát felhő esetében a helyi hálózaton vagy az intraneten; fenyegetettség: olyan állapot, amelyben az erőforrások felfedésre, módosításra vagy elpusztításra kerülhetnek;

funkcionalitás: az informatikai rendszerelem (ideértve az adatot is) tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a felhasználói céloknak megfelel és használható; gyenge pont: az informatikai rendszerelem olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;

hálózat: informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;

hálózati végpont: Az informatikai eszközök informatikai hálózathoz való csatlakozását szolgáló fizikai és logikai csatlakozási pont;

hardver: az informatikai rendszer eszközei, fizikai elemei;

hazatelefonálás: Az operációs rendszer, illetve szoftver – a fejlesztője által meghatározott szerverekre – háttérben történő adatküldései, amelyek tartalmazhatják az adott dokumentumot, azok metaadatait, a billentyűzet-leütéseket (jelszavakkal együtt), a beviteli eszközök további telemetriai és biometrikus adatait stb., amelyek biztonsági kockázatot jelentenek;

helpdesk alkalmazás: A felhasználó eszközeinek és programjainak hibája esetén ezek jelzésére és követésére létrehozott informatikai alkalmazás;

helyreállítás: a katasztrófa következtében megsérült erőforrások eredeti állapotának biztosítása eredeti helyen;

hitelesség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik;

honlap: a weben megjelenő egyedi szolgáltató rendszer, amely információkat tartalmaz az adott helyről, szervezetről, és amelyen megtalálhatók a további kapcsolódások, oldalak kiindulópontjai. hozzáférés: olyan eljárás, amely valamely elektronikus információs rendszer használója számára elérhetővé tesz a rendszerben adatokként tárolt információkat; illetéktelen személy: aki az adat megismerésére nem jogosult;

IBSZ: informatikai Biztonsági Szabályzat

IFO: Informatikai és Finanszírozási Osztály

információvédelem: az elektronikus információs rendszerekben kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme;

informatikai eszköz: az információs tevékenységek végrehajtását, folyamatát támogató, vagy megvalósító eszköz;

informatikai infrastruktúra: mindazon hardver- és szoftvereszközök, elektronikus információs rendszerek, hálózatok, alkalmazások, programok összessége, amelyek segítik és kiszolgálják a szervezet kommunikációs, adatfeldolgozó és adatátviteli tevékenységét;

informatikai központ: informatikai központoknak minősülnek azon helyiségek, melyek működő szerverek és hálózati elosztó elemek (router, switch) elhelyezésére és működtetésére szolgálnak; informatikai rendszer: A hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat- illetve információfeldolgozás különböző feladatainak teljesítésére alkalmazunk.

Internet: nyílt hálózatok (számítógépek és adatátviteli kapcsolóeszközök) illesztésével létrejött világméretű számítógépes metahálózat, amely a használói részére információs és kommunikációs lehetőséget kínál;

internet kijárat: zárt hálózatok azon csomópontja, amely lehetőséget biztosít az internet információs és kommunikációs szolgáltatásainak elérésére. Ez a csomópont magában foglalja az eléréshez szükséges vonalat, ha ez analóg vonal, akkor a digitális átvitelhez szükséges modemet, a forgalomirányítást végző routert és a belső hálózat védelmét biztosító tűzfalat;

internet végpont: az internet használatára alkalmassá tett (személyi) számítógép. Az alkalmassá tétel történhet műszaki bővítéssel (modem beépítésével vagy csatlakoztatásával) és/vagy speciális hálózati szoftverek telepítésével;

intranetes portál: a Szent Rókus Kórház és Intézményei internetes szabványokra épülő, zárt, belső használatú portálja, amely belső információk tárolására, továbbítására, elérésére szolgál;

image: adatállományokról, programokról, rendszerekről készített mentési állomány digitális bitkép formájában;

IT: Information Technology, azaz információtechnológia;

jelszó: védett karakterfüzér, amelyet a felhasználói névvel együtt használva a belépni szándékozót azonosítja;

katasztrófa-elhárítási terv: az elektronikus információs rendszer rendelkezésre állásának megszűnése vagy nagymértékű csökkenése utáni visszaállításra vonatkozó terv;

kiesési idő: az információrendszer leállásától a következő elérési lehetőségig eltelő idő;

kijelölt informatikus: AZ IFO által az adott munkaterületre az informatikai vagy speciális munkafeladat ellátására kijelölt informatikus;

kliens gép: számítógép, munkaállomás, amelyen keresztül egy szerverről kérhetünk információt (adatokat), szolgáltatásokat;

kockázat: a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata;

kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

kódolás: nyílt üzenet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A kódolás eredménye a titkosított üzenet;

kriptográfia: mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak a kutatása, alkalmazása, amelyek az információ bizalmasságát, hitelességét vagy sértetlenségét hivatottak megvédeni;

kulcs: a kriptológiában a kódolás és a megfejtés műveleteihez használt szimbólumok sorozata, az adatbázis-kezelésben egy rekord vagy rekordcsoport azonosítója, a mechanikai védelemben a zárak nyitásához és zárásához használt eszköz;

kulcsmenedzsment: a kriptográfiában a kódolás és a megfejtés műveleteihez használt kulcsok előállítása, tárolása, szétosztása, törlése, archiválása és alkalmazása és ezek szabályrendszere; megoldás: a kódolt üzenet legális címzettje által, az eljárás ismeretében az eredeti üzenet visszaállítása;

megszemélyesítés: egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel;

minősítés: az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik;

mobil eszközök: azok a számítógépek, amelyek hordozhatóak (pl. laptop/notebook, PDA, tablet stb.);

munkaállomások: Azok a számítógépek, amelyeken az egyes felhasználók dolgoznak. Itt fut az alkalmazás, ezek a gépek használják a hálózat erőforrásait (tárolóterület, nyomtató, szkenner stb.);

működésfolytonosság: az elektronikus információs rendszer üzemi működése folytonosságának azon szintje, amely során a kiesési kockázati szint a szervezet számára elviselhető; működtetés: az elektronikus információs rendszer funkcióinak rendeltetésszerű használata, az elektronikus információs rendszer adatainak kezelése (létrehozás, módosítás, törlés, lekérdezés, adattovábbítás stb.);

Nemzeti Távközlési Gerinchálózat (NTG): a kormányzati szerveket összekötő országos telekommunikációs hálózat;

program: a számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata;

rack szekrény: informatikai berendezések elhelyezésére szolgáló zárt fémszekrény, melyekben a hálózat vagy a kommunikáció működéséhez szükséges elemek találhatóak;

rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

rendszerelemek: az adatokat körülvevő, az elektronikus információs rendszer részét képző elemek, amelyek a következő rendszerelem-csoportokba oszthatók:

az elektronikus információs rendszer környezetét alkotó infrastruktúra,

o az elektronikus információs rendszer hardverelemei,

o az elektronikus információs rendszer szoftverelemei,

o az elektronikus információs rendszer kommunikációs elemei, o az adathordozók,

o az input és output dokumentumok, az elektronikus információs rendszerre vonatkozó dokumentációk,

o az elektronikus információs rendszerben részt vevő emberi erőforrások;

rendszerszintű beállítások: az operációs rendszerek vagy alkalmazások alapvető működését befolyásoló vagy szabályozó beállításai. A módosítás lehetőségei rendszerint csak megfelelő rendszergazdai jogosultsággal érhetők el;

rendszergazda: az elektronikus információs rendszerek üzemeltetését végző szakember, akivel szemben alapvető feltétel, hogy az informatikai vezető által előírt képesítési követelményeknek megfeleljen;

rendszerprogram (rendszerszoftver): az operációs rendszer részeként futó vagy operációs rendszer környezetben telepített általános célú program;

router (útvonal irányító): olyan eszköz (számítógép), mely a hálózati kapcsolatok felépülését a központ, és/vagy végberendezés között kialakítandó kapcsolatok útvonalának kijelölésével irányítja, biztosítva a csatlakoztatott eszközök közötti adatcsomagok áramlását.

sebezhetőség: a veszélyforrás képezte sikeres támadás bekövetkezése esetén az erőforrások sérülésének lehetősége;

Single sign-on (SSO): webes rendszerek egyszeri bejelentkezési módszere, amely olyan speciális formája a szoftveres azonosításnak, ami lehetővé teszi a felhasználó számára, hogy egy adott rendszerbe való belépéskor mindössze csak egyszer azonosítsa magát és ezután a rendszer minden erőforrásához és szolgáltatásához további authentikáció nélkül hozzáfér;

SSL (Secure Socket Layer): a Netscape által kifejlesztett nyílt szabvány ajánlásbiztonságos kommunikációs csatorna létrehozására a továbbított adatok védelme érdekében;

szerver: kiszolgáló gépek, általában nagy teljesítményű és tárolókapacitású, folyamatos üzemű számítógépek, amelyek a hálózatba kapcsolt többi gép számára szolgáltatásokat nyújtanak; szoftver: Az informatikai rendszer olyan logikai része (alkalmazás), amely a működtetés vezérléséhez szükséges. Ide számítanak a különféle használati/üzemeltetési utasítások, leírások is;

támadás: védett érték megszerzésére, megsemmisítésére, károkozásra irányuló cselekmény. Támadás alatt nem csak a személyek, szervezetek által elkövetett támadásokat, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is értjük, amely támadások legtöbbször nem közvetlenül érik a védett értéket, hanem a körülményektől függő támadási útvonalon zajlanak le; távmunka: olyan munkavégzés, amely a szervezet épületén kívül történik;

teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

trójai program: olyan program, ami mást tesz a háttérben, mint amit a felhasználónak mutat, azaz igyekszik elleplezni valódi – általában káros – tevékenységét. (A trójai falóról nevezték el.); tűzfal: a hálózat(ok) illetéktelen hozzáférés, behatolás elleni szűrését, védelmét biztosító eszközökből álló rendszer;

tűzszakasz: az építmény vagy szabadtér tűzvédelmi szempontból meghatározott olyan önálló egysége, amelyet a szomszédos egységektől – meghatározott éghetőségű és tűzállósági határértékű – tűzgátló szerkezetek, és a jogszabályban előírt tűztávolságok választanak el; üzletmenetfolytonosság-tervezés: az elektronikus információs rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek;

üzemeltetés: az elektronikus információs rendszerek működőképességét biztosító informatikai környezet létrehozása, karbantartása;

vírus: olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg mutálja is önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás" hatású kódja is elindul. Többnyire komoly károkat okoz, adatot töröl, formázza a merevlemezt, vagy adatállományokat küld szét e-mailben;

warez-oldal: illegális szoftvermásolatok (az eredeti programba épített másolásvédelmet vagy regisztrációt kijátszva/semlegesítve, és ez által bárki számára használhatóvá téve azt) közzétételére fenntartott internetes oldal – warez-site – ahonnan e programok ingyenesen letölthetők.

Web (World Wide Web, WWW): nyílt dokumentumszerkesztési és dokumentum-átviteli eljárás. Interneten elérhető, hypertext kapcsolatra épülő információs rendszer, amely a honlapokhoz tartozó címek alapján ér el (média) dokumentumokat és (média)állományokat;

VPN: (Virtual Private Network) virtuális magánhálózat;

4 Szabályozáshoz kapcsolódó külső és belső minőségirányítási dokumentumok

MSZ EN ISO/IEC 27001:2014

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról,

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról

249/2017. (IX. 5.) Korm. Rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól

246/2015. (IX. 8.) Korm. Rendelet az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól

301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról

233/2013. (VI. 30.) Korm. Rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus

információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

SZMSZ

Adatvédelmi Szabályzat

Informatikai Biztonsági Stratégia

Informatikai Biztonsági Politika

MF-02 Minőségirányítási dokumentumok készítése, módosítása és kezelése, külső dokumentumok figyelemmel kísérése

Munkaköri leírások

5 A szabályozás leírása

A szabályozás elkészítéséért, karbantartásáért és működtetéséért a Informatikai és Finanszírozási osztály vezetője a felelős, valamint mindazok felelősek a működtetésért, akik használják a Szent Rókus Kórház és Intézményei informatikai rendszerét.

6 Alapelvek

A Szent Rókus Kórház és Intézményei dolgozója az információvédelem területén az adott helyzetben általában elvárható magatartást köteles tanúsítani és tartózkodni minden károkozó tevékenységtől. Az informatikai eszköz használója csak az a Szent Rókus Kórház munkatársa lehet, aki a munkavégzéshez szükséges mértékű informatikai ismeretekkel rendelkezik, nyilatkozott az e szabályzatban foglaltak tudomásul vételéről, és a vezetője engedélyével hozzáférési jogosultságot kapott a Szent Rókus Kórház elektronikus információs rendszereihez.

Az elektronikus információs rendszer vagy eszköz működtetése során a munkaköri leírásban el kell különíteni a jogköröket és a feladatköröket az egyes személyek között annak érdekében, hogy a személyes felelősség megállapítása mindenkor biztosított legyen.

Az elektronikus információs rendszert úgy kell kialakítani, hogy biztosított legyen a megbízható működés, az egyes alrendszer vagy rendszerelem funkcionalitásának megfelelő zavartalan és folyamatos működése.

A Szent Rókus Kórház és Intézményei objektumaiban a Szent Rókus Kórház és Intézményei számára létrehozott logikai hálózathoz csatlakozó vagy a Szent Rókus Kórház és Intézményei által engedélyezett hálózatba nem kötött eszközök (a továbbiakban: eszközök) rendeltetésszerűen, munkavégzés céljából, a Szent Rókus Kórház és Intézményei érdekeinek szem előtt tartásával, a Szent Rókus Kórház és Intézményei által meghatározott módon, a felhasználó felelősségére használhatóak. Az eszközöket ettől eltérő célra használni nem szabad.

A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres vagy szoftveres módosítás.

A Szent Rókus Kórház munkatársak a Szent Rókus Kórház és Intézményei hálózati alkalmazásaihoz és az elektronikus információs rendszerekhez a munkájuk elvégzéséhez szükséges mértékű hozzáférést kapnak.

A felhasználó csak a saját azonosítójával jelentkezhet be a Szent Rókus Kórház és Intézményei hálózatára és másnak a saját bejelentkezési hozzáférését nem adhatja át, nem teheti lehetővé, hogy mások hozzáférjenek.

A nem Szent Rókus Kórház és Intézményei tulajdonban álló, idegen, információs, számítástechnikai és telekommunikációs eszközt engedély nélkül a Szent Rókus Kórház és Intézményei informatikai infrastruktúrájához csatlakoztatni nem szabad.

A felhasználó köteles a biztonságot támogató programok használatára. Az általa használt munkaállomásról a programot nem törölheti le, nem kapcsolhatja ki.

A felhasználó kizárólag munkavégzési célú programokat használhat.

7 Intézményi szabályozás

A Szent Rókus Kórház és Intézményei főigazgatójának feladata az elektronikus információs rendszerek, valamint az azokban kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának zárt, teljes körű és folytonos, a kockázatokkal arányos védelme. Ennek érdekében a szükséges utasítások, rendelkezések, valamint szabályzatok kiadása, továbbá irányítás és együttműködés az informatikai rendszerek üzemeltetéséért felelős vezetővel, valamint az Elektronikus Információs Rendszer biztonságáért Felelős személlyel (a továbbiakban: *EIRF*) a védelem adminisztratív, logikai és fizikai intézkedéseinek végrehajtásában. A feladat- és hatáskörökhöz mérten biztosítja a szükséges anyagi, technikai, információs és emberi erőforrásokat.

A Szent Rókus Kórház és Intézményei tulajdonában és használatában levő adatvagyonról leltárt kell készíteni, az informatikai elemeket biztonsági osztályokba kell sorolni bizalmasság, sértetlenség és rendelkezésre állás szempontjából.

Jelen szabályzatot az Informatikai és Finanszírozási Osztály (továbbiakban: IFO) vezetője köteles felülvizsgálni és szükség esetén módosítását kezdeményezni:

Minden olyan szervezeti változás esetén, amely a hivatkozott szervezeti egységek bármelyikének megszűnésével vagy jelentős átalakulásával jár;

a) Súlyos informatikai biztonsági események („incidensek") után, az esemény tanulságait figyelembe véve;

b) Minden olyan jogszabályváltozás esetén, amelyek a benne foglaltak érvényességét módosíthatják.

A szabályzat alkalmazásáért és betartásáért a kórházi szervezet minden egységének vezetője és minden további informatikai eszközt használó felelősséggel tartozik.

Az IBSZ személyi hatálya alá tartozó valamennyi személynek ismernie kell azokat a követelményeket és feladatokat, amelyeket az IBSZ számára meghatároz.

8 Az informatikai biztonság általános szabályai

A Szent Rókus Kórház és Intézményei területén végzett minden tevékenység (például építési és karbantartási munka, beteg- és ügyfélforgalom bonyolítása, üzemeltetési feladatok ellátása, postaszolgáltatások stb.) során figyelemmel kell lenni az IBSZ betartására és betartatására, az IT biztonság követelményeinek maximális fenntartására.

A Szent Rókus Kórház és Intézményei elektronikus információs rendszereinek meg kell felelniük a rendelkezésre állás, a sértetlenség, a bizalmasság, a megbízhatóság alapelveinek.

8.1 Rendelkezésre állás

Biztosítani kell a szolgáltatások és adatok elérhetőségét az arra jogosult felhasználók számára, továbbá védelmet kell biztosítani a jogosulatlan hozzáféréstől és adatmódosítástól, törléstől, illetve a szolgáltatás elérhetőségének megakadályozásától.

AZ IFO feladata biztosítani az informatikai rendszerek folyamatos rendelkezésre állását az alábbi eszközök felhasználásával:

a) rendszeres adatmentések és szoftvertelepítő készletek megfelelő biztosításával és megfelelő tárolásával;

b) tartalék eszközök és alkatrészek biztosításával;

c) helyreállítási módszerleírások, vészforgatókönyvek naprakész biztosításával.

8.2 Sértetlenség (integritás)

Az adatintegritás biztosítja, hogy adat ne módosuljon nem engedélyezett (nem tervezett) módon a tárolás, feldolgozás, adatátvitel során. A rendszerintegritás követelménye biztosítja, hogy a rendszer a megvalósított funkciót engedélyezetten, manipulációtól mentesen hajtsa végre.

Számítógép- vagy programhibából eredő adatvesztés gyanúja esetén – adatfeldolgozás szüneteltetése mellett – az EIRF-t haladéktalanul értesíteni kell. Az értesítés módja személyes, vagy telefonos értesítés, vagy elektronikus úton tett bejelentés. A probléma tisztázása után az informatikus útmutatása szerint kell folytatni az adatrögzítést, illetve adatfeldolgozást.

Az alkalmazások használata során az adatok felvitelét, módosítását, törlését kizárólag az IFO által elfogadott és biztosított, a feldolgozásra készült programmal – szigorúan követve a felhasználói dokumentáció útmutatását – lehet elvégezni.

Az alkalmazásokhoz és hálózati mappákhoz (könyvtárakhoz) való hozzáférés (jogosultságok) dokumentált engedélyeztetése és érvényesítése során gondoskodni kell arról, hogy jogosulatlan felhasználó azokat ne módosíthassa, és ne törölhesse, manipulálhassa azt.

A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sértetlenségét.

8.3 Bizalmasság

Bizalmas, vagy magántermészetű információ nem juthat jogosulatlan személy tudomására. A bizalmasság követelménye az adat tárolására, feldolgozására, átvitelére egyaránt vonatkozik.

A Kórház területén végzett minden betegellátási- és ügyfélforgalmi tevékenység során szem előtt kell tartani az ellátottak és a munkatársak adatainak, információinak, az ellátás és az ügymenet elemeinek bizalmas jellegét, ezért az informatikai infrastruktúrát és környezetet ennek megfelelően kell kialakítani.

8.4 Megbízhatóság

A különböző biztonsági intézkedések az irányítási, technológiai, működési, vezérlés területén megfelelően működnek, ha védik a rendszert és az általa feldolgozott adatot.

A megbízhatóság követelménye akkor teljesül, ha:

a) a kívánt funkció jelen van és pontosan megvalósított;

b) megfelelő védelem kerül alkalmazásra a nem szándékos hibák ellen;

c) megfelelő védelem van a szándékos hibák (behatolás stb.) ellen.

9 Szervezeti biztonság

9.1 Az információbiztonsági felügyeleti tevékenység

Az elektronikus információs rendszerek védelméért felelős vezető az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 11.pontja alapján a Szent Rókus Kórház és Intézményei főigazgatója, aki ezen feladatkörében a következő feladatokat látja el:

a) tervezi, szervezi, irányítja, koordinálja és ellenőrzi a Kórházban üzemeltetetett elektronikus információs rendszerek védelmével összefüggő tevékenységeket, megteremti ezek jogszabályokkal való összhangját;
b) meghatározza a szervezet felkészültségét az Ibtv.-ben meghatározott biztonsági feladatok kezelésére, ez alapján intézkedik a szervezet biztonsági szintjének besorolásáról;
c) kinevezi az az elektronikus információbiztonsági felelőst (EIRF)
d) közvetlenül irányítja és felügyeli az elektronikus információbiztonsági felelős tevékenységét;
e) ellátja a helyi információbiztonsági felügyeleti tevékenységet, gondoskodik az informatikai biztonsági szabályzat elkészítéséről, naprakészen tartja a Szent Rókus Kórház és Intézményei informatikai biztonsági szabályzó rendszerét, kockázatelemzéseket végez, gondoskodik a biztonsági események kezeléséről;
f) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról;
g) gondoskodik arról, hogy az elektronikus információs rendszer létrehozásában, üzemeltetési, javítási, adatkezelési, adatfeldolgozási feladatokban részt vevő külső közreműködők szerződéseiben szerepeljenek a szabályzatban előírt biztonsági intézkedések;
h) felügyeli a kórházi egységek informatikai, telekommunikációs és biztonságtechnikai fejlesztéseit, üzemeltetési tevékenységét;
i) közreműködik a személyes és különleges adatok tárolásával, továbbításával kapcsolatos szolgáltatások működtetésében, felügyeletében; végzi a személyes és különleges adatok védelmével kapcsolatos információbiztonsági tevékenységeket, rendszer-technológiai szempontból érvényesíti a differenciált hozzáféréssel kapcsolatos követelményeket;
j) irányítja a Szent Rókus Kórház és Intézményei egységek statisztikai adatgyűjtésének és adatszolgáltatásának informatikai, telekommunikációs és biztonságtechnikai támogatását;
k) az informatikai infrastruktúra üzemeltetés során biztonsági esemény vagy kritikus hibajavítás esetén dönt az infrastrukturális alrendszerek, szolgáltatások ideiglenes vagy időszakos szüneteltetéséről, felfüggesztéséről;
l) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

9.2 Az Elektronikus Információs Rendszer biztonságáért Felelős EIRF) feladatai

Az elektronikus információs rendszer biztonságáért felelős személy a Szent Rókus Kórház és Intézményeiben a Főigazgató által írásban megbízott személy, aki az Ibtv. 13. §-ában

foglaltak szerint összefogja és koordinálja az elektronikus információs rendszerek védelmének feladatait. Elvégzi az informatikai biztonsággal kapcsolatos, tervezéssel, szervezéssel, ellenőrzéssel, elemzéssel véleményezéssel kapcsolatos feladatokat:

a) munkája során kapcsolatban áll a Kórház szervezeti egységeivel, az érdekelt kereskedelmi, szállító és szolgáltató cégek megbízottjaival;
b) amennyiben új fenyegetettséget észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését;
c) ellenőrzi és értékeli a naplókat, ezek alapján értékeli az esetleges támadási kísérletet, illetéktelen adatfelhasználást;
d) kivizsgálja a biztonsággal összefüggő eseményeket és javaslatot tesz a főigazgatónak a további intézkedésekre, esetleges felelősségre vonásra;
e) elemzi és ellenőrzi az informatikai rendszerek jogosultsági rendszerét;
f) ellenőrzi és véleményezi a biztonsági rendszer elemeit, a rendszergazdák, felhasználók tevékenységét. E feladatkörében valamennyi rendszerelem megtekintésére, vizsgálatára jogosult;
g) együttműködve a szervezeti egységek vezetőivel előkészíti és karbantartja az IBSZ-t és a hozzá kapcsolódó eljárásrendeket, módszertani útmutatókat;
h) megszervezi az információs rendszereket használó Kórházi munkatársak, és külső szereplők rendszeres és soron kívüli oktatását;
i) megteszi a külső szervezetek számára a szakmai nyilatkozatokat és tájékoztatást nyújt;
j) elvégzi az információs rendszerek biztonsági osztályba sorolását;
k) meghatározza, és ellenőrzi az elektronikus információs rendszerek környezetének fizikai, mechanikai, elektronikai védelmét;
l) a mentéssel kapcsolatos adatlapokat és nyilvántartást legalább évente egyszer szúrópróbaszerűen ellenőrzi;
m) olyan vírusfenyegetettség esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet – a belső hálózaton (intraneten) kívül eső elektronikus levélforgalom ideiglenes leállításáról gondoskodik, és erről a Kórházi munkatársakat tájékoztatja;
n) az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a távmunka igénylések jogosságát és megfelelőségét, valamint a dokumentációt.

9.3 Az informatikai infrastruktúra üzemeltetésért felelős vezető feladatai

Az informatikai rendszerek üzemeltetéséért a Szent Rókus Kórház és Intézményeiben a Informatikai és Finanszírozási Osztály vezetője (továbbiakban: IFO vezető) felel. Elvégzi az üzemeltetéssel, valamint az informatikai műszaki fejlesztéssel kapcsolatos feladatokat.

a) munkája során kapcsolatban áll a Kórház szervezeti egységeivel, az érdekelt kereskedelmi, szállító és szolgáltató cégek megbízottjaival;
b) amennyiben új fenyegetettséget észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését;
c) javaslatot tesz a védelmi intézkedések módjára, értékeli és véleményezi az informatikusok, felhasználók biztonságra vonatkozó javaslatait;

d) közreműködik a biztonsági rendszer elemei, a rendszergazdák, a felhasználók tevékenysége ellenőrzésében és véleményezi azokat. E feladatkörében valamennyi rendszerelem megtekintésére, vizsgálatára jogosult.

9.4 *Az informatikai biztonsági megbízott (továbbiakban: IBM) feladatai*

Az elektronikus információs rendszerek üzemeltetését és az információbiztonsági felelős munkájának támogatását a rendszergazdák végzik. AZ IFO, mint szervezeti egység vonatkozásában ki kell jelölni az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyt, mint informatikai biztonsági megbízottat. Az informatikai biztonsági megbízottat az információbiztonsági felelős javaslatára a Főigazgató jelöli ki. Feladatait a munkaköri leírásában rögzíteni kell.

Az informatikai biztonsági megbízott (IBM) részt vesz a biztonsággal kapcsolatos vezetői döntések előkészítésében, hatáskörében intézkedik, vagy javaslatot tesz a hibák kijavítására. Munkája során szorosan együttműködik a biztonság megvalósításában résztvevő informatikai és egyéb szakemberekkel.

Feladatai továbbá:

- közreműködik az ellenőrzés módszereinek és rendszerének kialakításában és annak működtetésében. Véleményezi az IBSZ-t, javaslatot tesz annak módosítására;
- az informatikai rendszert üzemeltető vezetővel és az információbiztonsági felelőssel
- együttműködve közreműködik a biztonsággal kapcsolatban készítendő tervek és szabályzatok előkészítésében;
- informatikai biztonsági szempontból ellenőrzi a hozzá tartozó informatikai rendszer szereplőinek tevékenységét;
- az informatikai rendszerben észlelhető rendkívüli eseményeket, (pl.: esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést) jelzi az EIRF-nek;
- új informatikai szerverterem tervezése és kialakítása során ellenőrzi az IBSZ-ben megfogalmazott, a helyiségek fizikai paramétereire vonatkozó követelmények kielégítését és a meglevő helyiség paramétereinek értékét;
- ellenőrzi az informatikai szerverterembe történő beléptetési eljárást és a belépő személyek körének jogosságát;
- ellenőrzi a beléptető rendszerek kódjának szükség szerinti cseréjét;
- ellenőrzi a riasztórendszerek meglétét és megfelelő működését;
- az SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét;
- ellenőrzi a fejlesztő rendszerek elkülönítésének megfelelőségét az éles rendszertől;
- közreműködik az informatikai szerverterem, eszközök és az infrastruktúrát érintő karbantartási feladatok felügyeletében;
- közreműködik a beruházások, fejlesztések, az üzemvitel informatikai biztonsági szempontú felügyeletében, illetve javaslatot tesz az ilyen szempontú beruházásokra, fejlesztésekre;
- az új biztonságtechnikai eszközök és szoftverek tesztelésére ajánlást ad;
- ellenőrzi az egyes felhasználói gépek hardverkonfigurációját, és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverek listájával;

- ellenőrzi, hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott (a jogosultsági nyilvántartásban is szereplő) jogosultságokkal;
- ellenőrzi, hogy a javításra kiszállított eszközökön adat ne kerülhessen ki, illetve a javítást végző rendelkezzen aláírt titoktartási nyilatkozattal;
- ellenőrzi az adathordozók selejtezését/megsemmisítését, beleértve a számítógépek, nyomtatók, multifunkciós eszközök stb. beépített adathordozóin lévő adatok végleges megsemmisítését is;
- ellenőrzi és lehetőség szerint kerüli az ún. „hazatelefonálós" operációs rendszerek, szoftverek telepítését, alkalmazásuk esetén viszont kifejezetten tiltja ezen adatforgalmakat (Pl.: Windows 10, Adobe Acrobat Reader által megnyitott PDF állományok automatikus, ellenőrizetlen publikus felhőbe történő feltöltése, Google ilyen irányú szolgáltatásai stb.);
- közreműködik a publikálásra szánt dokumentumok rejtett metaadatainak, szövegeinek, korábbi szövegállapotainak, magánjellegű információinak törlésében;
- értékeli a rendszer eseménynaplóit;
- ellenőrzi a víruskereső programok használatát;
- ellenőrzi a dokumentációk meglétét és megfelelőségét (teljes körű, aktuális);
- ellenőrzi, hogy a vonatkozó informatikai biztonsági követelményeket a rendszerek a fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e;
- amennyiben új fenyegetéseket észlel, vagy hatékonyabb biztonsági intézkedések megtételét tartja szükségesnek, kezdeményezi a védelem erősítését;
- az adott szakterületek vezetőivel egyeztetve közreműködik az egyes feladatkörökhöz tartozóan az informatikai biztonsággal kapcsolatosan elsajátítandó ismeretek körének meghatározásában, és ellenőrzi az elsajátítás tényét;
- javaslatot tesz informatikai biztonságot erősítő továbbképzésre;
- az IBSZ évenkénti felülvizsgálatakor javaslatot tesz a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások miatt szükségessé váló módosításokra;
- javaslattételi joga van a fokozott és kiemelt védelmi osztályba sorolt informatikai rendszerek hozzáférési jogosultságainak kiadásában;

9.5 *Szervezeti egységek vezetője*

a) a szervezeti egység munkatársának felvétele, távozása, vagy munkakör változása, intézményen belüli áthelyezés esetén - amelyet a munkáltató jóváhagyásával végezhet - értesíti a változásról az IFO osztályvezetőt;

b) gondoskodik arról, hogy a szervezeti egység munkatársai megismerjék, és munkavégzésük során alkalmazzák az IBSZ-t;

c) ellenőrzi, hogy a szervezeti egység munkatársai betartják-e az IBSZ-t;

d) informatikai kérdésekben dönt az IBSZ-ben részére delegált területeken (igénylések, engedélyek stb.);

e) a munkavégzés során a rábízott eszközöket, szoftvereket felelősséggel, és az előírások, leírások, utasítások szerint használja és megőrzi;

f) az IBSZ-t megismeri és betartja és betartatja;

g) részt vesz az informatikai oktatásokon;

h) a számítógépes munkavégzése során tiszteletben tartja a felhasználói csoportjára vonatkozó szabályokat és korlátozásokat, valamint a számítógépére megállapított házirendet;

i) a számítógépes rendszerekhez használt hozzáféréseit biztonságos módon megőrzi, a hozzáférésével elkövetett visszaélésekből és károkból származó következményekért a jogszabályokban rögzített mértékű felelősséggel tartozik;

j) jelzi az információbiztonsággal kapcsolatos észrevételeit;

k) informatikai segítséget kér, ha olyan jellegű feladatot kell ellátnia, amelyhez nincs meg a megfelelő informatikai tapasztalata;

l) a munkájához szükséges eszközöket, alkalmazásokat és szolgáltatásokat a szervezeti egysége vezetőjének engedélyével igényelheti;

m) a publikálásra szánt dokumentumok rejtett meta-adatait, szövegeit, korábbi szövegállapotait, magánjellegű információit törli, vagy ehhez informatikus közreműködését kéri;

n) gondoskodik a szervezeti egységben keletkezett elektronikus dokumentumok, rendszeres (napi), (új dokumentum keletkezését követően, vagy meglévő dokumentum változása után) mentéséről, archiválásáról.

9.6 Műszaki osztály vezetője

a) biztosítja az informatikai eszközök és berendezések megfelelő működéséhez szükséges fizikai környezetet és a közműszolgáltatások, valamint egyéb szolgáltatások (vízhálózat, villamoshálózat, légkondicionálás, biztonsági berendezések, stb.) feltételeit;

b) az IFO vezető kérésére közreműködik az informatikai rendszerrel kapcsolatos átalakítási, építési, szerelési és karbantartási munkákban;

c) tájékoztatja az IFO vezetőt és egyeztet vele az IFO feladatkörébe tartozó kérdésekről.

10 Fizikai védelmi intézkedések

10.1 Informatikai infrastruktúrához kapcsolódó védelmi intézkedések

AZ IFO vezető az információbiztonsági felelőssel együttműködve a SZTROKUS-14-es melléklet táblázatának segítségével rögzíti a fizikai biztonsági zónába belépésre jogosultakat.

Az elektronikus információs rendszerek működési környezetét megfelelő fizikai, mechanikai, elektronikai és személyi védelemmel kell biztosítani (pl. rácsos ablakok, az áttörést megnehezítő üvegezés, acél ajtók stb.). Az alkalmazott védelmi formák körét, azok kialakítását az információbiztonsági felelős határozza meg a szabályzat előírásainak megtartása mellett, az adott létesítmény védelmi igényének és speciális feltételeinek figyelembevételével.

10.2 Informatikai eszközt tartalmazó helyiségekbe való belépés rendje

Szent Rókus Kórház és Intézményei olyan helyiségeit, ahol informatikai eszközökkel történik a munkavégzés, vagy informatikai eszközt tárolnak, lehetőség szerint zárszerkezettel kell ellátni, és a helyiséget távollét esetén vagyonvédelmi és biztonsági okokból zárva kell tartani.

A környezeti veszélyek és kockázatok mérséklése érdekében:

a) a berendezéseket úgy kell elhelyezni, hogy megakadályozzuk az illetéktelen hozzáférést és lehetőség szerint a helyiség észrevétlen megközelítését,

b) a környezeti határok és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével törekedni kell a szükséges működési feltételek biztosítására.

10.3 Informatikai szerverterem védelmi előírásai

Informatikai szerverteremnek minősülnek azon helyiségek, melyek működő szerverek elhelyezésére és működtetésére szolgálnak, kivételt képeznek azon egyéb helyiségek, melyekben zárt, kulccsal biztosított rack szekrény található.

Az informatikai szervertermek védelmének az adatok feldolgozását, tárolását, a hálózat működését biztosító berendezések védelmén túl ki kell terjedni a tárolt szoftverek, adatok és dokumentációk védelmére is.

A védelemnek az alkalmazások rendelkezésre állásának szükséges mértékével, a hardver és a szoftver beszerzési értékével, az adatok pótlásának költségével arányosan figyelembe véve a kiesési kockázatokat - teljes körűnek, zártnak és folytonosnak kell lennie.

az IFO vezetője, valamint a Műszaki osztály vezetője közös felelősséggel gondoskodik:

a) az informatikai szerverterem és a benne elhelyezett eszközök fizikai védelmét biztosító eszközök és berendezések meglétének és működőképességének rendszeres ellenőrzéséről, a tervezett karbantartásáról;

b) a szerverek működéséhez szükséges megfelelő fizikai környezet biztosításáról;

c) a megfelelő elektromos hálózat, villám-, túlfeszültség-, valamint érintésvédelmi berendezések meglétéről és működésének biztosításáról;

d) a behatolás elleni védelem és riasztórendszer kialakításáról (pl.: beléptető rendszer, elektromos behatolás jelző, mozgásérzékelő, belső térvédelem);

e) a megfelelő tűzvédelmi rendszerről;

f) füstjelző és riasztó rendszer kialakításáról;

g) automata tűzoltó rendszer kialakításáról, vagy kézi tűzoltó készülékek (elektromos berendezések tüzének oltására alkalmas gázzal oltó készülék) elhelyezéséről;

h) a szerverszoba klímájáról, oly módon, hogy az információtechnológiai eszközök környezeti hőmérséklete működés közben 15–25 °C, tárolási hőmérséklete 5–40 °C között maradjon, a relatív páratartalom pedig ne haladja meg a 40%-ot.

Az informatikai objektumok közüzemi ellátását (áramellátás, fűtés, szellőzés, vízszolgáltatás stb.) a vonatkozó szabályzatok és hatósági előírások szerint kell biztosítani.

Az informatikai szerverteremben vizesblokk kialakítása, átmenő víz- és szennyvíz vezetékek jelenléte nem engedélyezett. A szerverszobát védeni kell szennyvíz, illetve esővíz bejutása ellen. A kialakítás során törekedni kell arra, hogy felette vizesblokk ne helyezkedjen el.

Az informatikai szerverszobákban végzett építési és karbantartási munkákat az IFO osztályvezető, valamint a műszaki osztály vezetőjének az irányításával az informatikai biztonsági megbízott (IBM) felügyeli, az érintettek előzetes értesítése és az időpontok egyeztetése után.

Az üzemeltetés és hibaelhárítás során jelentkező alkatrész beszerzések, javítások és a rendszer fejlesztésére irányuló beszerzések szakmai előkészítése az IBM feladata az IFO osztályvezető irányításával. Amennyiben a javítás, fejlesztés kivitelezése építési munkával jár, az építési munkálatok ellenőrzése a Műszaki Osztály vezetőjének a feladata.

A teljes körű védelemről már a helyiségek kialakítása során gondoskodni kell. Az informatikai szervertermek üzemeltetése során biztosítani kell a mechanikai (építészeti) és a technikai (elektronikai) védelmet:

a) elektromos vagy fizikai (rács) védelmi eszközöket kell alkalmazni a nyílászárókon keresztül történő bejutás megakadályozása érdekében, beltéri vagy földszinti, illetve könnyen elérhető kültéri nyílászárók esetében egyaránt;

b) gondoskodni kell arról, hogy a szerverszobába kívülről nyitott nyílászárón vagy szellőzőn keresztül idegen anyagot bedobni ne lehessen;

c) a szerverszobára kívülről lehetőleg ne lehessen rálátni (pl. ablakon keresztül);

d) az ajtónak kulccsal és/vagy mágneskártyával, illetve kóddal zárhatónak kell lennie, valamint:

e) egy kulcsot vagy mágneskártyát, illetve kódot a portán, és az IFO vezetőjénél kell elhelyezni lezárt, hitelesítéssel ellátott borítékban vagy lepecsételhető kulcsdobozban,

f) a kulcshoz vagy a mágneskártyához, illetve kódhoz való hozzájutás csak naplózottan történhet, az IFO osztályvezető — vészhelyzetet, rendkívüli helyzetet kivéve — előzetes értesítésével és tudtával (aláírással, keltezéssel),

g) a borítékon meg kell jelölni a felvételére jogosultak nevét és beosztását, kulcsdoboz esetén a használható pecsét számát,

h) a doboz vagy boríték rendkívüli felnyitásáról telefonon és feljegyzésben haladéktalanul értesíteni kell az IFO osztályvezetőt és dokumentálni kell a felnyitás tényét (ki, mikor, miért)

i) a boríték felnyitását, a kód használatát követően a kódot meg kell változtatni.

j) Az informatikai szerverterembe csak az arra jogosult személyek léphetnek be.

Állandó vagy egyedi belépési jogosultságot az informatikai szerverterembe az IFO osztályvezetője, illetve a Szent Rókus Kórház és Intézményeinek főigazgatója adhat.

A belépési jogosultsággal nem rendelkezők az informatikai szerverteremben csak az arra jogosultak felügyelete mellett tartózkodhatnak.

Az informatikai szerverterembe külső személyek beléptetése esetében a külső személy:

a) előre időpontot egyeztet az IFO osztályvezetőjével vagy a Szent Rókus Kórház és Intézményeinek főigazgatójával;

b) a helyiségben csak kísérettel és szoros felügyelet mellett tartózkodhat;

c) a helyiségbe idegen számítástechnikai eszközt csak az IFO osztályvezetője engedélyével vihet be.

Az informatikai szerverteremben tilos

a) állandó jelleggel munkát végezni;

b) az eszközök közelében ételt, italt fogyasztani;

c) tűz- vagy robbanásveszélyes anyagot tárolni.

Az informatikai szerverteremben elhelyezett szerver- és nem szerverként működő számítógépeket, hálózati eszközöket, az informatikai szerverteremben használt klímaberendezéseket és biztonsági berendezéseket az év minden napján, a nap 24 órájában folyamatosan kell üzemeltetni.

Az informatikai szerverteremben elhelyezett számítógépeken telepített szoftverek karbantartását csak kijelölt informatikusok végezhetik.

Az IFO osztályvezetőjét értesíteni kell az informatikai szerverterem területén érzékelt, különös jelentőséggel bíró egyéb események bekövetkezéséről (pl.: betörési kísérlet, áramszünet stb.).

A hálózati eszközök üzemeltetése és felügyelete a szakmai irányító, szakmai irányításban közreműködő támogatókkal együttműködve történik.

Áramellátás szolgáltatási rendje:

a) az informatikai eszközök a vonatkozó szabványnak megfelelően kizárólag védőföldeléssel ellátott 230 V feszültségű elektromos hálózati dugaszoló aljzatba csatlakoztathatók;

b) a szervezeti szintű alkalmazások működését befolyásoló informatikai- és távközlési eszközöket (pl.: szerverek, rack szekrény stb.) lehetőség szerint szünetmentes tápegységekkel kell ellátni.

Az energiaellátó hálózat kábelezésének előírásai

a) védett kábeleket kell használni a károkozás, szándékos vagy gondatlan beavatkozás elhárítására, a környezeti veszélyek (tűz, robbanás, füst, víz, por, elektromágneses sugárzás) káros hatásai következményeinek elhárítására, csökkentésére,

b) az adatátviteli (távközlési) kábelt el kell különíteni az energiaellátás kábeleitől,

c) a Szent Rókus Kórház és Intézményei területén az informatikai rendszert, áramellátó hálózatot, telefonhálózatot érintő bármilyen beavatkozást, építést, karbantartást, átalakítást csak az IFO osztályvezető tájékoztatása után, annak jóváhagyásával és felügyeletével lehet végezni,

d) a kábeleket a kábelrendező és a csatlakozó aljzatok között rögzített csatornában kell vezetni, a lengőkábelek nem keresztezhetnek közlekedési utat. A hálózat valamennyi elemét olyan környezetben kell elhelyezni, ahol a jogosulatlan fizikai hozzáférés megakadályozott.

Az elektronikus védelmi rendszert az épület teljes területén, egyedi esetben a mechanikusan is elválasztott, a szervezeti biztonsági szint besorolásnak megfelelő biztonsági osztályba sorolt területen kell kiépíteni. A riasztásoknak az épület biztonsági szolgálatánál vagy a legközelebbi illetékes rendvédelmi szervnél kell jelezniük. Az elektronikus védelemnek szabotázsvédettnek kell lennie.

10.4 Az aktív informatikai berendezések védelme

Az informatikai szerverteremnek nem minősülő, de az informatikai biztonság szempontjából fontos helyiségeket szükség szerint megfelelő fizikai és elektronikai védelemmel kell ellátni.

Ilyen eszközök lehetnek:

a) hálózati rendezők;

b) kulccsal biztosított rack szekrények.

Az aktív informatikai berendezések védelme érdekében biztosítani kell:

a) a berendezések üzemi hőmérsékletét (lehetőség szerint klímaberendezés üzemeltetésével);

b) a megfelelő elektronikus védelmet, riasztóberendezést;

c) az illetéktelen hozzáférést korlátozó fizikai védelmet.

10.5 Hálózati végpontok védelme

A hálózati végpontok és az azokra csatlakoztatott eszközök végpontvédelméről minden informatikai eszköz esetében gondoskodni kell. A védelem során gondoskodni kell arról, hogy:

a) illetéktelenek ne férjenek szabadon maradt hálózati végpontokhoz;

b) illetéktelenek ne léphessenek be a számítógépekbe;

c) ne legyen támadható vezeték nélküli, vagy vezetékes kapcsolat a rendszerben;

d) a felhasználók ne tölthessenek le, illetve ne másolhassanak ki engedély nélkül adatot a számítógépekről.

A Kórház területén hálózati végpontot csak ellenőrzött körülmények között lehet létesíteni. A betegek közlekedési útvonalain, valamint a kórtermekben, rendelőkben és irodákban a használaton kívüli végpontoknak, az aktív és passzív hálózati elemekkel (router, switch, hub stb.) való kapcsolatát meg kell szüntetni, azokat a strukturált hálózatról le kell választani.

A vírusvédelmi rendszert a Szent Rókus Kórház és Intézményeinek minden számítógépére telepíteni kell.

Tilos olyan eszközt az informatikai hálózathoz csatlakoztatni, amelyet az Informatikai osztály munkatársai nem ellenőriztek, nem történt meg az Intézeti rendszerbe való integrálása és nem rendelkezik megfelelő vírusvédelemmel. (PC, notebook, tablet, switch, intelligens medikai eszköz stb.) Adathordozók esetében (pen drive, CD,DVD, mobil HD, memóriakártya, egyéb adathordozó eszközök stb.), csak tesztelt, vírusmentes eszköz csatlakoztatható az intézet rendszerébe. Ezért a felhasználó (csatlakoztatást végző) tartozik felelősséggel. Ennek ellenőrzését az informatika munkatársai végzik el.

Szakmai ellenőrzés hiányában az eszközt fogadó számítógéppel vírusellenőrzést kell végezni az eszközön és ebben az esetben az eszköz használója tartozik teljes körű felelősséggel az informatikai rendszerben bekövetkező, az eszköz használatával kapcsolatba hozható káreseményért.

Használaton kívül helyezett informatikai berendezés és a Szent Rókus Kórház és Intézményeinek összes hálózata közötti összeköttetést meg kell szüntetni.

Bármilyen eszköz kizárólag a kijelölt informatikus előzetes ellenőrző tevékenysége után csatlakoztatható az informatikai hálózatra. Bármilyen eszköz (kivéve a mobil eszköz) csak a kijelölt informatikus ellenőrző tevékenységével távolítható el az informatikai hálózatról. Idegen, nem Szent Rókus Kórház és Intézményeinek tulajdonát képező, nem a Szent Rókus Kárház és Intézményei által bérelt/használt eszköz csatlakoztatása nem engedélyezett.

10.6 Hardverekhez kapcsolódó általános védelmi intézkedések, a felhasználók által használt eszközökre vonatkozó előírások

Az informatikai eszközöket és az azokban tárolt, kezelt adatokat védeni kell a jogtalan közzététel, módosítás vagy eltulajdonítás ellen. Fokozottan ügyelni kell a megelőzésre, valamint a megfelelő védelmi intézkedések működtetésére a károk és veszteségek mérséklése érdekében.

A monitorokat úgy kell elhelyezni, hogy az azokon megjelenő adatokat illetéktelen személy ne láthassa.

A képernyővédőket jelszavas védelemmel kell ellátni.

A 2–4. biztonsági osztályba tartozó rendszerek munkaállomásai csak zárolás után hagyhatók felügyelet nélkül.

A BIOS-SETUP UEFI állítását jelszóhoz kell kötni úgy, hogy annak el kell térnie a felhasználói jelszótól, és azt a számítógépet felügyelő rendszergazdának kell beállítania, biztosítva, hogy a felhasználó ne tudja az indítási konfigurációt megváltoztatni.

Számítástechnikai eszközt, adathordozót, programot kizárólag a szervezeti egységek vezetőinek írásos engedélyével és az IFO vezetőjének hozzájárulásával, meghatározott időtartamra lehet kivinni a munkavégzés helyéről a személyi felelősség egyértelművé tételével. Ez alól kivételt képez a munkakör ellátásához biztosított mobil eszköz, melynek dokumentált átadása egyben a munkavégzés helyén kívüli használat engedélyezését is jelenti és használója felelősségét..

A kivitt eszközön tárolt adatok illetéktelenek általi elérhetetlenségére fokozottan kell ügyelni.

Meghibásodott eszköz cseréje esetén – garanciális esetben is – adathordozó csak úgy vihető ki, ha arról minden adat visszaállíthatatlan módon törlésre került.

A munkaállomásokon egyidejűleg modem és hálózati kártya csak az IFO vezetőjének engedélyével használható.

Az informatikai eszközök rendeltetésszerű használatáért a számviteli leltárban az eszköz használójaként kijelölt Szent Rókus Kórház és Intézményei alkalmazott a felelős, vagy az a személy, aki vezetői utasításra és engedéllyel azt használta. Közös használatú eszköz esetén az eszközök rendeltetésszerű használatáért az a személy a felelős, akit a szervezeti egység vezető kijelölt az eszköz felügyeletére (csoportvezető, ügyeletes, munkafelelős, stb.).

A munkája során számítógépet használó felhasználó köteles az általa működtetett számítógépet és az ahhoz csatlakoztatott eszközöket a rendeltetésnek megfelelően, munkavégzés céljából, szakszerűen, a Szent Rókus Kórház és Intézményei érdekeit szem előtt tartva az IBSZ-ben meghatározott módon használni.

A rövid, eltávozással járó szünet (2 óra vagy kevesebb) idejére a számítógépet a felhasználónak a hozzáférés ellen zárolni kell.

A munkaállomást illetéktelen személy (pl. beteg vagy ügyfél) jelenlétében a felhasználó nem hagyhatja felügyelet nélkül zárolatlan állapotban.

A napi munkavégzés befejezését követően a felhasználó a munkaállomást kikapcsolja. A non-stop betegellátást végző munkahelyeken is a munkaállomásokat minden nap újra kell indítani. Ettől eltérni csak az IFO vezetőjének előzetes értesítését követően és időtartamban szabad.

A nem használt (tartalék, javításra váró vagy javításból érkezett) informatikai eszközök tárolásáról az IFO, vagy az érintett szervezeti egység vezetője intézkedik. Ezen eszközök és kellékanyagok tárolása zárt, betörés elleni védelemmel biztosított, a tároló helyiségekre vonatkozó előírásoknak megfelelő helyiségben történhet.

Az informatikai eszközök használata során nem engedélyezett:

⇨ az eszközt illetéktelen személynek átengedni;

⇨ az eszköz közelében folyadékot, éghető anyagot, illetve felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni;

⇨ az eszközt a telepítési helyéről elmozdítani és elvinni a kijelölt informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök).

Az informatikai eszközöknek a munkafeladattól eltérő célra történő használatához a szervezeti egység vezetőjének engedélye és az IFO osztályvezető hozzájárulása szükséges.

Az informatikai eszközökhöz bármilyen külső eszközt, illetve kábelt csatlakoztatni csak a kijelölt informatikus engedélyével vagy közreműködésével lehet. Az informatikus által már

csatlakoztatott és beüzemelt eszköz további használata visszavonásig engedélyezett (pl.: pendrive, fényképezőgép).

Címkét, jelölést, feliratot csak a kijelölt informatikus helyezhet az informatikai eszközökre, illetve távolíthat el onnét. Az eszközök burkolatát megbontatni tilos! Alkatrészt vagy modult csak a kijelölt informatikus helyezhet be az eszközbe, illetve szerelhet ki az eszközből.

10.7 Informatikai eszközök karbantartása

Az informatikai eszközök rendelkezésre állásának biztosítása érdekében az IFO kijelölt informatikusai szükség szerint, illetve tervezett és a felhasználókkal egyeztetett módon karbantartást végeznek.

Az informatikai eszközök és berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében:

a) a specifikációban javasolt időközönként a karbantartási eljárásrendnek megfelelően, kell elvégezni a berendezések karbantartását;

b) a berendezések kezelését, illetve javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik,

c) az informatikai eszközök külső helyszínen (Szent Rókus Kórház és Intézményei területén kívül) történő javítása, karbantartása esetén gondoskodni kell az eszközön tárolt adatok végleges (visszaállíthatatlan) törléséről, vagy az adathordozó eltávolításáról.

10.8 Mobil eszközök használati szabályai

A hordozható eszközök használatba adása-vétele

A Szent Rókus Kórház és Intézményei tulajdonát képező mobil informatikai eszközöket (pl.: laptop, táblagép, PDA, okostelefon, a továbbiakban: mobil eszközök) a Kórház területén kívül csak az érintett felhasználó, aki részére az eszköz átadásra került, használhatja azt. A mobil eszköz harmadik fél részére történő átadása tilos!

A mobil eszközök és mobil adattárolók (pendrive, mobil merevlemez, memória kártya, a továbbiakban: mobil adattárolók) szoftvereit, operációs rendszerét a helyi informatikai munkatárs ellenőrzi és/vagy telepíti. Ugyancsak az üzemeltetésért felelős informatikai munkatárs végzi az alkalmazói szoftverek letöltését, telepítését, verzió-frissítését, a beállítások megváltoztatását.

Használatba adás előtt az alábbi védelmi eszközöket kell telepíteni, konfigurálni (laptopokra):

a) helyi biztonsági házirend,

b) vírusvédelmi, behatolás védelmi szoftver,

c) személyi tűzfal,

d) szükség esetén titkosító szoftver és/vagy hardver megoldás,

e) BIOS jelszóval történő zárolás.

Használatba adás előtt az alábbi védelmi eszközöket kell telepíteni, konfigurálni (okostelefonra, táblagépre):

a) vírusvédelmi, behatolás védelmi szoftver,

b) szükség esetén titkosító szoftver és/vagy hardver megoldás.

c) A felhasználónak és a használatba adónak az eszköz átadásakor, a használatba vétel megkezdése előtt ellenőrizni kell:

d) a mobil eszköz és tartozékainak meglétét,
e) a telepített védelmi eszközök meglétét (vírusvédelmi eszköz, személyi tűzfal),
f) az átadás-átvétel tényének dokumentálását,
g) mobil adattároló esetén a tartalmazó adatnak megfelelő titkosítási szint feltüntetését.

A hordozható eszközök használata

a) A hordozható eszközök konfigurációjának, beállításainak, paramétereinek megváltoztatására kizárólag az üzemeltetésért felelős informatikai munkatársak jogosultak.
b) Amennyiben az eszköz hosszabb ideig (1-2 hét) nem csatlakozik a helyi hálózathoz, a vírusédelmi szoftver szignatúrájának frissítését a felhasználónak kell megoldani. Ehhez szakmai segítséget az informatikai munkatársaktól kell kérnie.
c) A felhasználó köteles a hordozható eszközt a hivatali munkával kapcsolatos feladatokra, rendeltetésszerűen használni.
d) A mobil eszközön tilos a magánjellegű adatok tárolása, feldolgozása.
e) A szükséges frissítések, illetve konfigurációs változtatások végrehajtására, legalább havi rendszerességgel, a helyi informatikai üzemeltetés kérésére a felhasználó köteles a hordozható eszközt a beavatkozás idejére biztosítani.
f) A mobil eszközökhöz csak szabványos adathordozók használhatók.
g) Mobil eszközön, csak titkosított formában hagyhatja el adat az intézet területét.

Távmunkavégzés mobil informatikai eszközökön

a) Mobil informatikai eszközökön – az elektronikus levelezéshez való hozzáférésen kívül – távoli hozzáféréssel végzett munka kizárólag indokolt esetben, írásbeli kérelem alapján történhet az IFO vezetőjének véleményezését követően, az EIRF engedélyével.
b) A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie a munkavégzés kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. Távmunka, távoli hozzáférés esetén a Szent Rókus Kórház és Intézményeinek érintett dolgozójának gondoskodnia kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely védelméről.
c) A távoli hozzáféréssel végzett munka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, valamint a megfelelő és rendszeres ellenőrzésről. A távmunkához használt informatikai eszközök tekintetében gondoskodni kell arról, hogy az adatok tárolására csak a munkavégzéshez szükséges mértékben és ideig kerüljön sor. Az informatikai eszközökhöz való hozzáférést és az adatokhoz való hozzáférést korlátozni kell a munkavégző jogosultságainak megfelelően a minimálisan szükséges jogokra.

Az EIRF az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a távmunka igénylések jogosságát és megfelelőségét, valamint a dokumentációt.

Mobil eszközök fizikai védelme

A hordozható eszközök mobilitásuknál fogva fokozott veszélynek vannak kitéve a fizikai biztonságukkal kapcsolatos fenyegetettségekkel szemben. A hordozható eszközök fizikai biztonsága érdekében az alábbi szabályokat kell betartani:

a) A laptopokat csak az arra rendszeresített vízlepergetős, bélelt táskában szabad szállítani.

b) A szállítás során biztosítani kell, hogy az eszköz - különös tekintettel a merevlemezt tartalmazó mobil eszközöket (laptop, mobil merevlemez) - ne legyen kitéve erős rázásnak, vagy ütésnek.

c) A mobil eszközt tilos gépjárműben, idegen helyen felügyelet nélkül hagyni.

d) Repülőn, autóbuszon, vagy vasúton történő szállítás esetén a hordozható eszközöket kézipoggyászként kell szállítani. A folyamatos felügyeletet ez alatt is biztosítani kell.

e) A Kórház területén kívül, idegen helyen történő tárolás esetén (szálloda, lakás) fokozott figyelmet kell fordítani a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemre.

f) A megjelenítő felülettel rendelkező eszközök fokozottan érzékenyek a fizikai behatásoknak, ezért annak tisztítását csak erre a célra alkalmas törlőkendőkkel, és tisztítóanyagokkal szabad elvégezni.

A mobil eszközök tárolása

A Szent Rókus Kórház és Intézményei telephelyein a hordozható eszközöket használaton kívül zárható helyiségben vagy szekrényben kell tárolni, hozzáférést csak a kiadásra jogosult személynek kell biztosítani.

A hordozható eszközök az arra jogosultak mobilitását szolgálják, így az épületből való kivitelhez külön engedély nem szükséges. Tartós használat esetén a leltári rendszer rögzíti a tartós használat tényét.

A hordozható eszközöket tilos kitenni:

- erős fizikai behatásnak;
- sugárzó hőnek;
- erős mágneses, vagy elektromágneses térnek;
- fröccsenő víznek;
- poros környezetnek.

Mobil eszközökön tárolt adatok védelme

Titkosítás

A hordozható eszközökön tárolt adatok védelmére hardveres és/vagy szoftveres titkosító eszközök használata szükséges. Ebben az esetben a titkosító kulcsokat külső eszközön kell tárolni (pl. PEN drive, SmartCard, Security Key, stb.). a titkosító kulcsokat tartalmazó eszközt a hordozható eszköztől külön kell kezelni (tárolni, szállítani, stb.).

a) Adatbiztonság: nem engedélyezett az eszköz engedély nélküli átruházása vagy adatainak közlése.

b) A vezeték nélküli interfészeket (bluetooth, infra, wifi) alaphelyzetben kikapcsolt állapotban kell tartani és csak a szükséges időtartamra lehet bekapcsolni.

c) Az ismeretlen forrás felől érkező vezeték nélküli interfész (bluetooth, infra, wifi) csatlakozási kérelmet tilos engedélyezni. Nem azonosított, nem megbízható forrásból származó adat letöltése és telepítése tilos.

d) Az automatikus adatátviteli szolgáltatásokat a mobil kommunikációs eszközökön, a használaton kívüli időben ki kell kapcsolni.

e) Amennyiben a mobil kommunikációs eszköz lehetővé teszi, alkalmazni kell az eszköz szolgáltatásból történő kizárására, zárolására vagy tartalomtörlésre biztosított távoli elérési

szolgáltatásokat. Az ilyen programok telepítése előtt teszteléssel meg kell győződni a szolgáltatás működőképességéről, illetve arról, hogy a szolgáltatás nem megkerülhető.

f) A mobil kommunikációs eszközök által kezdeményezett ismeretlen program telepítésének engedélyezése tilos.

g) A mobil kommunikációs eszközökön alkalmazni kell a biztosított logikai védelmi alkalmazásokat, magasabb biztonsági osztályú adat esetén az eszköz sajátosságainak megfelelő kiegészítő szoftveres védelmet kell alkalmazni.

h) Magántulajdonú memóriakártyát az eszközbe helyezni vagy arról adatot feltölteni tilos! A memóriakártyákat a használatból történő kivonáskor a visszaállítás és elemzés megakadályozása érdekében az adatok bizalmasságával arányos törlési eljárásokat kell alkalmazni. Ez a szabály vonatkozik a normál mobil telefonok memóriakártyáira is. Törlésre csak engedélyezett eljárások alkalmazhatók, ennek hiányában fizikai megsemmisítést kell alkalmazni.

Csatlakozás Wifi hálózatokhoz

A mobil eszközön nem titkosított, nyílt hálózati kapcsolatok (Wi-Fi, Bluetooth stb.) használata biztonsági szempontok miatt nem engedélyezett.

Mobil eszközök felelősségi kérdései

Felhasználó felelőssége:

a) A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok bizalmasságának megőrzéséért, az eszköz eltűnéséért, megsérüléséért.

b) A mobil infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét haladéktalanul az IFO vezetője felé jelenteni kell a szükséges intézkedések megtétele érdekében.

Teendők a hordozható eszköz eltulajdonítása esetén

Amennyiben a hordozható eszközt eltulajdonították, az alábbiakat kell tenni:

a) Értesíteni kell az IFO vezetőjét, illetőleg a rendőrséget, aki kiállítja a bejelentésről szóló jegyzőkönyvet. Értesíteni kell az információbiztonsági felelőst, aki intézkedik a felhasználó jelszavának megváltoztatásáról.

b) Az információbiztonsági felelős illetve az informatikus intézkedik az esemény kivizsgálására annak érdekében, hogy megállapítható legyen a felhasználó esetleges felelőssége.

c) Ha a rendőrségi nyomozás nem jut eredményre a nyomozás befejezéséről szóló jegyzőkönyvet, és a bejelentésről szóló jegyzőkönyvet át kell adni a szervezet gazdasági vezetőjének.

10.9 *Eszközkivonási biztonsági intézkedések, újra felhasználás*

a) Megsemmisítésre kijelölt eszközöket és kellékanyagokat megsemmisítésig a használatban lévő eszközöktől elkülönítetten kell tárolni és kezelni, figyelembe véve: a veszélyes anyagok tárolására és a megsemmisítésre vonatkozó szabályokat (fizikai védelem, szállítás);

b) az adatvédelem biztonsági követelményeit (hozzáférés elleni védelem) be kell tartani.

c) a Szent Rókus Kórház és Intézményei eszközeinek leltározási és leltárkészítési szabályzata alapján kell eljárni a feleslegessé vált eszközök selejtezésekor és hasznosításakor.

Az informatikai berendezések végleges használaton kívül helyezése előtt gondoskodni kell az összes adat, szoftver visszaállíthatatlan eltávolításáról és felülírásáról, vagy a beépített adathordozó eltávolításáról/roncsolásáról és megfelelő tárolásáról a minősített adattörlés szabályainak megfelelően.

A különleges adatok törlése a DMS 2008 Standard for Physical HDD Destruction európai szabványnak, az adathordozó biztonsági szintjének megfelelően roncsolással, a Szent Rókus Kórház és Intézményei területén kell, hogy megtörténjen.

Külső fél által javításra, megsemmisítésre elszállított informatikai eszközökből el kell távolítani a beépített adathordozót, ha ez nem megoldott, a külső fél arra felhatalmazott képviselője a külső fél nevében joghatályos nyilatkozatot köteles tenni az adatvédelmi és titoktartási szabályok betartására vonatkozóan. Ezt a nyilatkozatot az informatikai biztonsági megbízott rendelkezésére kell bocsátani.

11 Az elektronikus információs rendszerek üzemeltetéséhez, védelméhez kapcsolódó szabályok

11.1 Szoftverekhez kapcsolódó általános védelmi intézkedések

Az elektronikus információs rendszer valamennyi szoftver eleméről nyilvántartást kell vezetni. A nyilvántartásnak tartalmaznia kell a működtető szoftverek egyedi beállításait és elhelyezkedését, az azokért felelős személy nevét. Az üzembiztonság érdekében a szerverek operációs rendszereit (a beállításokkal együtt) lehetőség szerint tartalék adathordozón is tárolni kell, amely szükség esetén azonnal betölthető.

Szoftvert a Szent Rókus Kórház és Intézményei által használt informatikai eszközre [beleértve a mobil eszközöket is: pl. okostelefon, tablet stb., amelyekre (kis)alkalmazások letöltése is tilos] csak kijelölt informatikus tölthet le, másolhat és telepíthet, valamint a számítógépről csak kijelölt informatikus távolíthat el. Az informatikusnak lehetőség szerint minden esetben kerülnie kell a „hazatelefonálós" (kis)alkalmazások telepítését, használatuk esetén azonban kifejezetten tiltaniuk kell az ez irányú adatforgalmakat. (Pl.: Windows 10, Adobe Acrobat Reader által megnyitott PDF állományok automatikus, ellenőrizetlen publikus felhőbe történő feltöltése, Google ilyen irányú szolgáltatásai stb.)

A felhasználó a munkaállomás használata során a munkaállomásra telepített alkalmazásokat használhatja. Új alkalmazások telepítését vagy a meglévő alkalmazásokat illető jogosultság változást a szervezeti egység vezetője engedélyével az erre szolgáló MNY-521, MNY522, MNY528 formanyomtatványon igényelhet. A felhasználó a számítógépre telepített alkalmazásokat a felhasználói leírás szerinti módon, szakszerűen köteles használni.

A központi szakmai irányításban közreműködő szervek által üzemeltetett On-line alkalmazásokhoz (továbbiakban: OKA) kapcsolódó jogosultságokra vonatkozó igénylések, változásjelentők és levelezések másodpéldányát a szervezeti egységek kapcsolattartó személyei kötelesek megőrizni.

11.2 Elektronikus információs rendszerek tervezése és átvétele

A megfelelő kapacitás és a szükséges erőforrások elérhetősége érdekében előzetes tervezést és előkészületeket kell végrehajtani. Ennek során a rendszer túlterheltségével járó kockázatok

mérséklése érdekében fel kell mérni a várható kapacitásigényt, meg kell határozni az új rendszerek üzemeltetési követelményeit, a rendszer átvétele és üzembe helyezése előtt el kell végezni a követelmények dokumentálását, és le kell futtatni a szükséges teszteket.

A rendszer működtetéséhez, működéséhez szükséges adatfeldolgozó és adattároló kapacitásokról való gondoskodás során:

a) fel kell mérni, nyomon kell követni a várható kapacitásigényt;

b) figyelembe kell venni a környezet és a rendszer támasztotta igényeket;

c) nyomon kell követni a rendszer erőforrásainak – processzorok, központi tárolóegységek, adatállományok tárolására rendszeresített eszközök, nyomtatók és egyéb kimenetek, adatátviteli rendszerek – felhasználását, terhelését;

d) ki kell szűrni és meg kell szüntetni a rendszer biztonságát és a felhasználói szolgáltatásokat veszélyeztető szűk keresztmetszeteket, és meg kell tervezni a rendszer helyreállításához szükséges intézkedéseket.

Az elektronikus információs rendszerek átvétele során átadás-átvételi jegyzőkönyv készül, mely tartalmaz minden, az átvétellel kapcsolatos feladatot, kötelezettséget, dokumentációt, de legalább a következő dokumentumokat:

a) logikai rendszerterv, melynek tartalmi elemei a logikai felépítés, használati esetek és szerepkörök, szerepkörfunkció-összerendelés, folyamatok leírása, képernyőtervek, logikai adatmodell, adatfolyam ábrák, interfészek logikai specifikációja, határvédelem, mentési megoldás, adatmennyiségi és feldolgozási kapacitáskövetelmények, hibakezelés, installálás;

b) fizikai rendszerterv, melynek tartalmi elemei a szoftverkörnyezet, tervezési alapelvek, szoftverarchitektúra, szoftverkörnyezet-függőségek, a megoldás határai, folyamatok leírása, rendszerkomponensek, rendszerbiztonság, jogosultságkezelés és regisztráció, képernyőtervek, interfészek;

c) konfigurációs leírás, melynek tartalmi elemei a rendszerarchitektúra felépítése, rendszerelemek kapcsolatai, alapinfrastruktúra hardverei és szoftverei, hálózati felépítés, védelmi konfigurációs megoldások, hálózati szegmensek közötti forgalom átengedés konfigurációja, terheléselosztás, magas rendelkezésre állás, teszt és oktatási rendszer, mentési megoldás konfigurációja;

d) üzemeltetési kézikönyv, melynek tartalmi elemei a rendszer és egyes elemeinek telepítési leírása, mentési és helyreállítás, monitorozás felügyelet-üzemeltetési feladatok, adminisztrátori funkciók, rendszerműködési követelmények, beállítások, lehetséges hibajelenségek;

e) biztonsági rendszerek, alrendszerek dokumentációja, melynek tartalmi elemei a biztonsági funkciók leírása, azok installációja, aktiválása, leállítása és használata a fejlesztés, valamint az üzemeltetés során;

f) oktatási kézikönyv, melynek tartalmi elemei a felhasználói funkciók, adminisztrátori funkciók, biztonsági elvárások;

g) felhasználói kézikönyv, melynek tartalmi elemei a felhasználói funkciók, biztonsági elvárások.

Az elektronikus információs rendszerek átvételének feltétele az önálló jogi oltalomban részesíthető termék kapcsolódó dokumentációinak rendelkezésre állása és átadása a Szent Rókus Kórház és Intézményei számára az üzletmenet-folytonosság biztosítása érdekében. Az átadott dokumentációk alapján a Szent Rókus Kórház és Intézményei tesztkörnyezetében– a

tesztkörnyezet korlátainak figyelembevételével – a felhasználói kézikönyvben meghatározott funkciókkal működőképes elektronikus információs rendszert kell tudni üzemeltetni.

11.3 Új rendszerprogramok bevezetésének rendje

Az új rendszerprogram bevezetését az IFO vezetője engedélyezi. Ennek érdekében az új rendszerprogram-tervezetet az IFO kijelölt munkatársa véleményezi.

A rendszer bevezetése és oktatása az IFO munkatársainak közreműködésével hajtható végre.

Fejlesztés során az éles környezet mellett külön fejlesztői-, külön teszt- és külön oktatói környezet kialakítása szükséges. A tesztkörnyezetnek tartalmaznia kell mindazon elemeket, amelyekben valamely módosításra sor kerül. A tesztkörnyezetnek, a tesztelni kívánt elem kivételével, lehetőleg ugyanolyan beállításúnak kell lennie, mint az éles környezetnek.

A fejlesztői környezetből tesztelés nélkül semmilyen elem sem kerülhet át az éles környezetbe. Nem éles környezetben csak olyan próbaadatok használhatók, amelyek nem sértik az éles környezetben használt adatokra vonatkozó adatvédelmi szabályokat.

11.4 Az elektronikai információs rendszer változáskezelésének biztonsági követelményei

Az informatikai rendszerben változtatni csak az alábbi követelmények betartása mellett lehet:

a) a Kórház által üzemeltetett rendszerprogramok (alapszoftver), illetve a felhasználói programok telepítését a központi számítógépekre (szerverekre) és munkaállomásokra csak az erre feljogosított informatikusok végezhetik el. Portable (telepítés nélkül futtatható) programok futtatása is csak az informatikusok által megengedett, a felhasználók részéről tilos! Jogosultságot az Informatikai Osztály vezetője engedélyezhet;

b) az alapszoftverrel kapcsolatos bármely konfigurálási, hangolási műveletet csak az IFO kijelölt informatikusa, illetve – előzetes jóváhagyása mellett – az erre felhatalmazott üzemeltető végezhet. Az alkalmazói szoftvereken végzendő, azok bármely funkcióját megváltoztató művelethez az IFO és a szakmai terület vezetőjének együttes engedélye szükséges. A verzióváltás és egyéb, jelentős beavatkozást igénylő hangolás elvégzéséhez az IFO vezetőjének engedélye kell;

c) a felmerült változtatási igényeket kielégítő beállításokat tesztkörnyezetben az IFO vezetője által meghatározott időszakon át, munkarendszerűen tesztelni és üzemeltetni kell;

d) teljes körű tesztelési eljárásokkal kell megbizonyosodni az új rendszer bevezetése előtt;

e) próbaüzem és terhelési próbák során meg kell vizsgálni az új rendszer üzembiztonságát és megbízhatóságát még a bevezetés előtt;

f) a tesztelésről készített jelentés felhasználásával dönt az Informatikai Osztály vezetője a beállítások, illetve alkalmazások bevezetéséről;

g) a Kórház informatikai rendszerében beállításokat, illetve alkalmazásokat helyi előzetes

h) tesztelés nélkül csak a rendszerszállító szakmai irányítójának, szakmai alkalmazási igazolása mellett szabad alkalmazni;

h) alapszoftvert és alkalmazói szoftvert csak érvényes, arra vonatkozó licenc alapján szabad felhasználni.

A rendszerben használt szoftvereket csak megbízható forrásból (ismert szállítótól) szabad beszerezni az álcázott csatornán keresztüli beavatkozás és „trójai" programok bejuttatásának kivédésére.

A külső céggel végeztetett szoftverfejlesztés esetén rögzíteni kell a tulajdonosi, használati és licencjogokat. Rögzíteni kell a követés módját, formáját és minimális időtartamát.

A Szent Rókus Kórház és Intézményei rendszerében végzett, külső cég általi szoftverfejlesztés esetén vizsgálni kell:

a) az IT-biztonsági veszélyeket és kockázatokat a fejlesztés során,

b) a fejlesztő szervezet megbízhatóságát,

c) a fejlesztésre vonatkozó szerződésben a fejlesztőnek garanciát kell vállalnia arra, hogy a fejlesztett alkalmazás nem jelent kockázatot az IT-biztonságra.

11.5 Biztonság a felhasználói rendszerekben

A felhasználói rendszerek integrált biztonsága kiterjed a rendszerekben tárolt felhasználói adatok illetéktelen hozzáférésének, módosításának, törlésének, nem megfelelő felhasználásának stb. megelőzésére. A rendszertervek összeállítása során mérlegelni kell a rendszerbe beépítendő automatikus ellenőrző eszközök, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.

A felhasználói rendszerek biztonsága érdekében a felhasználói rendszerekben – többek között a felhasználó által kifejlesztett alkalmazásokban – meg kell tervezni a megfelelő ellenőrző eszközöket és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatok, a belső adatfeldolgozás és a kimenő adatok hitelesítését. A biztonsági intézkedéseket pontosan, minden részletre kiterjedően dokumentálni kell, az adatfeldolgozó rendszerekben bevitt adatokat hitelesíteni, ellenőrizni kell.

A bemenő adatok ellenőrzésének eszközei:

a) az ismételt adatbevitel és az ebből származó adat-karbantartási anomáliák elkerülésére írt eljárások;

b) időszakos adatmező- és adatállomány-vizsgálat, valamint a felvitt adatok hitelességének, valamint integritásának ellenőrzése és igazolása;

c) az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése és ezek engedély nélküli módosításának megakadályozása, valamint az engedélyezés kikényszerítésére írt eljárások;

d) az adathitelesítési hibák kiküszöbölését elősegítő eljárások;

e) adatbevitel során, a mezőtípus-kompatibilitást biztosító és az adattartalom helyességét ellenőrző és kikényszerítő eljárások és függvények;

f) az alkalmazáshoz történő hozzáférés naplózása;

g) a feldolgozásban részt vevő Szent Rókus Kórház és Intézményei munkatársak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

A pontosan és hiánytalanul bevitt adatok biztonságát, integritását a feldolgozás ideje alatt a következő intézkedésekkel kell szavatolni:

a) az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni, különös tekintettel az adatmódosító, adattörlő funkciók helyére;

b) az adatfeldolgozási hibák megelőzése érdekében hibadetektáló és a további rendszerfutást leállító eljárásokat kell beépíteni;

c) korrekciós programokat kell alkalmazni a feldolgozás során felmerülő hibák korrigálására;

d) a folyamatba épített ellenőrzés alkalmazása.

e) az azonosítás és a hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni;

f) a hitelesítést a felhasználó és a rendszer között egy, a felhasználó által megnyitott védett csatornán keresztül kell biztosítani.

Az adatfeldolgozás rendszerében ellenőrizni, hitelesíteni kell a kimenő adatokat. Ennek során a kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:

integritás-ellenőrzés;

az adattartalom meglétének, értékének ellenőrzése;

a megfelelő minősítés meglétének ellenőrzése;

a kimenő adatok értékelésében és hitelesítésében részt vevő Kórházi munkatársak feladatainak és felelősségének meghatározása a munkaköri leírásokban.

Webes felületetek elérhetőségét kizárólag titkosított https csatornán szabad biztosítani. A webes felületeken biztosítani kell a felhasználó azonosító adatok rejtettségét.

11.6 Az operációsrendszer-szintű és rendszerszoftver szintű hozzáférések ellenőrzése

Informatikai eszközök használata minden esetben azonosított felhasználói hozzáféréssel történhet, amelyről naplót kell vezetni.

A Szent Rókus Kórház és Intézményei munkatárs kizárólag a saját nevében férhet az informatikai eszközökhöz, ami alól kivételt képeznek azok a funkciók, melyek a gyártó által dokumentáltan nem végezhetőek el, csak a beépített magas szintű adminisztrátori jogosultsággal (administrator, sys, system, root stb.) rendelkező technikai felhasználó nevében., illetve közös használatú felhasználói munkaállomásokon (gyógyító osztályokon) lévő felhasználói profilhoz.

A gyártók által beépített felhasználókat telepítéskor zárolni kell, azokat munkavégzés céljából használni nem lehet.

Az informatikai eszközök illetéktelen elérésének megakadályozása érdekében az operációs rendszer szintjén rendelkezésre álló biztonsági lehetőségeket is fel kell használni a számítástechnikai erőforrásokhoz való hozzáférés korlátozásához.

Ezeknek a következőket kell lehetővé tenniük:

a) az engedéllyel rendelkező felhasználó személyének azonosítása és hitelesítése, szükség esetén a terminál vagy hely azonosítása;

b) a sikeres és az eredménytelen hozzáférési kísérletek rögzítése;

c) megfelelő hitelesítési eszközök és – jelszókezelő rendszer használata esetén – minőségi jelszavak biztosítása;

d) adott esetben a felhasználók csatlakozási idejének korlátozása.

Ha a kockázatok alapján ez indokolt, más hozzáférést vezérlő módszerek (pl. ujjlenyomat azonosító eszközök, chipkártya, kérdés-felelet) is alkalmazhatók.

A számítógéprendszerbe való bejelentkezési folyamatnak minimumra kell csökkentenie az illetéktelen hozzáférés lehetőségét. Ennek során csak a bejelentkezés eredményes befejezése után jelenhet meg a használni kívánt rendszerre vonatkozó adat, azonosító, stb.

A bejelentkezés elfogadására vagy elvetésére csupán az összes szükséges adat megadása után kerülhet sor, sikertelenség esetén a rendszer nem jelölheti meg a hibás, elrontott azonosítót, jelszót.

Korlátozni kell az eredménytelen bejelentkezési kísérletek számát, rögzíteni kell az eredménytelen kísérleteket, időtúllépés esetén meg kell szüntetni az adatátviteli kapcsolatot.

Biztonságos bejelentkezési folyamatot kell kialakítani, amelynek során:

a) az azonosítás és hitelesítés keretében a hozzáférési jogosultságot jelszavakkal kell ellenőrizni. A jelszómenedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen megkerülhető, illetve könnyen megfejthető;

b) a felhasználók azonosítása egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas kell, hogy legyen;

c) a munkakör megváltozásakor a felhasználók hozzáférési jogosultságait felül kell vizsgálni, és ennek alapján módosítani kell;

d) biztosítani kell a felhasználói azonosítók időszakos vagy végleges letiltásának lehetőségét;

e) a rendszerhozzáférés szempontjából meghatározó erőforrásokhoz (pl. fájlok, tároló területek, berendezések stb.) olyan egyedi azonosítókat kell rendelni, amelyek a hozzáférési jogosultság meghatározásának alapjául szolgálnak.

Mindazon operációs rendszerelemeket, segédprogramokat, amelyek a munkavégzéshez nem szükségesek, nem telepíthetők, amennyiben ez elkerülhetetlen, úgy a telepítési folyamat zárásaként el kell távolítani azokat a rendszerből. Alkalmazásszintű hozzáférések vezérlése

Az illetéktelen hozzáférés megakadályozására a felhasználói rendszereken belül biztonsági eszközöket is kell alkalmazni.

A programok és az adatok logikai hozzáférését minden esetben az engedéllyel rendelkező felhasználókra kell korlátozni. A felhasználói rendszernek nem szabad befolyásolnia olyan más rendszerek biztonságát, amelyekkel az adott rendszer megosztva használ különböző informatikai erőforrásokat.

12 Adminisztratív védelmi intézkedések

12.1 A felhasználói jogosultságok kezelése

Munkaviszony megszűnésekor a szervezeti egység vezetője kezdeményezésére, a munkáltatói jogkör gyakorlója gondoskodik az IFO osztályvezetőjének értesítéséről, a jogosultságok töröltetéséről. A felhasználóval kapcsolatban felmerülő, de nem jogosultsághoz kapcsolódó egyéb informatikai igényeket a Szent Rókus Kórház és Intézményei elektronikus HelpDesk (továbbiakban: eHD) rendszerén keresztül kell benyújtani pl.:

a) informatikai eszközigénylés, mozgatás, áthelyezés és átvezetés;

b) informatikai eszköz meghibásodása,

c) kellékanyag igénylése,

d) szoftveres tudásigény-támogatás bejelentése

e) informatikai rendszerhez hozzáférés-változtatási igény (igénylés, módosítás vagy törlés);

f) informatikai szolgáltatáshoz, alkalmazáshoz, hálózati mappához (könyvtár) való hozzáférés, valamint ezekkel kapcsolatos jogosultság változása (igénylés, módosítás vagy törlés).

g) alkalmazástelepítési vagy -eltávolítási igény;

h) inaktívvá válás esetén újraaktiválás kérése;

i) munkavégzési hely vagy feladat változása esetén egyedi vagy tömeges eszközmozgatási és telepítési igény;

j) hálózattal kapcsolatos igény (kiépítés, bővítés, elbontás);

Az MNY-521formanyomtatvány alapján a megbízott informatikai munkatárs elvégzi az informatikai rendszerben az engedélyezett módosításokat,

az adatok átvezetését, a szükséges beállításokat;

a) letiltja vagy engedélyezi az informatikai szolgáltatásokat (pl.: levelezés, internet, hálózati mappa elérése, nyomtatás stb.);

b) szükség esetén, továbbítja az illetékes adminisztrátor részére az igényt, (pl.: EESZT V-Matrix jog kezelése esetén a Szent Rókus Kórház és Intézményei adminisztrátor részére)

c) elvégzi a jogosultságok nyilvántartását:

1. amennyiben az adott rendszerből az informatikus által lekérdezhető, akkor a jogosultságok rendszerben történő átvezetésével,
2. egyéb esetben külön (elektronikus vagy papíralapú) jogosultsági nyilvántartás vezetésével;

d) Kezeli [átadja/átveszi/átvezeti/beállítja/törli] az informatikai eszközöket és jogokat a belépő/kilépő/meglévő felhasználóknak, ugyanakkor módosítja a kapcsolódó nyilvántartásokat, amennyiben ehhez nincs jogosultsága, akkor továbbítja az illetékes adminisztrátornak, szükség esetén a munkahelyi vezetőjének.

Az IFO kijelölt informatikusa elvégzi az informatikai eszközök nyilvántartására vonatkozó alábbi teendőket:

1. az eszközök mozgásáról – ha nem kellett az eszközök mozgását rögzítő munkakör átadás- átvételi jegyzőkönyvet készíteni - eszköz átadás-átvételi adatlapot állít ki,
2. az adatlapot az utalványozó aláírja
3. az adatlapot az érintett felhasználókkal aláírattatja,
4. az aláírt adatlapot átadja a változások analitikus nyilvántartáson történő átvezetése érdekében a Pénzgazdálkodási Osztálynak;

A jogosultságkezelésnél biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága munkakörüknek megfelelő legyen.

A hozzáférés-jogosultság vezérlésére a szerepkör szerinti hozzáférés elvét kell alkalmazni, vagyis az elektronikus információs rendszereknek alkalmasnak kell lenniük a hozzáférési jogok csoportszinten való megkülönböztetésére és szabályozására. Kivételes esetekben a hozzáférési jogok egyedileg is hozzárendelhetők a felhasználókhoz.

Hálózati rendszergazdai jogosultság kizárólag az Informatikai Osztály vezetőjének engedélyével adható.

A lokális rendszergazdai fiókok jelszavai elzárt borítékban, páncélszekrényben kerülnek eltárolásra az IFO vezetőjének irodájában.

A rendszergazdai jelszavakkal kapcsolatban, amennyiben a rendszerben erre lehetőség van, biztosítani kell az alábbi követelmények teljesülését:

a) a jelszó legalább 9 karakterből álljon;

b) a jelszót a kisbetűk (a–z), a nagybetűk (A–Z), a számok (0–9) és a jelek halmazából mindhárom csoport felhasználásával kell képezni, különleges karaktereket nem szabad alkalmazni (!,%,*,?,; stb.),

c) a jelszó 7 sikertelen kísérlet után zárolásra kerül;

d) a számítógépes rendszerekben a jelszavakat nem lehet nyílt formában tárolni. A jelszófájlokat megfelelő kódolási védelemmel kell ellátni.

Hálózati felhasználói jogosultságot a szervezeti egység vezetőjének írásban a MNY-521 formanyomtatvány benyújtott kérelmére, jóváhagyásokat követően az IFO kijelölt informatikusa adja meg.

Számítógépen helyi (lokális) rendszergazdai jog csak az IFO Osztályvezető egyedi írásos engedélyével, személyhez kötött módon adható, kizárólag üzemeltetési indok alapján.

A felhasználó helyi (lokális) felhasználói névvel közvetlenül egyik gép operációs rendszerébe sem jelentkezhet be.

A számítógép-programokhoz, rendszerprogramokhoz és adatokhoz csak az arra jogosult informatikusok számára megengedett a hozzáférés biztosítása. Ezt az operációs rendszerek védelmi rendszerének kell biztosítania, és csak ennek megfelelő operációs rendszereket szabad használni.

Az informatikai szerverteremben működő rendszerek rendszergazdai és adminisztrátori jogait nyilvántartó dokumentumot az IFO vezetője hagyja jóvá. Ebből egy példányt tárolni kell az érintett informatikai szerverteremben.

AZ IFO vezetőjének egyedi engedélye alapján kap valamely belső vagy külső munkatárs adminisztrátori/üzemeltetői jogokat.

A nem személyhez köthető adminisztrátori (root, superuser, teljes jogú adminisztrátor stb.) azonosító nem lehet napi használatban, az csak olyankor használható, amikor elengedhetetlen.

A nem személyhez köthető adminisztrátori azonosítókat és jelszavakat lezárt, és az adminisztrátor által aláírt borítékban az IFO osztályvezetője őrzi páncélszekrényben.

Az EIRF az alkalmazásokhoz tartozó felhasználói jogok felülvizsgálatát szúrópróbaszerűen ellenőrzi, az ellenőrzés eredményét dokumentálja.

A kiemelt jogosultsággal rendelkező felhasználók esetében az EIRF rendszeresen ellenőrzi, hogy ilyen jogokkal csak egyedileg azonosítható felhasználók, csoportok és eszközök rendelkezhessenek.

A munkakörök változását a munkáltatónak jeleznie kell az IFO osztályvezetője felé, az erre rendszeresített nyomtatványok használatával. (SanitasX jogosultság igénylő, CT-ECOSTAT jogosultság igénylő, Jogosultság és bejelentkezés igénylő lap)

A felhasználó csak a számára meghatározott információkhoz férhet hozzá. Minden egyéb hozzáférési kísérletet biztonsági eseményként kell kezelni.

Az informatikai rendszerbe belépő felhasználókhoz kapcsolt Single sign-on (hálózati authentikáció, egypontos bejelentkezés több alkalmazásba) biztosítása az érintett alkalmazások üzemeltetőjének és IFO vezetőjének megállapodása alapján történik. A megállapodásban rögzíteni kell a beállítással kapcsolatos feltételeket.

Az alkalmazásokhoz a felhasználói jogosultság beállítása alkalmazásszintű felelősség. Meg kell határozni, hogy az adott alkalmazásban milyen modulokat, menüstruktúrákat, adathalmazokat érhet el, módosíthat a felhasználó. (Csak lekérdezéseket végezhet; adatrögzítést végezhet, de törzsadatokat nem módosíthat; törzsadatokat is kezelhet; adatfeldolgozásokat indíthat pl. zárások, külső rendszerek felé indíthat kommunikációt stb.)

a) A szervezeti egység vezetője határozza meg a felhasználó részére, hogy milyen számítástechnikai rendszerekhez, milyen jogosultsági szinten (pl.: megtekintő, adatrögzítő, adatfeldolgozó, alkalmazásfelelős, rendszergazda) férhet hozzá.

b) Gazdasági rendszer a CT-ECOSTAT ezen belül a munkavégzéshez szükséges modulok és ezen belül a munkavégzés célterülete : főkönyv, pénzügy, kötelezettségvállalás, rendelés, intézeti elbírálás, rendelés, osztályos igénylés, munkalap, raktár/készlet, tárgyi eszköz, medkontroll, cashflow, élelmezés, rendszergazdai modulok (paraméter kezelő, védelmi rendszer)

c) Medikai rendszer SanitasX : osztályvezető főorvos, főorvos, szakorvos, főnővér, nővér, adminisztrátor, betegfelvétel, rendszergazda.

d) Intézeti gyógyszertári rendszer GYURIKA: főgyógyszerész, gyógyszerész, adminisztrátor, rendszergazda.

e) Közforgalmú patikai rendszer QB-Pharma: főgyógyszerész, gyógyszerész, adminisztrátor, rendszergazda.

f) Labor rendszer ANDROMÉDA: labor vezető, validáló, orvos/biológus, adminisztrátor

g) Képalkotó diagnosztikai rendszer IMPAX : szakorvos, adminisztrátor, rendszergazda.

h) Bérszámfejtési rendszer KIRA: osztályvezető, ügyintéző, rendszergazda.

i) Humánpolitikai rendszerek ORGWARE és NEXON IHr : osztályvezető, ügyintéző, rendszergazda.

Minden alkalmazás esetén az adatgazda határozza meg és jelöli ki a jogosultságok beállításáért felelős személyt (alkalmazásfelelős vagy más néven alkalmazásgazda).

A jogosultsági igényléseket az IFO osztályvezető által kijelölt informatikus tárolja és tartja nyilván a jogosultsági nyilvántartásban.

A jogosultságokat az alkalmazásfelelős informatikus állítja be a kitöltött MNY-521, MNY522, MNY 528 formanyomtatványok alapján. A beállítást követően a változtatás időpontját és elvégzését az IFO kijelölt dolgozója aláírja, ellenőrzésre az IFO vezetőjének továbbítja. A lapot a jogosultsági nyilvántartást megalapozó iratként kell megőrizni elektronikus és papír alapon egyaránt.

Jogosultsági igény elutasítása esetén írásban jelezni kell az igénylőnek az elutasítás okát.

Ha egy igény a teljesítése esetén a már meglévő jogokkal együtt összeférhetetlenséget eredményezne, az igénylést el kell utasítani. Szintén el kell utasítani az igénylést, ha az IFO vezetője úgy ítéli meg, hogy a kért jog megadása az elfogadható mértékű informatikai biztonsági kockázatot meghaladja.

Ha a felhasználó a jogosultságával visszaélve kárt okoz, vagy vállalhatatlan mértékű kockázatot jelent az elektronikus információs rendszerre, az EIRF-től telefonon is kérhető a jogosultság megszüntetése. Ebben az esetben az EIRF a helyzet értékelése után dönt a jogosultság visszavonásáról vagy a kérés elutasításáról. A döntést és a megkeresést is dokumentálni kell. Ha az EIRF a jogok felfüggesztése mellett dönt, azonnal intézkedik a jogok visszavonásáról. Az alkalmazásfelelős/alkalmazásgazda ilyen esetben feljegyzésben vagy egyéb módon írásban jelez vissza az EIRF-nek, aki a nyilvántartásokban is átvezetteti a módosítást a nyilvántartás és a valós beállítások egyezőségének biztosítása érdekében.

Az IBSZ jogosultságok kezelése elnevezésű függelékben található a felhasználói jogok kezelésének, kiadásának részletes útmutatója.

12.2 A felhasználói jelszavak kezelése

A felhasználó írásban felelősséget vállal személyes jelszavainak bizalmas kezeléséért.

A belépéskor kapott vagy – pl. ha a felhasználó elfelejtette a jelszavát – az ideiglenes jelszó átadása csak biztonságos csatornán történhet aláírással ellátott kérelme alapján, a felhasználó

előzetes – pl. személyes – azonosítása után. Biztonságos csatornának tekintendő a belépéskor megadott személyes mobil telefonszám. Az ideiglenes jelszavak megváltoztatása kötelező az első belépést követően.

A jelszót a felhasználó megváltoztathatja.

A felhasználói jelszavakkal kapcsolatban (ha a rendszerben erre lehetőség van) biztosítani kell a következő követelmények teljesülését:

a) a jelszó legalább 9 karakterből álljon;

b) a jelszót a kisbetűk (a–z), a nagybetűk (A–Z), a számok (0–9) és a jelek halmazából legalább két csoport felhasználásával kell képezni, a jelszó 12 hónapig és legalább 4 jelszóváltásig nem ismételhető;

c) Speciális karakterek használata a jelszavak képzésében nem engedélyezett, (pl.: *,?,%,",stb.)

d) a jelszó maximális élettartama 3 hónap;

e) a jelszó 7 sikertelen kísérlet után zárolásra kerül;

f) a központi jelszó megadása utáni első bejelentkezéskor kötelező a jelszó cseréje;

g) a számítógépes rendszerekben a jelszavakat nem lehet nyílt formában tárolni. A jelszófájlokat megfelelő kódolási védelemmel kell ellátni.

Automatikus bejelentkezési eljárások (pl. batch-fájlok vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót. A felhasználói azonosítók és jelszavak csak kódolt formában tárolhatók. Felhasználói azonosítók, jelszavak, kriptográfiai kulcsok és az ezekhez tartozó jelszavak nyomtatott formában, lezárt, lepecsételt borítékban, lemezszekrényben tárolhatók. A lezárt borítékot a lezárónak alá kell írni a lezárás dátumának feltüntetésével. Ha a Kórházi felsővezetők felhasználói azonosítóit, jelszavait, illetve kódoló titkos kulcsait, személyes aláírói tanúsítványait vagy az ezekhez tartozó jelszavakat tárolni kell, akkor azt az EIRF által meghatározott helyen lezárt, lepecsételt borítékban kell őrizni. Különösen védendő munkaállomásokon mérlegelni kell a chipkártyás, illetve biometrikus vagy más azonosítás alkalmazását.

Ha a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal köteles módosítani azt.

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.

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

A felhasználó felel az azonosítójával és jelszavával az elektronikus információs rendszerben végrehajtott műveletekért.

A felhasználó gondoskodik a felügyelet nélkül hagyott eszközök megbízható védelméről. A felhasználó által használt helyiségben felállított és a hosszabb időre felügyelet nélkül hagyott berendezéseknél – többek között munkaállomásoknál vagy szervereknél – szükség esetén külön védelmet kell alkalmazni az illetéktelen hozzáférés megakadályozására.

Azokban a rendszerekben, ahol lehetőség van rá, biztosítani kell a hosszabb ideig inaktív munkaállomások rendszer által kikényszerített kijelentkezését vagy a berendezés blokkolását (lock), pl. 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).

12.3 Külső személyek hozzáférése, a hozzáférés feltételei

A külső személyek számára is hozzáférhető elektronikus információs rendszerek és eszközök biztonságának fenntartása érdekében a hozzáféréseket minden esetben ellenőrizni kell. Az ellenőrzésért a Szent Rókus Kórház és Intézményei részéről felelősként, kapcsolattartóként meghatározott szervezeti egység vezetője – ha a szerződésben nem került feltüntetésre, úgy a szerződést kötő szervezeti egység vezetője – a felelős.

A biztonsági kockázatokat és az ellenőrzés, valamint a felügyelet követelményeit fel kell mérni. A felmérésért a szerződést – szakmai oldalról – előkészítő személy a felelős. A külső személlyel megkötött szerződésben egyértelműen meg kell határozni az előzőekhez kapcsolódó elvárásokat.

A jelen szabályzat előírásainak betartása az ilyen szerződések létrejöttének, valamint az adatfeldolgozási vállalkozási szerződés megkötésének elengedhetetlen feltétele.

Külső személynek ideiglenes hozzáférési lehetőséget csak engedélyeztetési eljárás lefolytatásával lehet biztosítani. A hozzáférési engedélyt minden esetben csak a szervezeti egység vezetője kérheti. Az EIRF a biztonsági előírások figyelembevételével dönt az engedély megadásáról, a kiadott engedély másolatát átadja a hatáskörrel rendelkező szervezeti egységnek. A hozzáférést mindaddig ki kell zárni, amíg a szükséges ellenőrzést el nem végezték, illetve szerződésben nem határozták meg a hozzáférés feltételeit. A visszavonás és a lejárat időpontját minden esetben szerepeltetni kell a hozzáférési engedélyben.

A külső személyek hordozható számítógépein és más informatikai eszközein tárolt – a munkavégzés során megszerzett és a Kórházzal kapcsolatos – adatokat a munkavégzés befejezése után visszaállíthatatlanul törölni kell, amiről a partnernek – a szerződéses kapcsolat lezárásának feltételeként – írásos nyilatkozatot kell tennie.

12.4 Helyszíni tevékenységet végző külső vállalkozók

A szerződéses vagy egyéb jogviszony alapján helyszíni tevékenységet végző külső személyek által okozott biztonsági gyengülés megelőzése érdekében:

a) a külső személlyel kötött szerződésekben ki kell kötni a Kórház ellenőrzési jogosultságát;
b) a külső személyek helyszíni tevékenységének informatikai biztonsági ellenőrzése során a munkahelyi vezetőnek együtt kell működnie az EIRF-el;
c) az EIRF -nek – még a munka megkezdése előtt – meg kell vizsgálnia a külső személyek várható helyszíni tevékenységét; a külső vállalkozó számára jelen szabályzatban foglalt biztonsági szabályok ismerete és betartása kötelező.

13 Vírusvédelem, mentés, naplózás, hibakezelés szabályai

13.1 Védelem a rosszindulatú programok ellen, vírus-ellenőrzési mechanizmus előírása

Törekedni kell a rosszindulatú programok (vírusokkal fertőzött termékek, hálózati férgek, trójai programok, malware –ek, ransomware-ek, logikai bombák stb.) megfelelő intézkedésekkel történő megakadályozására, illetve kiszűrésére.

A felhasználók számára az IFO vezetője kötelező oktatást szervez a rosszindulatú és engedély nélküli programok alkalmazásával járó veszélyekről. A Kórházi munkatársak felhasználói oktatása kitér a vírusvédelmi rendszer működésére is.

AZ IFO vezetője gondoskodik a rosszindulatú programok kiszűrésére és megelőzésére alkalmas ellenőrző eszközök alkalmazásáról, beszerzéséről.

A rosszindulatú programokkal szembeni védekezés része a szűrés és a programok bevezetése előtti ellenőrzés, a felhasználók tájékoztatása és oktatása, a hozzáférés-védelem, továbbá a változtatások felügyelete és ellenőrzése. Ennek során szükséges:

a) az olyan eszközök alkalmazása, melyek megkövetelik a jogtiszta programok használatát, és tiltják az engedély nélküli termékek alkalmazását;
b) a külső hálózatokból vagy azokon keresztül és egyéb adathordozókról telepített adatállományok és programok felhasználásával járó kockázat elhárításához szükséges intézkedések bevezetése;
c) a rosszindulatú programokat felismerő és megsemmisítő programok telepítése és rendszeres frissítése;
d) az operációs rendszerek aktuális frissítéseinek telepítése a szerver és kliens oldalon egyaránt,
e) az alkalmazások aktuális frissítéseinek telepítése a szerver és kliens oldalon egyaránt,
f) a kritikus folyamatokat támogató rendszerek adattartalmának és programjainak rendszeres vizsgálata;
g) a bizonytalan eredetű adatállományok ellenőrzése, vírusok kiszűrése;
h) az e-mail kiterjesztések, csatolt dokumentumok és letöltések használat előtti ellenőrzése;
i) a vírusokkal szembeni védelemre vonatkozó feladatok és eljárások meghatározása, alkalmazásuk oktatása, a vírustámadások naplózása és az eredeti állapot helyreállítása;
j) a megfelelő üzletmenet-folytonossági terv összeállítása, a szükséges adatállományok és programok back-up példányainak és a helyreállítás eljárásainak elkészítése;
k) a hamis vagy hamisított programra vonatkozó összes információ ellenőrzése, a figyelmeztető tájékoztató kiadványok folyamatos frissítése, meglétének ellenőrzése.

AZ IFO kijelölt informatikusának feladata a vírusvédelmi rendszer oly módon történő konfigurálása, hogy:

a) minden kimeneti és bemeneti eszköz, valamint csatorna esetében folyamatos legyen a valósidejű vírusfigyelés;
b) a vírusvédelmi szoftver vírustalálat esetén a vírust távolítsa el az érintett fájlból, vagy a fájlt helyezze karanténb
c) a vírusvédelmi szoftver vírusincidens esetén értesítést küldjön az IFO kijelölt informatikusának/informatikusainak;
d) a kliens gépeken teljes víruskeresés történjen, legalább heti egy alkalommal, olyan időszakban, amikor a legtöbb kliens gép be van kapcsolva, de a gépek leterheltsége a lehető legkisebb (pl. a hét közepén, ebédidőben vagy éjszaka).

Amennyiben a vírusvédelmi rendszert szerződött partner üzemelteti, úgy a vírusvédelmi feladatokat a kijelölt informatikus a külső partnerrel együttműködve végzi.

Az informatikai üzemeltetésért felelős informatikus értesíti a felhasználókat a rendszerhibát okozó láncievelekről, illetve az illegális programok használatának veszélyeiről, továbbá

folyamatosan figyelmezteti a felhasználókat a frissen megjelent fenyegetésekről. A felhasználót a gépén tárolt illegális programokért felelősségre kell vonni!

Központosított hálózati felhasználó adminisztrációt, Actív Directory-t (továbbiakban:AD) kell kialakítani – az egyenrangú hálózatokat fel kell számolni – a felhasználókat tartományba kell bejelentkeztetni.

Szerverek esetén alkalmazandó vírusvédelmi eljárások:

a) Minden szerverhez, amelyhez kereskedelmi forgalomban beszerezhető vírusvédelmi szoftver, azt be kell szerezni, és telepíteni kell. Biztosítani kell, hogy a szerveroldali vírusvédelmi szoftver, víruskereső motor és vírusminta adatbázisa automatikusan frissüljön.

b) A levelező szerver esetében a levelezésért felelős alkalmazásba beépülő, a levélforgalom vizsgálatát végző vírusvédelmi szoftvert kell alkalmazni.

Biztosítani kell, hogy hetente minden, víruskereső szoftverrel ellátott szerveren és kliensen teljes víruskeresés fusson le, de lehetőleg különböző időpontokban.

Az elektronikus levelezés biztonsági irányelveinek érvényesítéséről a levelező rendszer üzemeltetője felelős. Az irányelvek a következők:

a) a folyamatos üzembiztonság megvalósítása;

b) az elektronikus küldemények adatintegritásának megtartása;

c) a levelezőrendszer vírusvédelmének biztosítása és folyamatos frissítése;

d) az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelme szoftverfrissítések, service pack-ok és security-patch fájlok telepítése).

13.2 Adatmentési, archiválási feladatok

A mentési és visszaállítási eljárásokat úgy kell kialakítani, hogy az üzemeltetett rendszerek előre nem látható esemény (katasztrófa vagy hardver, illetve szoftver meghibásodása, emberi mulasztás) bekövetkezte után, szükség esetén helyreállíthatók legyenek, biztosítva a folyamatos napi működést. Biztosítani kell, hogy az üzemidőkiesés, adatsérülés, adatvesztés minimális legyen.

AZ IFO osztályvezető által elkészített mentési rendet folyamatosan karban kell tartania. A mentési rendet legalább évente egyszer, november 1-15. között felül kell vizsgálnia. A mentési rendet mentési egységenként kell készíteni, és táblázatba kell foglalni. A kinyomtatott mentési rendet az érintett szervezeti egység vezetőjének és az IFO vezetőjének kézjegyével kell hitelesítenie.

A mentés ütemezését mentési egységenként lehetőleg úgy kell kialakítani, hogy a mentés a munkafolyamatokat, a munkafolyamatok a mentési eljárást ne akadályozzák.

A biztonsági mentés a napi adatbiztonságot szolgáló, rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a napi munka során felmerülő kisebb meghibásodásokból származó adatvesztések, adatbázis-konzisztenciahibák megszüntetését a lehető legkisebb időráfordítással.

A biztonsági mentés:

a) egy másik szerverre (azonos tűzszakaszban elhelyezett);

b) vagy az adott szerverbe beépített tartalék HDD-re;

A biztonsági mentés során ellenőrizni szükséges a mentésről készített digitális naplót vagy meg kell győződni a mentés megtörténtéről. E mentésfajta használata mellett biztosítani kell

egy tűzvédelmi mentést is. Ahol napi rendszerességgel készül tűzvédelmi mentés, ott a biztonsági mentés elhagyható.

A tűzvédelmi mentés az adatbiztonságot szolgáló, rendszeresen készülő mentésfajta (szerveren vagy munkaállomáson), amely biztosítja a súlyosabb meghibásodásokból származó (katasztrófa, hardver-, illetve szoftver meghibásodás esetén történő) rendszerösszeomlások, adatvesztések, adatbázis-konzisztenciahibák megszüntetését, a lehető legkisebb időráfordítással. A tűzvédelmi mentés történhet egy másik szerverre, ha az nem azonos tűzszakaszban található a mentett eszközzel (hálózaton keresztül történő mentés). Használata esetén a következőket kell biztosítani:

a) a mentés sikerességét ellenőrizni kell;

b) a mentés során használt adathordozónál biztosítani kell a mentési adathordozók rendszeres váltott cseréjét;

c) figyelemmel kell lenni az adathordozók felhasználhatóságának paramétereire (pl.: hányszor írható);

d) biztosítani kell az adathordozók előírás szerinti tárolását.

Ahol a hálózaton keresztüli mentés nem biztosított, ott a mentési rendben foglaltak szerint hordozható adattárolóra kell menteni, és az adattárolót másik tűzszakaszban kell biztonságosan tárolni.

Egyedi mentéssel kell biztosítani azon munkaállomások és mobil eszközök háttértárolóin keletkezett alkalmazások és felhasználói állományok (levelezés, dokumentumok, egyedi adatállományok és programok) mentését, melyekről

a) nem történik rendszeres napi mentés a hálózatra;

b) vagy az eszközzel kapcsolatban egyedi mentési igény merül fel;

c) azon hálózati közös meghajtók rendkívüli mentését, amelyre vonatkozó igény a tárkapacitás túlterheltsége miatt merült fel.

d) Ezen feladatokért a szervezeti egység vezetője, valamint a munkaállomáson adatokat tároló felhasználók a felelős.

A hálózaton tárolt telepítő készletek és programok mentéséről folyamatosan gondoskodni kell.

Valamennyi mentésről mentési és archiválási nyilvántartást (naplót) kell vezetni a mentési feladatban résztvevő informatikusnak.

Egyedi mentésnél a mentés elvégzéséről egyedi mentési és archiválást kell készíteni, és azt a mentési és archiválási nyilvántartáshoz kell csatolni. A mentett állomány törlését, ha szükséges, csak ezt követően lehet elvégezni.

Az adatlapokat és a nyilvántartást a mentés helyétől és az adathordozók tárolási helyétől különböző mentéssel kapcsolatos adatlapokat és nyilvántartást az EIRF legalább évente egyszer szúrópróbaszerűen ellenőrzi.

A mentés elkészítéséhez használt adathordozó típusok kiválasztásánál az alábbiakat kell figyelembe venni:

a) a mentendő adatmennyiségnek megfelelő tárolókapacitás;

b) a megfelelő adatmegőrzési idő (legalább 5 év, különleges beavatkozás, speciális eljárások alkalmazása nélkül);

c) megfelelő ellenállás a környezeti viszonyoknak (hőmérséklet, páratartalom, fény stb.);

d) adatvisszaállítás esetére szükséges eljárások és eszközök rendelkezésre állása.

AZ IFO kijelölt informatikusának az adathordozó típusától, valamint a rögzítés módjától függően eltérő időközönként, de évente legalább egyszer ellenőrizni kell az adathordozó használhatóságának mértékét.

13.3 Biztonsági naplózási feladatok

Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert kell kialakítani, hogy utólag megállapíthatók legyenek az elektronikus információs rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ellenőrizhetővé kell tenni a hozzáférések jogosultságát, megállapíthatóvá kell tenni a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy annak kísérletét.

AZ IFO vezetője a Szent Rókus Kórház és Intézményei informatikai rendszerének megfelelő működése és biztonsága érdekében a számítógépes hálózatot, valamint az Internet-szolgáltatást monitorozhatja. Az Internet-használat ellenőrzése csak az Adatvédelmi Szabályzatban foglaltak szerint valósulhat meg.

Az elektronikus információs rendszer által naplózott rendszergazdai tevékenységek naplóit legalább 30 napig meg kell őrizni.

A Szent Rókus Kórház és Intézményei informatikai infrastruktúrájában lévő rendszereknek képesnek kell lenniük minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására, de legalább a következő események regisztrálására:

a) rendszerindítás, -leállás, -leállítás;

b) rendszerhiba és korrekciós intézkedés;

c) programindítás és -leállás, -leállítás;

d) felhatalmazott személy azon művelete, amely a rendszer biztonságát érinti.

A rendszer valamennyi, időinformáció kezelésére alkalmas elemének egységes időalapot kell biztosítani.

Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.

Az üzemzavarok elhárítása érdekében, a bejelentést követően az EIRF korrekciós intézkedést kezdeményez. A felhasználók által jelentett, az adatfeldolgozás vagy átviteli rendszerek működésében észlelt hibákat naplózni kell.

Az üzemzavar kezelése során az EIRF megvizsgálja a hibanaplót, ellenőrzi a hiba kezelését, elhárítását, megvizsgálja a korrekciós intézkedéseket, ellenőrzi ezek végrehajtásának és a kezdeményezett intézkedések engedélyezésének szabályosságát.

13.4 Hibakezelési, hibaelhárítási rendszer

A Szent Rókus Kórház és Intézményei az informatikai infrastruktúra vonatkozásában un. e-HelpDesk (továbbiakban e-HD) elektronikus hibabejelentő rendszert üzemeltet.

A hibaelhárításra vonatkozóan a kijelölt informatikus feladata, hogy szükség esetén gondoskodjon az eszköz javításáról, az eszköz helyettesítéséről, az eszköz szervizbe szállításáról.

A kijelölt informatikus feladata, hogy folyamatosan tájékoztassa az érintett felhasználót az eszköz javítási folyamatáról, illetve sorsáról.

Olyan esetben, ha a hiba a Kórház rendszereinek működésére komoly kihatással van (pl. üzembiztonságot veszélyeztető helyzet, katasztrófahelyzet áll fenn), vagy más jellegű, de

rendkívül fontos eset következik be (pl. bűncselekmény gyanúja áll fenn) az észlelő köteles haladéktalanul értesíteni az IFO vezetőjét.

14 Külső és belső informatikai hálózatokkal kapcsolatos szabályok

14.1 Hálózatmenedzsment

A hálózatmenedzsment célja a hálózatok adattartalma biztonságának és az infrastruktúra védelmének meghatározása.

A hálózat felügyeletét az IFO informatikusai, illetve az üzemeltetésbe bevont partner megbízottjai látják el, együttműködve a Nemzeti Infokommunikációs Szolgáltató Zrt. és a Magyar Telekom munkatársaival.

A Szent Rókus Kórház és Intézményei közvetlen szervezeti és fizikai felügyeletén kívül eső kapcsolatok esetében kriptográfiai módszereket (kódolás, digitális aláírás, SSL/TLS, https stb.) kell használni.

Gondoskodni kell olyan ellenőrző eszközökről, amelyek biztosítják a hálózatokban kezelt és továbbított adatok – a biztonsági osztálynak megfelelő – biztonságát, valamint a kapcsolt szolgáltatásokat megóvják az illetéktelen hozzáférésektől.

A nyilvános hálózatokon keresztül továbbított adatok és a kapcsolt rendszerek védelmére pótlólagos ellenőrző eszközöket kell alkalmazni.

AZ IFO vezetője meghatározza a hálózat határait, és gondoskodik a hálózat biztonságos szegmentálásának kialakításáról.

A Szent Rókus Kórház és Intézményei belső informatikai rendszeréhez való, nyilvános internet felőli hozzáféréshez (VPN kapcsolat) az IFO vezetője felé, az adott szervezeti egység vezetője által benyújtott írásos és indoklással ellátott kérelemmel igényelhető jogosultság. Ez a kapcsolat kizárólag biztonságos csatornán keresztül létesíthető.

A különböző felhő alapú szolgáltatók (Dropbox, Google Drive, Onedrive) tárhelyeinek kórházi eszközről és a kormányzati gerinc hálózatról történő használata, illetve az ezzel összefüggésben lévő kórházi email címmel (pl.: rokus.hu) történő regisztráció, valamint a tárhelyen a kórházi munkaanyagok elhelyezése kiemelt kockázati tényezőnek tekintendő és szigorúan tilos!

Vezeték nélküli kapcsolat (Wi-Fi) a Kórház területén csak az IFO Osztályvezető engedélyével létesíthető egyedi tervezés, megvalósítás, nyilvántartás, ellenőrzés mellett. SOHO eszköz nem használható, ajánlott megolások: ARUBA, CISCO, speciálisan konfigurált open WRT:

A vezeték nélküli kapcsolatot legalább WPA2-PSK titkosítással kell létrehozni.

Vezeték nélküli hálózat és a Kórház vezetékes hálózata között átjárás csak szabályozottan engedélyezett, a két hálózat között biztosítani kell a teljes szeparáltságot.

Vezeték nélküli hálózaton keresztül elektronikai információs rendszer elérése nem lehetséges, kivéve ha rendkívüli helyzetben az elérés szükségessége igazolható. Ilyen esetben az EIRF írásban engedélyezheti a hozzáférést.

14.2 Az elektronikus levelezés biztonsága

Az elektronikus levelezés biztonságának szabályozásakor a következő fenyegetettségeket kell figyelembe venni:

a) az üzenetek illetéktelen elérésének, vagy módosításának, vagy a szolgáltatás megtagadásának veszélye;

b) az emberi hibákból eredő veszélyeztető tényezők (pl. rossz címzés vagy irányítás);
c) az érzékeny adatok továbbításának lehetősége és ennek veszélyei;
d) a feladó- és címzett hitelesítési problémák és a levél átvételének bizonyítása;
e) a kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek;
f) távolról bejelentkező felhasználó biztonsági problémái.

Az elektronikus levelezés biztonsági irányelvei:

a) a levelezőrendszer vírusvédelmét folyamatosan frissíteni kell, valamint követni kell az új mail vírusok megjelenését;
b) az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni az új szoftverfrissítések, service packok és security-patch fájlok megjelenését);
c) az elektronikus levelező rendszeren keresztül történő támadások esetén, ha a rendszer védelme átmenetileg nem biztosított – pl. olyan vírusfenyegetettség esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet – a belső hálózaton (intraneten) kívül eső elektronikus levélforgalom ideiglenes leállításáról az EIRF gondoskodik, és erről a főigazgatót és a kórházi munkatársakat tájékoztatja;
d) definiálni kell a felhasználók felelősségét;
e) a nem hitelesíthető, kétes forrásból származó üzeneteket ki kell vizsgálni, az elektronikus levelezés forgalmát – a technikai lehetőségek szerint – tartalmilag szűrni kell, a bizalmas adatok kiszivárgásának elkerülése érdekében minden felhasználót fel kell világosítani arról, hogy a Kórház levelezőrendszerén tárolt és továbbított levelek a Kórház tulajdonát képezik, ezért a kórházi szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van;
f) a Kórház levelezőrendszere reklám, valamint egyéb üzleti célokra nem használható;
g) a levelezőrendszer elérése csak védett (hiteles és kódolt) csatornán (pl. https) keresztül valósítható meg. A hozzáférés csak jelszavas védelmen keresztül történhet. A felhasználó felügyeleti lehetőségein kívüli (például nyilvános, idegen tulajdonú) munkaállomások, terminálok használata esetén csak ennek megfelelő üzemmódban szabad bejelentkezni.

A felhasználók személyes és szakmai postafiókjának mobil eszközről történő elérése külön a szervezeti egység vezetőjének engedélyéhez kötött.

Az egyes osztályok kérésre szakmai e-mail címeket kaphatnak. A szakmai e-mail címeinek személyes elérésével, jogosultsági kérdéseivel kapcsolatban a osztály vezetője, mint adatgazda dönt. A szakmai címek mobil eszközről elérése szintén külön a szervezeti egység vezetőjének engedélyéhez kötött.

A szakmai címek elérését az érintett szervezeti egység vezetőjének/adatgazdájának engedélyével az IFO informatikusai aktiválják/deaktiválják.

A felhasználók a Szent Rókus Kórház és Intézményei levelező rendszerében személyes postafiók címet kapnak, amelynek kezeléséről maguk gondoskodnak (archiválás, törlés, testre szabás). A Szent Rókus Kórház és Intézményein belül ezeket a postafiókokat kell használni az elektronikus kommunikációra és kapcsolattartásra.

A felhasználóknak rendszeres ellenőrzés és archiválás útján gondoskodniuk kell arról, hogy a személyes postafiókjuk mérete ne lépje túl az engedélyezett keretet. Megfelelően alátámasztott indok és írásban az IFO osztályvezetőjének benyújtott, engedélyezett kérelem alapján az elektronikus postafiók kerete (Quota) emelhető.

A szakmai postafiókok esetében szükséges egy elsődleges felhasználó kijelölése. Ezt a kijelölést az osztály vezetője/adatgazdája teszi meg. Az elsődleges felhasználó kötelessége naponta egyszer ellenőrizni a szakmai postafiók méretét, tartalmát, szükség esetén e-mailben jelezni az IFO informatikusai felé az archiválási igényt. A postafiók adatainak mentéséért a postafiók felhasználó felelős.

Az elektronikus levelezés során a hivatalos és a személyes postafiókokat vírusvédelmi rendszer védi. Az elektronikus postafiókba érkező, ismeretlen feladótól (gyanús, értelmezhetetlen vagy külföldi) származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, illetve idegen nyelvű küldeményekkel – a fennálló vírusveszély miatt – fokozott óvatossággal kell eljárni. Gyanús küldemény érkezésekor, illetve a vírusvédelmi rendszer riasztása esetén haladéktalanul értesíteni kell az EIRF-t. A csatolmányt ilyen esetben tilos megnyitni. Nem engedélyezett a lánclevelek indítása vagy továbbítása.

A munkavégzésre irányuló jogviszony megszűnésekor, illetve munkakör változáskor az elektronikus levelezési fiókkal kapcsolatos feladatok:

a) a postafiókot a felhasználó számára azonnal elérhetetlenné kell tenni (pl. jelszómódosítással);
b) gondoskodni kell a helyettesítésről, vagy a postafiókba érkező levelek továbbításáról;
c) gondoskodni kell a feladó automatikus értesítéséről a levelezési fiók megszűnéséről;
d) a jogviszony megszűnésének napjától számított 30 napig meg kell őrizni a felhasználó elektronikus levelezését;
e) megőrzendők továbbá azok az elektronikus levelek, amelyek fegyelmi, büntető vagy polgári eljárások alapját képezhetik az eljárás befejezéséig.

14.3 Az Internet használatának rendje

A szakmai feladatok hatékony ellátásához szükséges információkhoz, szolgáltatásokhoz való hozzáférés érdekében a Szent Rókus Kórház és Intézményei valamennyi felhasználója jogosult a munkahelyi Internet, intranetes portál használatára. A munkahelyi eszközökön az Internet szolgáltatásait kizárólag csak a munkaköri feladatok ellátásához lehet igénybe venni, személyes célokra nem. Tekintettel arra, hogy az Internethasználat a munkáltató által biztosított infrastruktúrán és szolgáltatási költségen valósul meg, a Szent Rókus Kórház és Intézményei jogosult bármikor bármilyen weblap, internetes szolgáltatás elérésének korlátozására, vagy teljes kizárására.

A hálózat számára nagy terhelést jelentő kép- (pl. grafikus fájl, video) és hang- (pl.: *.mov,*.mp3, *.avi, *.wav. stb.) információkat tartalmazó anyagok letöltése, továbbítása csak az IFO kijelölt informatikusával egyeztetve engedélyezett.

A felhasználók a Kórház nevében nem tölthetnek fel engedély nélkül az Internetre adatot és anyagot (pl. Szent Rókus Kórház és Intézményei honlap, hirdetmények, cégkapu esetében).

A Szent Rókus Kórház és Intézményei tulajdonát képező szoftverek Interneten, vagy e-mailen keresztül történő továbbítása, mások részére való hozzáférhetővé tétele – külön engedély hiányában – nem engedélyezett.

Jogilag és erkölcsileg kifogásolható tartalmú oldalak látogatása, tiltott tevékenységek végzése a Szent Rókus Kórház és Intézményei informatikai rendszerében nem engedélyezett. Kivételt képeznek azok a felhasználók, akik munkájuk jellege miatt (pl. a jogsértések feltárása érdekében) erre engedélyt kapnak. Tiltott tartalmú oldalak és tiltott tevékenységek különösen a következők:

– szexuális tartalmú oldalak, különösen az alábbi tartalmakkal: kiskorúak veszélyeztetése,

- erőszak, brutalitás
- pornográf marketin tevékenységek
- az emberi méltóság megsértése;
- rasszizmus;
- szexuális beállítódás, vallás, nemzetiség vagy etnikai származás miatti megkülönböztetés;
- gazdasági biztonság veszélyeztetése;
- csalás;
- tiltott kereskedelmi tevékenység;
- bank- illetve hitelkártyával való visszaélésben való közreműködés;
- rémhírterjesztés;
- információbiztonság veszélyeztetése;
- rossz szándékú hackertámadás;
- hacker, cracker technológiák és leírásuk, eszközök terjesztése, használata;
- vírusprogramok terjesztése, írása;
- a magánszféra megsértése;
- személyes adatokkal való visszaélés;
- elektronikus zaklatás;
- a személyiségi jogok megsértése;
- rágalmazás;
- meg nem engedett összehasonlító reklám;
- a szellemi tulajdon megsértése;
- tiltott szerencsejáték;
- a szerzői jog által védett digitális anyagok (művek, szoftverek, zenék stb.) jogosulatlan terjesztése;
- bombák készítéséhez adott segítségnyújtás;
- illegális kábítószer használat, előállítás és terjesztés;
- nemzetbiztonsági kérdések;
- terrorista tevékenység;

Azoknak a felhasználóknak, akiknek a munkaköréhez tartozóan indokolt a tiltott tartalmú oldalak látogatása, külön igény alapján az IFO osztályvezetője biztosítja a hozzáférés körülményeit, erről nyilvántartást vezet.

A Szent Rókus Kórház és Intézményei által üzemeltetett hálózaton keresztül Internetes hozzáféréssel rendelkező felhasználók esetén az igénybevétel jogszerűségének ellenőrzésére az EIRF jogosult. Ha az ellenőrzés során nem indokolható Internethasználatot észlel, erről soron kívül tájékoztatja az érintett felhasználót és az érintett felhasználó közvetlen vezetőjét, mely tájékoztatás alapján a felhasználó közvetlen vezetője dönt az Internet igénybevételi lehetőségének megszüntetéséről, és erről soron kívül tájékoztatja az IFO vezetőjét.

Az igénybevétel jogszerűségének vagy jogszerűtlenségének megállapítására irányuló eljárás során az érintettnek lehetőséget kell adni arra, hogy a szakmailag indokolatlannak tűnő Internethasználat munkaköri feladatainak ellátásához szükséges voltát bizonyítsa.

A Szent Rókus Kórház és Intézményei által biztosított e-mail cím csak a munkakör ellátásához kapcsolódó regisztrációs folyamatokhoz használható.

AZ IFO a Szent Rókus Kórház és Intézményei hálózati infrastruktúráját és a folyamatos üzemmenetet veszélyeztető hálózati műveleteket korlátozhatja vagy letilthatja.

14.4 Az On-line Központi Adattárak kezelésének szabályai

On-line Központi Adattárak (továbbiakban: OKA) körébe tartoznak:

a) Cégkapu;
b) Magyar Államkincstár KIRA rendszere
c) MÁK netbank
d) NEAK TAJ ellenőrzési rendszere
e) NEAK EESZT rendszerei
f) NEAK OJOTE rendszere
g) NEAK Várólista rendszere
h) GIRO
i) Nemzeti Rákregiszter
j) ÁEEK ügykörök
k) ÁEEK-VIR
l) NEXON-Ihr
m) implantátum regiszter
n) ágyszámregiszter

és az egyéb jogszabályokban meghatározott kapcsolatok.

Az OKA-val kapcsolatos fontos biztonsági szabályok:

a) Az OKA rendszereit kizárólag a Kórház irodahelyiségében elhelyezett Kórházi munkaállomásról szabad kezelni (idegen eszközről, otthonról nem megengedett);
b) Az OKA-ról érkezett dokumentumokat az OKA felelősnek az adott szervezeti egység hálózati meghajtóján kijelölt mappába (a továbbiakban: e-Tárhelyre) kell letöltenie.

Az adott szervezeti egységnél a kijelölt informatikus feladata az e-Tárhely mappa biztonságának kialakítása, kezelése, az OKA felelősök és iktatók e-Tárhelyhez kötődő jogosultságainak biztosítása, a mentések, archiválások elvégzése. A mentések javasolt gyakorisága:

- napi mentés a helyi szerverre;
- havi mentés CD, DVD lemezre, NAS tárolóra vagy DAT kazettára.

AZ IFO Osztályvezető feladata a Szent Rókus Kórház és Intézményei elektronikus űrlapjainak elkészítése, a hozzá tartozó publikus és titkos kulcsok generálása, valamint a publikus kulcsok e-Tárhelyen, az elektronikus űrlapok és a kapcsolódó fájlok honlapon való publikálása.

A cégkapu kapcsolattartó feladata a cégkapu felelősök értesítése az üzemszünetekről, technikai változásokról, beérkezett anyagokról.

14.5 Nyilvános rendszerek használatának rendje

Nyilvános rendszerben (pl. egy Interneten keresztül elérhető webszerveren) a fokozott integritást igénylő számítástechnikai programok, adatok és egyéb információk védelméhez megfelelő eszközökre – pl. digitális aláírás alkalmazására – van szükség. Az elektronikus hirdető rendszereknél – különösen azoknál, amelyek lehetővé teszik a visszajelzést és az információ közvetlen beléptetését – megfelelő eszközökkel kell gondoskodni a következőkről:

a) az információ megszerzésének módja feleljen meg az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseinek;

b) időben kerüljön sor a rendszerbe bekerülő információ pontos és hiánytalan feldolgozására;

c) az adatok kezelése (gyűjtés, tárolás, feldolgozás) során gondoskodni kell az adatok, valamint az elektronikus információs rendszerek védelméről;

d) a rendszerhez való külső hozzáférés ne tegye lehetővé az illetéktelen hozzáférést azokhoz a belső hálózatokhoz, amelyekhez a rendszer csatlakozik.

14.6 VPN kapcsolat, Mobil informatikai tevékenység, távmunka

Mobil informatikai eszközökön – az elektronikus levelezéshez való hozzáférésen kívül – távoli hozzáféréssel végzett munka kizárólag az IFO vezetőjének engedélyével, indokolt esetben, írásbeli kérelem alapján történhet.

A Szent Rókus Kórház és Intézményei hálózatában csak az érintett szervezeti egység vezetőjének javaslata alapján, az IFO vezetőjének engedélyével, az általa ellenőrzött eszközökkel, az általa megadott módon végezhető távmunka.

A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot. A szükséges védelemnek összhangban kell lennie a munkavégzés kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. Távmunka, távoli hozzáférés esetén a Kórház érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely védelméről.

A mobil informatikai eszközök nem hagyhatók felügyelet nélkül, ha nem biztosítható azok előírt védelme. Ki kell alakítani a mobil informatikai eszközök megfelelő fizikai védelmét, és a kommunikációhoz védett csatornáról kell gondoskodni. Vírus- és behatolásvédelmi eszközöket kell biztosítani a mobil eszközökre. Fokozott figyelmet kell fordítani a mobil eszközökön tárolt adatok bizalmasságának védelmére. A távoli elérésre vonatkozó szabályokat a mobil informatikai eszközökre is alkalmazni kell.

A távoli hozzáféréssel végzett munka esetén is gondoskodni kell a biztonsági követelmények és előírások betartásáról, valamint a megfelelő és rendszeres ellenőrzésről. A távmunkához használt informatikai eszközök tekintetében gondoskodni kell arról, hogy a munkavégzéshez szükséges mértékben és időben szabad adatokat tárolni. Az informatikai eszközökhöz való hozzáférést és az adatokhoz való hozzáférést korlátozni kell a munkavégző jogosultságainak megfelelően a minimálisan szükséges jogokra.

Az EIRF az éves ellenőrzések során szúrópróbaszerűen ellenőrzi a távmunka igénylések jogosságát és megfelelőségét, valamint a dokumentációt.

15 Adatok továbbításának, védelmének szabályai

15.1 *Adathordozókhoz kapcsolódó általános védelmi intézkedések*

Az eszközök károsodásának megelőzése és a tevékenységben okozott fennakadás megakadályozása érdekében:

a) gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről;

b) meg kell előzni a dokumentumok, a számítástechnikai adathordozók (szalagok, lemezek, kazetták, flash drive-ok, stb.), az input/output adatok és a rendszerdokumentációk károsodását, eltulajdonítását és engedély nélküli törlését;

c) szabályozni kell az adathordozók beszerzését, tárolását és kezelését;

d) biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében – a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjék;

e) az adathordozókat használatba venni csak az előírt ellenőrző eljárások (pl. vírusellenőrzés) elvégzése után szabad;

f) minden adathordozót újra alkalmazás előtt vagy selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell;

g) az adatok sértetlen és hiteles állapotának megőrzését biztosítani kell.

Az iratkezelés által érintett adathordozókat biztonságos módon kell kezelni az iratkezelési szabályzat és a biztonsági szabályzat előírásainak megfelelően.

Az adathordozókat – azokat is, amelyek használaton kívül vannak – biztonságos helyen kell tárolni, vagy amennyiben munkaközi példányok, azokat vagy helyreállíthatatlanul törölni kell, vagy meg kell semmisítenie az adathordozó birtokosának, és arról jegyzőkönyvet kell készítenie az iratkezelési szabályzatnak megfelelően.

Adathordozónak minősül:

a) a kinyomtatott dokumentum;

b) a hang- vagy egyéb adatrögzítés;

c) az egyszer használatos nyomtatószalag;

d) a mobil diszk és kazetta, mágnesszalag;

e) a CD, DVD vagy más tárolóeszköz (pendrive, rádiótelefon, memóriakártya stb.);

f) a programlista; a tesztadat;

g) a rendszerdokumentáció.

Az érzékeny adatokat, mentéseket, archiválásokat tartalmazó adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces tűzállósági tároló szekrényben történhet.

Az adatok illetéktelen közzétételének, illetve felhasználásának megakadályozása érdekében szükségesek az adatkezelést szabályozó eljárások. Ezeknek az eljárásoknak – az adatok érzékenységének megfelelően – igazodniuk kell az előírásokhoz, szabályzatokhoz, számítástechnikai rendszerekhez, hálózatokhoz, a használt számítástechnikai eszközökhöz, távközlési, hangátviteli és multimédiás stb. rendszerekhez, levelezőrendszerhez, az informatikai szolgáltatásokhoz.

15.2 Adatok és programok átadása

A szervezeti egységek között cserélt adatok és programok elvesztésének, módosításának és illetéktelen felhasználásának lehetőségét is meg kell akadályozni. Az adatok és a programok szervezeti egységek közötti átadását, cseréjét ellenőrizni kell. Az adatátadásról és programátadásról való döntés előtt mérlegelni kell az elektronikus adatcsere és az e-mail biztonsági kockázatát, annak következményeit és az ellenőrző eszközök alkalmazására vonatkozó követelményeket.

A Szent Rókus Kórház és Intézményei más szervezettel adat- és programcserét kizárólag írásos nyilatkozat (szerződés, megállapodás stb.) alapján hajthat végre, amelyben utalni kell az érzékeny információk kezelésére is.

A csere biztonsági feltételeire vonatkozó megállapodásban meg kell határozni:

a) az adatátvitel, -feladás, -fogadás és -átvétel ellenőrzésének és bejelentésének eljárási szabályait;

b) az adatok biztonságos átvitele előkészítésének és tényleges átvitelének műszaki szabványait;

c) az adatvesztéssel kapcsolatos kötelezettséget és felelősséget;

d) az adatátvitel során a biztonságos (szükség esetén kódolt) környezet előírásait minden érintett félnél;

e) az érzékeny adatok védelméhez szükséges speciális eszközök igénybevételét (pl. titkosított adattartalom, kriptográfiai kulcsok használata).

15.3 Kiszervezett üzemeltetési és adatfeldolgozási tevékenységek

A Szent Rókus Kórház és Intézményei elektronikus információs rendszereinek üzemeltetésére, adatfeldolgozására külső személlyel, szervezettel kötött vállalkozási szerződés rögzíti a Kórház ellenőrzési jogosultságát, lehetőségeit, eszközeit és eljárásait.

A szerződéskötés során figyelembe kell venni:

a) az alkalmazások és adatok érzékenységét, biztonsági osztályát;

b) a szükséges jóváhagyások beszerzését;

c) az üzletmenet-folytonosságra gyakorolt hatását;

d) a vállalkozó által alkalmazandó biztonsági szabályokat és alkalmazásokat;

e) a biztonsággal, valamint az adatkezeléssel összefüggő tevékenységek hatékony nyomon követhetőségét;

f) a biztonsági eseményekre vonatkozó jelentéstételi kötelezettséget, illetve a kezelésükre vonatkozó feladatokat és eljárásokat.

15.4 Adatok titkosítása

Olyan nyílt adatok esetében, ahol más védelmi eszközök nem nyújtanak kellő biztonságot, kriptográfiai eszközökkel és technikákkal kell gondoskodni az adatvédelemről.

Kriptográfiai rendszerekkel és technikákkal kell gondoskodni az adatok kódolásról, ha az adatokat illetéktelen személyek által is hozzáférhető helyen kell továbbítani vagy tárolni, valamint minden olyan esetben, ahol fennáll, hogy az adatok bizalmassága sérül.

Nyílt kulcsú titkosítást csak az IFO vezetőjének engedélyével lehet alkalmazni. A titkosítási rendszer kialakítása és a rendszer nyilvántartása az EIRF feladata.

A nyílt kulcsú titkosítás eszközeinek és jelszavainak kezeléséért és megőrzéséért a kulcsot alkalmazó felhasználó felelős.

A nyílt kulcsú titkosítás azonosítóit és a titkos kulcsok jelszavait az IFO kezelésében lévő páncélszekrényben, zárt borítékban kell tárolni. A boríték csak az IFO vezetőjének utasítására bontható fel.

15.5 Fáljrendszerek titkosítása

A fájlrendszerek titkosítását az IFO vezetőjének engedélyével lehet alkalmazni a mobil adathordozóknál és mobil informatikai eszközöknél.

A rendelkezésre álló szoftver telepítése és beállítása, és a titkosított rendszer használatának nyilvántartása a kijelölt informatikus feladata.

A fájlrendszer-titkosítás eszközeinek és jelszavainak kezeléséért és megőrzéséért a felhasználó felelős.

A fájlrendszer titkosításának azonosítóit és jelszavait az IFO kezelésében lévő páncélszekrényben, zárt borítékban kell tárolni. A boríték csak az IFO vezetőjének utasítására bontható fel.

Az informatikai rendszerek által is használt belső hálózaton történő adatforgalom védelmére, a távmunka során a kommunikációs vonalon rejtjelezéssel védett VPN-t kell igénybe venni.

Az alkalmazott kriptográfiai eszközöknek meg kell felelniük a magyar jogszabályi előírásoknak.

15.6 Elektronikus aláírás

Elektronikus aláírást jogszabály vagy az érintett szervezeti egység vezetőjének javaslata alapján informatikus feladatot ellátó munkatárs által történő telepítés után lehet alkalmazni.

Az elektronikus aláírás eszközeinek és jelszavainak kezeléséért, megőrzéséért a felhasználó felelős.

16 Biztonsági események és üzemzavarok kezelése

16.1 A váratlan események kezelési eljárásai

Mindazon biztonsági eseményeket, amelyek a folyamatos éles üzemet megzavarják, a napi feldolgozást hátráltatják, azonnal jelenteni kell az IFO vezetőnek. A jelentést követően az üzemzavart mielőbb meg kell szüntetni.

Mérsékelni kell a működési zavarok következményeit. Nyomon kell követni az eseményeket, biztosítani kell a mielőbbi normális üzemre való visszaállást, és a tapasztalatokat szükség esetén feljegyzésben kell rögzíteni.

Az események biztonságos kezeléséhez szükség van arra, hogy az eseményt követően nyomban összegyűjtsék a meglévő bizonyítékokat, és felterjesszék vezetőjük felé további vizsgálatok lefolytatása céljából.

A váratlan eseményre való gyors, hatékony és szabályos válaszadás érdekében meg kell határozni a váratlan eseményekkel kapcsolatos felelősségeket és eljárásokat.

A következő események kezelésére kell egyedi eljárást kidolgozni:

a) az elektronikus információs rendszer hibái és a szolgáltatás megszakadása,

b) szolgáltatás megtagadása,

c) pontatlan és hiányos adatokból származó hibás eredmények,

d) a bizalmasság elvesztése.

Az üzletmenet-folytonosság fenntartásához a következő eljárásokat kell alkalmazni:

a) azonosítani és elemezni kell az események okait,

b) terveket kell kidolgozni a nem kívánt események ismétlődésének megakadályozására,

c) az eseményeket naplózni kell,

d) gondoskodni kell a visszaállítás megoldásáról.

A biztonsági események és rendszerhibák javítását a következők szerint kell végrehajtani:

a) csak az engedéllyel és a kellő szaktudással rendelkező személyek férhetnek az „éles" rendszerekhez és azok adataihoz,

b) az adott feladatra kijelölt informatikusnak/külső partnernek ismernie és ellenőriznie kell minden, rendkívüli esemény során az IFO vezetője által alkalmazandó/alkalmazott eljárást,

c) minden rendkívüli esemény során az alkalmazandó/alkalmazott eljárást jegyzőkönyvben rögzíteni kell,

d) a rendkívüli eseményeket követően az adatok sértetlenségét haladéktalanul ellenőrizni kell.

16.2 Informatikai biztonsági események jelentése

A Szent Rókus Kórház és Intézményei munkatársa az észlelt informatikai biztonsági eseményt (betörés, lopás, tűz, víz, villámcsapás, balesetveszélyes eszköz, eszköz elvesztése vagy eltűnése, áramkimaradás, stb.) a szervezeti egység vezetőjének jelenti, valamint mindent megtesz a szükséges bizonyítékok összegyűjtésére. A szervezeti egység vezetője jelentését és a felvett jegyzőkönyvet haladéktalanul továbbítja az EIRF-nek, aki az eseményt a lehető legrövidebb idő alatt kivizsgálja, és ha a felelősségre vonás szükségessége fennáll, értesíti a munkáltatói jogkör gyakorlóját.

Biztonsági esemény esetén a szervezeti egység vezetője haladéktalanul telefonon értesíti az IFO vezetőjét vagy helyettesét, aki az esemény jellegétől függően intézkedik.

A biztonsági eseményt követően az eseményről jegyzőkönyvet kell készíteni, és azt az IFO részére írásban elküldeni (e-mail: informatika@rokus.hu). A jegyzőkönyvben rögzíteni kell az esemény részleteit, valamint az informatikai szerverteremben tartózkodók nevét, a tartózkodás időtartamát és okát.

Az informatikai rendszerekben észlelt hibák, gyanús működés esetén a felhasználó

a) haladéktalanul értesíti telefonon vagy személyesen az informatikai biztonsági megbízottat;

b) az eseményt, bekövetkezte után lehetőleg azonnal, vagy rövid időn belül, írásban e-mail-en az informatika@rokus.hu címen is jelzi;

Veszélyhelyzet, vészhelyzet vagy rendkívüli helyzet esetén (pl.: betörés, tűz, villámcsapás stb.) az informatikai szerverterembe, valamint IT eszközöket és adathordozó eszközöket tároló helyiségekbe az őrzésvédelmet ellátó szervezetnél (porta, rendészet), vagy a titkárságon, vagy a szervezeti egység vezetőjénél elhelyezett zárt és lepecsételt borítékban vagy dobozban elhelyezett biztonsági kulccsal, illetve biztonsági kóddal lehet bejutni utólagos jelentési kötelezettség és jegyzőkönyvezés mellett.

A szervezeti egység vezetője köteles e-mail-en (informatika@rokus.hu), hálózati hiba esetén telefonon, vagy személyesen jelezni az informatikai biztonsági megbízottnak bármely, az informatikai biztonságot érintő gyanús eseményt (pl.: előző nap lekapcsolt, de reggel bekapcsolva talált gépet), vagy ezzel kapcsolatos gyanúját.

A Szent Rókus Kórház és Intézményei által felügyelt informatikai rendszerrel szemben végrehajtott internetes támadás esetén vagy a Szent Rókus Kórház és Intézményei által felügyelt internetes oldalakra vonatkozó sérülékenység felmerülése esetén az EIRF a helyzet értékelése után dönt az internetes oldal lezárásáról vagy az internetes támadással kapcsolatos intézkedésről. A döntést dokumentálni kell, és a döntésről értesíteni kell az érintett Szent Rókus Kórház és Intézményei szervezeti egységeket.

Az informatikai rendszer bármely felhasználói pontján jelentkező, a hálózattal, eszközzel, illetve adott alkalmazással kapcsolatban felmerülő rendellenes működés, jelenség, vírusjelzés, futási hiba esetén a felhasználó köteles a tapasztalt jelenséget, és ha van, a jelenséget kísérő hibaüzenetet regisztrálni és haladéktalanul bejelenteni az IFO informatikusának.

16.3 A rendszerek és a programok működési zavarainak kezelése

A Szent Rókus Kórház és Intézményei minden szerverén és munkaállomásán folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit.

Rendszer- vagy alkalmazáshiba esetén:

a) figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket;

b) amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás vagy vírustámadás okozta, az érintett munkaállomást, számítógépet le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is (pendrive, CD-ROM, mentési médiák), melyeket az EIRF-nek vizsgálat céljára át kell adni.

A Szent Rókus Kórház és Intézményei hozzáférési és egyéb adatvédelmi rendszereinek működés zavarát, a megtett intézkedéseket, haladéktalanul írásban jelenteni kell a szervezeti egység vezetőjének és az EIRF-nek.

A meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

16.4 A biztonsági események nyilvántartása és kivizsgálása

Az informatikai incidensekről az IFO megbízott munkatársa nyilvántartást vezet.

Az informatikai biztonsági megbízott a rendelkezésre álló nyilvántartásokat negyedévente elemzi, és továbbítja az IFO vezetőjének. AZ IFO osztályvezetője felhasználja azt a

a) a beszerzések tervezésénél;

b) a selejtezések tervezésénél;

c) a biztonsági konzekvenciák levonásakor;

d) a beszámoló készítésekor;

e) az IBSZ felülvizsgálatakor.

16.5 Az események tapasztalatainak elemzése és értékelése

Az eseményeket:

a) típus;

b) terjedelem;

c) az általuk okozott károk, helyreállítási költségek;

d) a feljogosítási és monitorozási rendszer működési zavara alapján értékelni kell.

Az elemzés alapján – szükség esetén – kezdeményezni kell a biztonsági irányelvek felülvizsgálatát, a szabályzatok korszerűsítését.

A biztonsággal összefüggő munkavállalói kötelességek megszegésének gyanúja esetén a felelősségi vizsgálat megindítása a munkáltatói jogkört gyakorló vezető feladata.

Az informatikai biztonsági megbízott a hiba elhárítása érdekében intézkedik, vagy a probléma elhárítását elvégzi, a hiba megszüntetéséről és a további teendőkről a felhasználót folyamatosan tájékoztatja. Helyettesítő eszköz biztosításával gondoskodik a felhasználó munkavégzési lehetőségéről.

16.6 Eljárás a biztonsági előírások megsértőivel szemben

Az informatikai rendszer rendellenes működése vagy a biztonságot veszélyeztető esemény elhárítása érdekében az informatikai eszközök használatát, a hálózat működését, az Internet és levelezés használatát az IFO vezetője részben vagy egészben korlátozhatja vagy leállíthatja a szervezeti egység vezetőjével, vagy a főigazgatóval történt tájékoztatást vagy egyeztetést követően.

A Szent Rókus Kórház és Intézményei szankciókat alkalmazhat az Internethasználat és elektronikus levelezés szabályainak megszegése esetén, ha a felhasználó az internetezés során a figyelmeztetését követően is szándékosan és rendszeresen:

a) megszegi az Internethasználat szabályait;

b) vagy olyan magatartást tanúsít, amely által súlyosan vét a munkahelyi etikai szabályok ellen;

c) vagy tiltott tartalmú kategóriába sorolt oldalakat látogat (kivéve egyedi írásos engedéllyel);

d) vagy tiltott tevékenységet folytat.

Az IBSZ szándékos, vagy az ismeret hiányából eredő megszegőjével szemben az IFO vezetője az érintett felhasználó felettesénél figyelmeztető felszólítást vagy fegyelmi eljárást kezdeményezhet.

Ha a Szent Rókus Kórház és Intézményei munkatársa, vagy szerződött partnere az informatikai biztonsági szabályok megszegésével olyan magatartást tanúsít, amely bűncselekmény gyanúját veti fel, az EIRF jelzése alapján a munkáltatói jogkör gyakorlója, vagy a főigazgató – a tudomására jutását követően haladéktalanul – feljelentést tesz ellene az illetékes nyomozóhatóságnál.

Ha a Szent Rókus Kórház és Intézményei munkatársa az informatikai biztonsági szabályokat vétkesen megszegve a Kórháznak kárt okoz, a Főigazgató fegyelmi, illetve kártérítési eljárást kezdeményezhet vele szemben.

17 Az informatikai biztonság dokumentálásának, ellenőrzésének szabályai

17.1 Az informatikai biztonság dokumentálása

Az informatikai biztonság szabályozó dokumentumai:

a) az IBSZ szabályai által előírt és naprakészen vezetett adatlapok, naplók és nyilvántartások;

b) az informatikai munka során készített feljegyzések, jelentések, jegyzőkönyvek;

c) a közbeszerzési dokumentumok.

Az informatikai biztonság ellenőrzése az alábbi eszközökkel biztosítható:

a) dokumentált eszközkezelés (üzembe helyezési, eszközátadási, eszközszállítási, leltározási és selejtezési események dokumentálása);
b) a jogosultságok és hozzáférések adatlapokkal történő dokumentálása;
c) ellenőrzött szoftverkezelés (jogtisztaság, tesztelt szoftverek, szoftvernyilvántartás vezetése, telepítési jogosultság szabályozása);
d) mentések és archívumok készítésére, valamint azok tárolására vonatkozó előírások és kapcsolódó nyilvántartások vezetése;
e) a munkahelyek, hálózatok, informatikai szervertermek kialakítására és üzemeltetésére vonatkozó előírások betartása, kapcsolódó események naplózása;
f) hibakezelési (e-HD) rendszer alkalmazása és ellenőrzése, elemzése;
g) az IT-biztonság többszintű ellenőrzése.

17.2 Az informatikai biztonság ellenőrzése

Az EIRF az éves ellenőrzések során szúrópróbaszerűen ellenőrzi az IT-biztonsági dokumentumokat és jelentés formájában tájékoztatja az elektronikus információs rendszerek védelméért felelős vezetőt.

Az informatikai biztonsági ellenőrzések területei:

a) környezeti veszélyek – pl. természeti károk, tűz stb.;
b) fizikai veszélyek – lopás, rongálás, betörés;
c) informatikai veszélyek – vírusok, számítógépes betörés stb.;
d) humán veszélyek – szabotázs, gondatlanság, tudatlanság, felelőtleng stb.;
e) szervezeti veszélyek – szervezeti problémák, irányítási gondok stb.

Az informatikai biztonság ellenőrzési rendszere a Kórházban:

a) alapszintű ellenőrzés: az informatikai biztonsági megbízott;
b) középszintű ellenőrzés:
   ba) a szervezeti egység vezetők személyes részvételével,
   bb) az IFO vezetője, az EIRF, vagy az őt képviselő informatikai biztonsági feladatok ellátásában közreműködő személyek ellenőrzései,
   bc) a Belső Ellenőrzési Osztály ellenőrzései;
c) felsőszintű ellenőrzés:
   ca.)Kórház management,
   cb.)szakmai irányításban közreműködő szervek, hatóságok ellenőrzései, felügyeleti kontrollja.

18 Felhasználók oktatása, képzése

18.1 Informatikai biztonsági oktatás és képzés

A Szent Rókus Kórház és Intézményei rendszereit csak olyan személyek használhatják, akik megfelelő informatikai ismeretekkel rendelkeznek. Az új belépő Kórházi munkatársat az illetékes szervezeti egység vezetője utasítja a szükséges informatikai ismeretek megismerésére. Ezt követően a kijelölt informatikus tájékoztatja a felhasználót az informatikai rendszer használatához szükséges alapvető ismeretekről és eljárásokról, a rá vonatkozó informatikai szabályzatok elérhetőségéről, és felkéri annak megismerésére és

betartására. A szükséges informatikai ismeretek és az informatikai szabályzatok megismerésének tényét a Szent Rókus Kórház és Intézményei munkatárs aláírásával igazolja. A megismerési dokumentumot az IFO őrzi elektronikus és papír alapon.

Jelen szabályzat hatálybalépését követően, és olyan változások esetén, amely jelentősen érinti az informatikai biztonságot, valamennyi Kórházi munkatárs köteles részt venni ún. informatikai biztonsági képzésen.

18.2 Az elektronikus információbiztonsághoz kapcsolódó képzési rend

Az elektronikus információs rendszer biztonságáért felelős személy (EIRF) az lehet, aki

a) felsőfokú végzettséggel rendelkezik és elvégezte a Nemzeti Közszolgálati Egyetem által szervezett 2 féléves elektronikus biztonsági vezető képzést és megkapta az oklevelét;

b) vagy felsőfokú végzettséggel és információbiztonság területén szerzett 5 év igazolt szakmai gyakorlattal rendelkezik (Ibtv. 13. § (10) és a 26/2013. (X.21.) KIM rendelet 7. §-a alapján);

c) vagy felsőfokú végzettséggel rendelkezik és van legalább egy, a 26/2013. (X.21.) KIM rendelet 7. § (2) bekezdésében előírt nemzetközi képesítése.

Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személyek kötelesek részt venni a szakmai képzésen, valamint az éves továbbképzéseken.

Minden felhasználó köteles az IFO által megszervezett biztonsággal kapcsolatos oktatási anyagot megismerni, majd a vizsga tesztfeladatokból sikeres vizsgát tenni. A vizsga-feladatsor az IBSZ anyagából és az intraneten közzétett információbiztonsági tudatosító anyagokból kerül összeállításra, amely felülvizsgálata és frissítése az IBSZ évenkénti egy alkalommal történő aktualizálásával egyszerre történik meg.

A szervezeti egységek vezetői kötelesek a jelen szabályzatot, és az esetlegesen kiadott biztonsági hírleveleket a munkatársaikhoz eljuttatni, a felhasználók kötelesek azt áttanulmányozni és a rendelkezések szerint végezni a tevékenységüket.

A belső informatikai biztonsági oktatások és továbbképzések tematikájának kidolgozásáért, a szükséges tájékoztató anyagok biztosításáért az EIRF felelős.

Minden felhasználó köteles a vonatkozó informatikai-szakmai szabályzatokat megismerni és betartani, illetve köteles ezek betartása során az informatikai rendszer használatát irányító személyekkel együttműködni.

19 Szabályzáshoz kapcsolódó /hivatkozott formanyomtatványok

Azonosító szám	Formanyomtatvány megnevezése	Megőrzési idő	Megőrzésért felel
MNY-521	SANITAS jogosultság igénylő és megszüntető	Iratkezelési szabályzat szerint	IFO vezető
MNY-522	CT-ECOSTAT jogosultság igénylő	Iratkezelési szabályzat szerint	IFO vezető
MNY-528	Jogosultság és bejelentkezés igénylő	Iratkezelési szabályzat szerint	IFO vezető
MNY-661	Eseménynapló	Iratkezelési szabályzat szerint	IFO vezető

20 Záró rendelkezések

Jelen szabályzat 2019.01.01. napján lép hatályba és ezzel együtt a 2015. október 21-étől hatályos Informatikai Biztonsági Szabályzat *(iktatószám: 615./2015.Kp.)* hatályát veszti.

Budapest, 2018. december 21.

Karis István
informatikus

1 Szabályzáshoz kapcsolódó mellékletek

1.1 Mentési terv

MENTÉSI TERV

Mentési eljárás

Biztonsági mentéseknek kell készülnie

az online elérhető (éles, tartalék, teszt) adatbázisokról és fájlrendszer könyvtárakról,

az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról,

szoftverek telepítőkészletéről.

Normál (FULL adatbázis): azaz minden mentési folyamattal mentésre kerül az összes állomány, függetlenül az előző mentés időpontjától és annak státuszától.

Inkrementális: azaz csak az előző mentés óta változott állományok kerülnek mentésre.

Teljes (FULL rendszer) : nemcsak az adatbázis, hanem a működtető szoftverkörnyezet is mentésre kerül.

A mentések akkor végezhetők el ugyanarra a szerverre, amennyiben az adattárolás tekintetében rendelkezik megfelelő biztonsági megoldásokkal :

RAID 1 – tükrözés,

RAID 5-6 – paritásos adattárolás, minimum 4 meghajtó esetében 1, illetve 2 meghajtó meghibásodását is elviseli a rendszer,

RAID 1+0;5+0 - a fenti módszerek kombinációja.

Az alábbi táblázat összefoglalóan tartalmazza az adatmentések gyakoriságát és az alkalmazott mentési típust:

Forrás	Naponta	Hetente	Havonta	Kitüntetett időpontban
Levelezőszerver, internetserver (külső szolgáltató)	INK	FULL adatbázis	FULL rendszer	FULL/adatbázis/vagy FULL rendszer
Medikai fileserverek, SanitasX, MeditCom	INK	FULL adatbázis	FULL rendszer	FULL/adatbázis/vagy FULL rendszer
Gazdasági (CT-ECOSTAT), Kórházi gyógyszertári (GYURIKA), közforgalmú gyógyszertár (QB-Pharma) és Munkaügyi fileserverek, iktató rendszer(DMSONE), humánpolitikai rendszerek (ORGWARE és NEXON IHr)	INK	FULL adatbázis	FULL rendszer	FULL/adatbázis/vagy FULL rendszer
Labor és mikrobiológiai serverek	INK	FULL adatbázis	FULL rendszer	FULL/adatbázis/vagy FULL rendszer

(ANDROMÉDA)				
Képalkotó diagnosztikai rendszerek (RTG, CT, UH, mammográfia, tüdőgondozó)	INK	Az IMPAX (AGFA) rendszerébe kerülnek át archiválásra a digitális felvételek.		

A mentéseket ütemezett feladatként, automatikusan kell elvégezni, minden hétköznap.

Az automatikus mentés elindítását munkaidőn túl kell ütemezni, hogy az alkalmazások ne legyenek használatban és ne legyenek nyitott állományok. Emiatt az automatikus mentést célszerű a napi munkavégzést követően elvégezni. A mentés eredményességét és futási idejét a mentés másnapján az informatikai biztonsági adminisztrátornak kell ellenőriznie. Minden rendellenességet jeleznie kell az informatikai biztonsági vezetőnek.

A mentés a szerverre való másolással történik.

Az adatbázis szerverekről célszerű külső eszközre mentést készíteni, melyeket backup számítógépre, vagy NAS tömbre kell másolni.

Archiválási eljárás

Az előző heti napi mentések közül a heti megadott időpontban a mentést archiválni kell. Az archiválás során a heti mentést kifejezetten erre a célra beszerzett külső merevlemezre NAS tömbre (HDD-re) kell átmásolni.

Az archivált állományokat tartalmazó elektronikus eszközöket, HDD-ket, lehetőség szerint egyedi azonosítóval kell ellátni, és tűzálló páncélszekrényben kell tárolni. Az eszközökről nyilvántartást kell vezetni.

Az archiválást az Informatikai biztonsági vezető, vagy az általa kijelölt informatikai munkatárs jogosult elvégezni.

Az archiválás után az utolsó hét előtti napi mentéseket törölni kell.

Az archivált állományokat tartalmazó eszközöket évente felül kell vizsgálni és szükség esetén selejtezni kell. A selejtezés során az egy éven túli archív állományokat tartalmazó HDD-ket alacsony szintű formázással formattálni kell. Az archív állományok selejtezéséről jegyzőkönyvet kell rögzíteni.

Visszatöltés mentési állományból

A visszatöltés igénylését az adott szervezeti egység vezetője írásban kezdeményezheti az Informatikai biztonsági vezetőnek címzett e-mail-ben. Az e-mail-nek tartalmaznia kell, hogy

melyik állomány visszatöltését igényli;

milyen dátumú állomány visszaállítását igényli;

milyen célból igényli az állomány visszaállítását

Az Informatikai biztonsági vezető megvizsgálja, hogy milyen okai vannak a visszatöltési igénynek. Ezek lehetnek:

adatvesztés/programhiba;

felhasználói hiba;

természeti katasztrófa.

Amennyiben adatvesztés vagy programhiba történt, az Informatikai biztonsági vezető gondoskodik a hiba elhárításáról. Katasztrófa esetén a Katasztrófatervnek megfelelően jár el.

Az Informatikai biztonsági vezetőnek meg kell vizsgálnia, hogy a visszatöltéssel nem sérülnek, illetve változnak meg az adott rendszer adatai. A visszatöltés jogosságát az Informatikai biztonsági vezető dönti el az adott rendszer adatgazdájával történt egyeztetés után. Amennyiben az ellenőrzés nem talált kizáró okot, és a visszatöltési kérelemben megadott dátumú mentés elérhető, az adott napi állományt vissza kell tölteni a kért helyre.

A sikeres visszatöltés tényét jegyzőkönyvben kell rögzíteni

Felelősség

Az adatmentések felelőssége az Informatikai biztonsági vezető hatáskörébe tartozik.

1.2 Informatikai Biztonsági Politika

Általános bevezető

Az Szent Rókus Kórház és Intézményeinél fellelhető információ, így különösen az informatikai rendszerekben megjelenő információ a Szent Rókus Kórház és Intézményeinek olyan adatvagyona, amelyet védeni kell a különböző fenyegetések ellen, a rendelkezésre állás, az integritás, a bizalmasság és a megbízhatóság biztosítása érdekében. A Szent Rókus Kórház és Intézményei főigazgatója az Informatikai Biztonsági Stratégiára figyelemmel határozza meg az informatikai biztonsági alapelveket és belső biztonsági alapkövetelményeket.
Informatikai biztonsági alapelvek

A Szent Rókus Kórház és Intézményei a kialakításra kerülő biztonsági eljárásokat, illetve az informatikai biztonsági szempontból kritikus munkafolyamatokat az alábbiakban megfogalmazott biztonsági alapelvek szerint építi fel:

Alapelvek:

Az emberi erőforrásokra/személyzetre vonatkozóan az Intézmény a rendelkezésre álló erőforrások figyelembe vételével

Gondoskodik arról, hogy az információ feldolgozó eszközöket használók tudatában legyenek az információ biztonságát fenyegető tényezőknek és a kialakított védelmi környezetnek.
Gondoskodik továbbá arról, hogy a biztonságot sértő események és zavarok okozta kár minimális legyen.
Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezéseinek megfelelően az elektronikus információs rendszerek biztonságáért felelős személynek (továbbiakban: EIRF) önálló informatikai biztonsági felelőst nevez ki. A Szent Rókus Kórház és Intézményei a közfeladat-ellátással összefüggő belső munkafolyamatainak megszervezése során a visszaélések megelőzése és detektálása érdekében a kritikus felelősségi köröket szétválasztja, valamint biztosítja az ellenőrzést, illetve a felülvizsgálatot.
Az elektronikus információs rendszer biztonsági felelős (EIRF) feladata az elvárt informatikai biztonsági szint eléréséhez és fenntartásához szükséges intézkedések, javaslatok, tervek, szakmai anyagok elkészítése. Az EIR ellenőrzi az informatikai biztonsági intézkedések megvalósulását, az 1. pontban meghatározott személyek és szervezetek tekintetében.

Fizikai és környezeti biztonságára vonatkozóan az Intézmény a reális működési környezetnek megfelelően

Megelőzi az információs vagyon elvesztését, sérülését vagy veszélyeztetését, valamint a munkatevékenységek megszakadását úgy, hogy az információs vagyont fizikailag védi a biztonsági fenyegetésektől és a környezeti veszélyektől.
Az információt és az információ feldolgozó eszközöket megvédi az illetéktelenek által nyilvánosságra hozataltól, lopástól, módosítástól, megsemmisítéstől.
A Szent Rókus Kórház és Intézményei informatikai biztonságának folyamatos felügyeletét, (monitoring) személyi és technológiai eszközökkel biztosítja.

A Szent Rókus Kórház és Intézményei az informatikai rendszereiben szükséges változtatásokat engedélyezett és dokumentált módon hajtja végre, így biztosítva a nyomon-követhetőséget, illetve a helyreállítás lehetőségét.
A Szent Rókus Kórház és Intézményei az elektronikus információ feldolgozó rendszereiben kezelt, illetve tárolt adatokról rendszeresen mentéseket készít az adatvesztés megelőzése, illetve következményeinek minimalizálása, valamint rendkívüli esemény bekövetkezése esetén a folyamatok minél rövidebb idejű kiesése érdekében.

Hozzáférés-ellenőrzésre vonatkozóan az Intézmény

Az információhoz és az üzleti folyamatokhoz való hozzáférést az üzleti és biztonsági követelmények alapján ellenőrzi oly módon, hogy a hozzáférés-ellenőrzés figyelembe veszi az információ terjesztés és a felhatalmazás szabályait.
A Szent Rókus Kórház és Intézményei informatikai rendszereihez való hozzáféréseinek szintjeit a szükséges és elégséges elv alapján határozza meg, azaz a felhasználó minden olyan jogosultsághoz, és információhoz kap hozzáférést, amely a munkájának elvégzéséhez szükséges, ugyanakkor csak olyan mértékben és időtartamban, amennyi a munkájához szükséges és elegendő.
A Szent Rókus Kórház és Intézményei a kezelésében lévő adatok tekintetében a biztonsági besorolásuknak megfelelő védelmet alakít ki és tart fenn.
Kiemelt figyelmet fordít különösen a Kórház által kezelt betegadatok különleges adatként történő kezelésére, az azokhoz kapcsolódó bizalmasság és sértetlenség elvére, az adatkezelés és feldolgozás teljes életciklusa alatt. A Szent Rókus Kórház és Intézményei tevékenységével és működésével összefüggésben kezelt személyes adatok védelmére kiemelt hangsúlyt helyez, biztosítja ezen adatok bizalmasságát, sértetlenségét és rendelkezésre állását.

Információbiztonsági incidensek kezelésére vonatkozóan az Intézmény

Az információbiztonsággal összefüggő incidenseket következetes és hatékony folyamat keretében kezeli, az egyértelmű felelősségek megjelölésével.

Információs rendszerek beszerzésére, fejlesztésére, és fenntartására vonatkozóan az Intézmény

Az új információs rendszerek beszerzését, vagy a meglévő információs rendszerek fejlesztését, fenntartását úgy végzi, hogy az információbiztonság valamennyi alapelve az információs rendszerekben megvalósuljon.
Figyelemmel kíséri a technikai fejlődésből adódó lehetséges újabb kockázatokat, és az azokat felszámoló védelmi megoldásokat.
A kialakított védelmi környezetet ezeknek megfelelően folyamatosan felügyeli, értékeli, és fejleszti.

Az információs vagyon osztályozására és ellenőrzésére vonatkozóan az Intézmény

Működése során az adatok kezelésénél és a rendszerek jogszabály szerinti biztonsági osztályba sorolásánál az alábbi szempontokat tartja szem előtt:
bizalmasság: az információ megvédése a jogosulatlan felhasználóktól.
sértetlenség: az információ pontosságának, hitelességének és

teljességének megtartása.
rendelkezésre állás: annak biztosítása, hogy az információ hozzáférhető legyen az arra jogosult felhasználók számára, amikor azt igénylik.

Fenntartja a szervezet vagyonának megfelelő védelmét az információs vagyon megfelelő felmérésével, védelmi igényeinek osztályokba sorolt meghatározásával.

Kommunikáció és az üzemeltetés irányítására vonatkozóan az Intézmény

Gondoskodik az információ feldolgozó eszközök pontos és biztonságos működéséről dokumentált üzemeltetési eljárások betartásával és betartatásával, a változások ellenőrzésével, a meghibásodások kockázatának minimalizálásával, rosszindulatú szoftverek elleni védekezéssel, az információfeldolgozás rendszergazda által történő állandó felügyeletével, valamint olyan hálózatok biztonsági menedzselésével, amelyek túlnyúlnak a szervezet határain.

Követelményeknek való megfelelőségére vonatkozóan az Intézmény

Folyamatos és határozott célja a törvényes, jogszabályoknak, szerződéses kötelezettségnek megfelelő információvédelem biztosítása.

A szervezet biztonságára vonatkozóan az Intézmény

Törekszik informatikai központilag menedzselhető keretrendszer felállítására, hogy a szervezeten belül ezzel kezdeményezze és ellenőrizze az információbiztonság megvalósítását.
Az informatikai biztonsági intézkedéseket és a biztonsági helyzet értékelését az informatikai biztonsági kockázatok rendszeres felülvizsgálatával, elemzésével támasztja alá.
Az informatikai biztonsági intézkedéseket az informatikai rendszer minden elemére és teljes életciklusára (fejlesztés, bevezetés, üzemeltetés, kivezetés) az életciklus szakasznak megfelelően érvényre juttatja.
Az informatikai biztonságot a szabályozás, az eszközök, az eljárások és az emberi tényezők oldaláról egyaránt kezeli, fizikai, logikai és adminisztratív intézkedések alkalmazásával.
Fenntartja az információ biztonságát akkor is, ha az információfeldolgozási felelősséget más szervezetnek alvállalkozásba adja át.

Üzletmenet folyamatosságának menedzselésére vonatkozóan az Intézmény

Folyamatos célja leküzdeni az üzleti tevékenységek megszakadásait és megvédeni a kritikus üzleti folyamatokat a nagyobb meghibásodások és katasztrófák hatásaitól.

A szabályozáshoz kapcsolódó további tevékenységek során az Intézmény

Az Informatikai Biztonsági Politikát 5 évente vagy az Szent Rókus Kórház és Intézményeinél bekövetkező jelentős informatikai változás alkalmával felülvizsgálja.
Jelen utasítás az aláírást követő napon hatályba lépteti azzal, hogy rendelkezéseit a folyamatban lévő ügyekben is alkalmazni kell.

Jelen utasítást körlevél, valamint ezzel egyidejűleg a Szent Rókus Kórház és Intézményei belső honlapján (Intranet) történő közzététel útján ismerteteti a Szent Rókus Kórház és Intézményei személyi állományával.

2 Függelék – Jogosultságok kiadása

1. Felhasználó azonosítás

1.1. Általános elvek a jogosultság kiosztásánál

A felhasználó azonosítás – más szóval autentikáció – minden informatikai rendszer biztonságának alapja. A felhasználók kellő megbízhatósággal történő azonosítása egy gép számára nem egyszerű feladat, a visszaélések ezért ezen a területen gyakoriak, így a megvalósításnál nagy figyelmet kell tanúsítani.

A felhasználó azonosításnak alapvetően három fajtáját ismerjük: tudás, birtok és biometria alapú eljárások. Mivel egyik módszer sem tökéletes, mindegyiknek vannak gyenge pontjai, így egy igazán biztonságos rendszer esetén a megbízható azonosításhoz legalább két módszer együttes és független alkalmazása szükséges.

A tudás alapú azonosítás esetén a felhasználót az alapján azonosítjuk, hogy mit tud, azt ellenőrizzük, hogy birtokában van-e a megfelelő (többnyire titkos) információnak. Ebbe a csoportba tartoznak a jelszavak és PIN kódok. Nagy előnyük, hogy olcsón és egyszerűen alkalmazhatóak, hátrányuk, hogy észrevétlenül eltulajdoníthatók (lehallgathatók, kitalálhatók), és az átlagos jelszavak nem biztosítanak igazán erős védelmet. Ezt le lehet tesztelni Pl.: http://www.passwordmeter.com, vagy a https://www.betterbuys.com/estimating-password-cracking-times/, oldalakon, ahol ki lehet próbálni, hogy adott jelszó mennyire jelent erős védelmet. (Pl. az egyszerű „zebra" jelszót, nagyon rövid idő alatt megtalálnak a jelszótörő programok az erre létrehozott szótárukban lineáris kereséssel, ellenben a „kiBhf4mr" jelmondat alapú betűszót csak kimerítő kereséssel lenne képes megtalálni kb. 10,3 év alatt, és ha ezt kiegészítem még egy betűvel, akkor már 1000 évnél is több időt venne igénybe a megfejtés.) Mivel a jelszavak jelentik a felhasználó azonosítás legelterjedtebb módját, így érdemes odafigyelni a megfelelő jelszó kiválasztására, és az Informatikai Biztonsági Szabályzatban segítséget kell nyújtani az erős jelszó választásához.

1.2. Logikai hozzáférésvédelem

A felhasználó azonosítást, autentikációt követi az autorizáció, a jogosultságok felhasználóhoz történő rendelése. A megfelelő védelem biztosítása érdekében az információkhoz való hozzáférést korlátozni kell, és ellenőrizni kell, hogy valóban csak az arra felhatalmazottak férhetnek hozzá az érzékeny adatokhoz. A jogosultság kezelésnek két elméleti megközelítése van.

A DAC (Discretionary Access Control), azaz önkényes (belátáson alapuló) hozzáférés védelmi mód esetén az objektum, dokumentum tulajdonosa határozza meg, hogy ki milyen módon férhet az adathoz. Ebben az esetben nagy a felhasználó felelőssége, és hozzá nem értése esetén ez komoly veszélyeket rejt magában.

A MAC (Mandatory Access Control), azaz előre meghatározott, kötelező hozzáférés védelem esetén a jogosultságok beállítását nem a tulajdonos végzi, hanem az központilag történik. Ezt az elvet alkalmazzák intézmények, vállalatok rendszerei esetén.

Ez a fajta jogosultság kezelés egyrészt megakadályozza a jogosulatlan hozzáférést, másrészt segít abban, hogy egy hozzá nem értő ne okozhasson károkat, hiszen egyszerűen nem fér hozzá az adatokhoz

1.3. Az egyes számítógépes rendszerekhez való jogosultságok kiosztásának elvei

Számítógépes rendszerhasználati jogok :

Minden munkavállaló felhasználói jogosultsággal rendelkezik az általa használt számítógépen, a rendszergazdák rendelkeznek, csak rendszergazdai jogokkal.

Informatikai alkalmazások jogai :

A felhasználók jogosultsági szintekbe sorolását az általuk betöltött pozíció alapján végezzük el. Ettől eltéréséket írásban kell igényelni a munkahelyi vezetőnek az Informatikai osztálytól. Az adott munkakör által meghatározott feladatok ellátáshoz szükséges rendszerek és a rendszereken belüli modulok, valamint a modulok egyes menüpontjainak a beállításával történik a megfelelő jogosultság létrehozása. Ez a beállítás meghatározza, hogy melyik felhasználó végezheti pl. az adott szoftver, adott moduljának a törzsadat kezelését, paraméterek beállítását, illetve, hogy milyen mélységben éri el az adott modul feldolgozásait.

2. Jelszókezelés

Az informatikai rendszer használatával való visszaélés kizárása érdekében minden felhasználónak egyedi felhasználó azonosítóval és az ahhoz tartozó jelszóval kell azonosítania magát. Felhasználó az Intézet dolgozója vagy hallgatója lehet, egyéni elbírálás alapján külső személy is kaphat felhasználó azonosítót.

Mivel sok és sokféle rendszerre lehet felhasználó azonosítót létrehozni, ezeket más-más szervezeti egységek felügyelik, ezért az alábbiakban csak általános vezérelvek lesznek felsorolva.

3.1. Intézetünk működő informatikai rendszerei :

A Szent Rókus Kórház és Intézményei informatikai rendszere egységes hálózatba szervezett, amelyen számos, az intézmény alaptevékenységét, valamint a gyógyítást segítő jelentős informatikai alkalmazás működik.

<u>Medikai alkalmazások</u> :

SanitasX járó- és fekvőbeteg ellátó rendszer,
Adroméda labordiagnosztikai rendszer,
AGFA PACS rendszer,
GYURIKA intézeti gyógyszertári rendszer
QB-Pharma közforgalmú patikai rendszer
TETFOG fogászati rendszer
Clinicom archív, medikai rendszer, nem aktív

Gazdasági és egyéb alkalmazások

ECOSTAT integrált gazdasági rendszer,
KIRA bérszámfejtési rendszer,
NEXON Ihr humánpolitikai rendszer,
DMSONE iktató rendszer.

A Szent Rókus Kórházban alkalmazott számítógépeken az informatikai rendszerbe belépni, a felhasználók számára név és jelszó megadásával lehet. minden egyes számítógépen. Az egyes rendszerekben és/vagy azok moduljaiban (pl.: SanitasX, CT-ECOSTAT, osztályos igénylés, munkalapos igénylés, gyógyszerigényles stb.) a munkahelyi vezető által meghatározott szintű és a munkakör ellátáshoz szükséges hozzáférés biztosított.

Asztali operációs rendszerek: /Windows NT, Windows XP, Windows 2000/Windows 7,8,10, LINUX (Debian, CentOS stb.).
Felhasználónként név és jogosultság definiálható, felhasználói tevékenységek szabályozhatók. Telepítésekor 1 db rendszergazdai fiók, 1 db korlátozott felhasználói fiók létrehozása. Domain használata esetében, minden felhasználó egyetlen azonosítót használ a domain bármelyik számítógépén.

Sanitas	IT-Rendszerház Kft.	integrált medikai rendszer	Teljes körű járó- és fekvőbeteg ellátás adminisztrációja, TAJ szám ellenőrzés, ambuláns lapok, kódolások, várólista, előjegyzés, finanszírozási jelentések készítése	A teljes adatvédelem biztosítva, felhasználónkénti jelszavas hozzáféréssel /napi mentése saját szerverén Havi mentés külön szerverre
Ecostat	Computrend Zrt.	Gazdasági és gazdálkodási rendszer	Főkönyvi könyvelés,pénzügyi nyilvántartások, számlakezelés és készítés, tárgyieszköz nyilvántartás, kötelezettség-vállalás, osztályos igénylés, gyógyszer ig.énylés, rendelés, szerződés nyilvántartás, leltározás,raktározás, anyagkezelés és anyagigénylés, cash flow, kontrolling	Szabályozható védelmi rendszer, Programmodulonként, menüpontonként. / a napi mentések a szerver saját lemezére történik, majd onnan a merevlemezre
Gyurika	SK Pont Kft.	Intézeti gyógyszertár készletgazdálkodása gyógyszer szakmai információinak kezelése	Gyógyszerbeszerzések, rendelési összeállítása, készletnyilvántartás, osztályos felhasználások kezelése, kimutatások készítése;	Felhasználónkénti jogosultsági rendszer. / a merevlemezre
QB - Pharma	QB-Pharma Zrt.	közforgalmú gyógyszer gazdálkodási rendszer	Készletgazdálkodás, elszámolások készítése, vevő szállítói számlák feldolgozása	Munkacsoportos, felhasználónkénti jogosultsági rendszer, /merevlemezre
Andromeda	Integramed Kft.	laboratóriumi informatikai rendszer	Labor és mikrobiológiai rendszer, adatbevitel vonalkódos és manuális azonosítóval, adatfeldolgozás, medikai rendszer számára kommunikáció, validálás, leletezés,	Felhasználónkénti, jogosultsági rendszer / a merevlemezre
AGFA PACS Rendszer	Silver Wood IT Kft.	komplex digitális képalkotó diagnosztikai rendszer	Digitális képalkotás foszforlemezes kiolvasóval, leletezés	Felhasználónkénti, munkaállomásonkénti jogosultsági rendszer/ Archiválás, mentés RAID tömbökre, külső lemeztömbre
NEXON Ihr	NEXON Kft.	Központosított munkaügyi rendszer	Munkaügyi nyilvántartások, adatszolgáltatások	Felhasználónkénti, jogosultsági rendszer, távoli eléréssel központi szerveren dolgoznak.
KIRA	MÁK	Központosított bérszámfejtési rendszer	Bérszámfejtés, ledolgozott munkaidő nyilvántartása, távollét, táppénz követése	Felhasználónkénti, jogosultsági rendszer, webes eléréssel központi szerveren dolgoznak.
Iktató rendszer	DMSOne	Iktató rendszer	Auditált iktatási rendszer	Felhasználónkénti, jogosultsági rendszer, webes eléréssel központi szerveren dolgoznak./NAS
TETFOG	NEAK	Fogászati jelentő rendszer	Fogászati ellátások dokumentálása, NEAK jelentése	Felhasználónkénti, jogosultsági rendszer / a merevlemezre

Informatikai jogosultsági szintek kategóriába sorolása:

- IFO osztályvezető,
- rendszergazda,
- beosztott informatikus,
- főigazgató,
- gazdasági igazgató,
- orvosigazgató,
- ápolási igazgató,
- MIR vezető,
- osztályvezető főorvos,
- kezelőorvos,
- adminisztratív személyzet,
- betegellátó (ápolási személyzet),
- gazdasági, műszaki, ellátó osztályok osztályvezetői,
- gazdasági, műszaki, ellátó osztályok beosztott dolgozói.

Hálózati belépési és munkavégzési jogosultságok szakma szerinti csoportosításban:

- Főigazgató:
  Belépési jogosultság olvasásra: minden rendszerbe.

- Orvos igazgató:
  Belépési jogosultság olvasásra: az egészségügyi rendszerbe.

- Ápolási igazgató:
  Belépési jogosultság olvasásra: az egészségügyi rendszerbe, jelenléti ív rendszerbe, gazdasági rendszer szerződés, munkalap, osztályos igénylés moduljaiba.

- Gazdasági igazgató:
  Belépési jogosultság olvasásra: a gazdasági rendszerbe, jelenléti ív rendszerbe.
- MIR vezető:

Belépési jogosultság olvasásra: az egészségügyi rendszerbe.

- MIR előadó:

A humánpolitika és a MIR vezető határozza meg a munkaköre ellátásához szükséges hozzáféréseket.

- IFO osztályvezető:

Belépési jogosultság írásra és olvasásra: a hálózat üzemben tartásához szükséges rendszer programokba, valamint az összes felhasználói alrendszerbe.
Jelszó kiadási jog: van
Új user felvételi jog: van

- Rendszergazdák:

Belépési jogosultság írásra és olvasásra: a hálózat üzemben tartásához szükséges rendszer programok, valamint az összes felhasználói alrendszer.
Jelszó kiadási jog: van
Új user felvételi jog: van

- Beosztott informatikus:

Belépési jogosultság írásra és olvasásra: a hálózat üzemen tartásához szükséges rendszer programok, valamint az összes felhasználói alrendszer.

Jelszó kiadási jog : nincs
Új user felvételi jog : nincs

- Pénzügyi osztályvezető:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer összes modulja.

- Pénzügyi osztály beosztott dolgozói:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer összes modulja.

- Műszaki osztályvezető:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés, készlet, tárgyieszköz nyilvántartás és munkalap rendszer moduljai.

- Raktáros:

A humánpolitika és a műszaki osztályvezető határozza meg a munkaköre ellátásához szükséges hozzáféréseket.

- Ellátási munkatársak:

A humánpolitika és a műszaki osztályvezető határozza meg a munkaköre ellátásához szükséges hozzáféréseket.

- Ellátási osztályvezető:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés, készlet, tárgyieszköz, munkalap rendszer moduljai.

Ellátási munkatársak:
A munkaköri leírásában lévő feladatok és az ellátási osztályvezető határozzák meg a munkaköre ellátásához szükséges hozzáféréseket.

- Humánpolitikai osztályvezető:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés és munkalap rendszer moduljai. A munkaügy nyilvántartási rendszer moduljai.

- Munkaügyi előadó:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés és munkalap rendszer moduljai. A munkaügy nyilvántartási rendszer moduljai.

- Belső ellenőr:

Belépési jogosultság olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés, munkalap rendszer moduljai.

- Kontroller:

Belépési jogosultság olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés, munkalap rendszer moduljai, az egészségügyi rendszerbe. Belépési jogosultság írásra: pénzügyi gazdasági alrendszer kontrolling modulja.

- Főgyógyszerész:

Belépési jogosultság írásra és olvasásra: pénzügyi gazdasági alrendszer megrendelés, szerződés és munkalap rendszer moduljai. A gyógyszer alrendszer moduljai.

- Gyógyszerés munkatársak:

A munkaköri leírásában lévő feladatok és a főgyógyszerész határozzák meg a munkaköre ellátásához szükséges hozzáféréseket.

- Osztályvezető főorvos:

Belépési jogosultság írásra és olvasásra: medikai rendszer, képalkotó programok.

- Osztályvezető főnővér:

Belépési jogosultság írásra és olvasásra: medikai rendszer. Szakmai anyag rendelés, gyógyszer rendelés, jelenléti ív program.

- Kezelőorvos:

Belépési jogosultság írásra és olvasásra: medikai rendszer, képalkotó programok.
Rezidens: Belépési jogosultság írásra és olvasásra: medikai rendszer.

- Osztályos adminisztrátor:

Belépési jogosultság írásra és olvasásra: medikai rendszer.

- Betegellátó (ápoló személyzet):

Belépési jogosultság írásra és olvasásra: medikai rendszer

Ellátási osztály jogosultsági mátrixa

Munkakör	Raktár	Intézeti elbírálás	Osztályos igénylés	Munkalapos igénylés	Tárgyi eszköz	Rendelés	Leltár
Raktáros	X	-	X	X	X	X	-
Anyaggazdálkodó	X	X	X	X	X	X	X
Adminisztrátor			X	X		X	
Leltározó	X		X		X		X
Leltárellenőr	X		X		X		X

Raktáros(ok) :

CT-EcoSTAT - Munkalap igénylés, Osztályos igénylés, Raktár, Rendelés, Tárgyi eszköz

Anyaggazdálkodó(k) - CT-EcoSTAT - Intézeti elbírálás, Leltár, Munkalap igénylés, Osztályos igénylés, Raktár, Rendelés, Tárgyi eszköz

Adminisztrátor - CT-EcoSTAT - Munkalap igénylés, Osztályos igénylés, Rendelés

Leltározó - CT-EcoSTAT – Leltár Osztályos igénylés, Raktár, Tárgyi eszköz

Leltárellenőr - CT-EcoSTAT – Leltár Osztályos igénylés, Raktár, Tárgyi eszköz

Pénzügyi osztály jogosultsági mátrixa

Munkakör	Pénzügyi modul	Főkönyvi Modul	Kötvállalási Modul	Cash flow Modul	Rendelés Modul
csop.vez	X	X	X	X	X

főkönyvi könyvelő	X	X	X	-	X
pénzügyi előadó I.	X	-	X	X	-
pénzügyi előadó II.	X	-	X	-	-
pénztáros	X		X		
analitikus könyvelő	X				X

Szent Rókus Kórház és Intézményei

1085 Budapest, Gyulai Pál u. 2.
Tel.: 235-6500. Fax: 266-4621.

MEGISMERÉSI NYILATKOZAT

A Szent Rókus Kórház és Intézményei **Informatikai Biztonsági Szabályzat** *(hatályos: 2019. január 01. napjától.)* tartalmát megismertem. Tudomásul veszem, hogy az abban foglaltakat maradéktalanul köteles vagyok betartani.

Név	Beosztás	Kelt	Aláírás
Dr. Göböl Zsolt	főigazgató	2018. 12. 21.	
Harsányi Imréné	gazdasági igazgató	2018. 12. 21.	
Kanis István	informatikus	2018.12.21	
BUGARSZKINÉ S. GIZELLA	ÁPOLÁSI IGAZGATÓ	2018.12.27	
BERECZ LÁSZLÓNÉ	MIR munkatárs	2018.12.27	
Bátori József	EFO ov.	2018.12.27	
BŐSZE-HUSZTI [illegible]	[illegible]	2018. 12. 27.	
LACZKOVSZKI EMESE	PÉNZÜGYI ÜGYINTÉZŐ	2018.12.29.	
HADARAS DÓRA	FINANSZ. ELŐADÓ	2018. 12. 27.	
Patkó Tünde	gazdálkodó	2018.12.29.	
Hnb Veronika	adminisztrátor	2018.12.27.	Hnb Veronika
Heller Sándorné	adminisztrátor	2018.12.27.	
DOBJÁN ZOLTÁN	műszaki és üzemeltet.	2018.12.21	
KARCZAI ÉVA	HUMPA ov.	2018.12.27	
Balázs Tóth Enikő	Hum. pol. ov.	2018.12.27.	
CZENCZER NORBERT	Minőségügyi munkatárs	2018. 12.27	
KARPATI ZOLTÁN	MIR UEZ	2018.12.27.	
KÁLLAI ANETT	IGAZGATÁSI KOORDINÁTOR	2018.12.27.	