Iktatószám: 587./2018.Kp.

Információ Biztonsági Politika

Hatályos: 2018. december 22-étől

Iktatószám: 587./2018.Kp.

Információ Biztonsági Politika

Hatályos: 2018. december 22-étől

Készítette:

Bátori József

informatikai és finanszírozási osztályvezető

Jóváhagyta

Dr. Göböl Zsolt

főigazgató

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

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.

Az intézmény főigazgatója és az intézmény felső vezetői az Információ Biztonsági Politika (továbbiakban: IBP) meghatározásával az információ biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségét kívánják deklarálnia jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására.

Jelen IBP alapul szolgál az Informatikai Biztonsági Stratégia és a belső szabályozási eszközök (Informatikai Biztonsági Szabályzat, és egyéb informatikai tárgyú eljárásrendek) kialakítására és megvalósítására.

Az IBP hatálya

Az IBP személyi hatálya alá tartozóknak ismerniük kell a politika célkitűzéseit, melynek érvényre juttatását biztosítani kell.

Az IBP személyi hatálya kiterjed a Szent Rókus Kórház és Intézményei:

- minden munkatársára;
- a tevékenység ellátását segítő külső partnerekre, beszállítókra;
- az informatikai fejlesztést végző szerződéses viszonyban tevékenykedőkre.

Az IBP tárgyi hatálya alá tartoznak: az adathordozók, alkalmazások, alapszoftverek, hardver elemek, környezeti infrastruktúra elemei és objektumai.

Az IBP területi hatálya alá tartoznak: a Szent Rókus Kórház és Intézményei székhelye, telephelyei, személyes (otthoni használatra) adott eszközökre.

Az információvédelem megvalósítása érdekében tervezni és biztosítani kell azokat az erőforrásokat, amelyek lehetővé teszik a kialakított irányvonal megteremtését és folyamatos fenntartását.

Az IBP elhelyezkedése, megfelelősége

Az IBP az intézményi szabályozási hierarchia legfelsőbb szintjén helyezkedik el, és ilyen módon hatással van a teljes szabályozási struktúrára.

Ismerete, és betartása minden az IBP hatálya alá tartozóra kötelező érvényű.

Az IBP-re épül az Információ Biztonsági Stratégia, és az Informatikai Biztonsági Szabályzat. A Szabályzat kiadása és közzététele az intézmény főigazgatójának, a folyamatos karbantartása és felülvizsgálata az Informatikai osztályvezetőnek a feladata. A felülvizsgálatot törvényi, környezeti, feladatváltozás esetén hatvan napon belül, egyéb esetben legalább kétévente el kell végezni.

Informatikai biztonságpolitikai alapelvek és célkitűzések

Informatikai biztonságpolitikai alapelvek

- *Teljes körűség:* a fizikai, logikai és adminisztratív védelem területén az informatikai rendszer összes rendszerelemére, teljes számítástechnikai infrastruktúrájára, összes alkalmazására, mind a központi, mind a végponti informatikai eszközökre kiterjed
- *Védelem zártsága:* akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések feltárásra került, mind az adminisztratív, a fizikai, mind a logikai védelem területén és azok szerves egységet alkotnak.
- *Védelem folytonossága:* a kialakított védelmi képességeket a rendszer teljes életciklusa alatt állandóan biztosítani és fejleszteni kell.
- *Kockázatarányosság:* védelem mértéke és költségei arányosak legyenek a felmért kockázatokkal. Cél: minimális védelmi költséggel, maximális védelmi képesség.

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

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

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 EIRF ellenőrzi az informatikai biztonsági intézkedések megvalósulását, az IBP hatálya alá tartozók vonatkozásában.

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:

Hitelesség: az intézmény vezetésének a célja a kezelésében lévő adatok hitelességének biztosítása, azaz a bekerülő adatok forrásának megállapíthatósága, adat valóságnak való megfelelősége, feldolgozás, felhasználás, tárolás során az adat minőségének megőrzése.

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 lép hatályba 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.

Budapest, 2018. december 21.

Bátori József
informatikai és finanszírozási
osztályvezető

Szent Rókus Kórház és Intézményei

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

TÜV CERT Rendszertanúsító ISO 9001:2015

MEGISMERÉSI NYILATKOZAT

A Szent Rókus Kórház és Intézményei **Információ Biztonsági Politika** *(hatályos: 2018. december 22. 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.	
BÁTORI JÓZSEF	INFORM. OV.	2018.12.21.	
Kovács István	informatikus	2018.12.21	
BUGARSZKINÉ S. GIZELLA	ÁPOLÁSI IGAZGATÓ	2018.12.22	
BERECZ LÁSZLÓNÉ	HIR munkatárs	2018.12.27	
Bódis [illegible]	ANALITIKA	2018.12.27.	
LACZKOVSZKY EMESE	PÉNZÜGYI ÜGYINTÉZŐ	2018.12.27.	
MADARAS Dóra	FINANSZ. ELŐADÓ	2018.12.27.	
Patkó Tünde	gazdálkodó	2018.12.27.	
Kaob Veronika	adminisztrátor	2018.12.27	
Keller Sándorné	adminisztrátor	2018.12.27.	
DERZSÁN ZOLTÁN	anyag és eszközgazd.	2018.12.27	
KARCZMÁRNÉ ÉVA	[illegible] OV.	2018.12.27	
Bakáné Török Enikő	[illegible]	2018.12.27.	
CZENCZER NORBERT	MINŐSÉGÜGYI MUNKATÁRS	2018.12.27	
KÁRPÁTI ZOLTÁN	MK. VEZ.	2018.12.27	
KÁLLAI ANETT	IGAZGATÁSI KOORDINÁTOR	2018.12.27.	