Iktatószám: 586./2018.Kp.

Információ Biztonsági Stratégia

Hatályos: 2019. január 1-jétől

Iktatószám: 586./2018.Kp.

Információ Biztonsági Stratégia

Hatályos: 2019. január 1-jétől

Készítette:

Bátori József
informatikai és finanszírozási osztályvezető

Jóváhagyta:

Dr. Göböl Zsolt
főigazgató

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

1. Bevezetés

A magyar Országgyűlés 2013. április 15-én fogadta el az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (továbbiakban: Ibtv.), melynek hatálya kiterjed a Szent Rókus Kórház és Intézményeire is.

Az Ibtv. 5. §-a és 6. §-a szerint az Ibtv. hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét. A szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást, a biztonsági események kezelését.

A nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága tárgyában a teendőket 2013. évi L. törvény valamint a biztonsági osztályba sorolási szempontjait a többször módosított 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 című rendelet együttesen határozza meg .

2. Az informatikai biztonsági stratégia célja

Az Informatika Biztonsági Stratégia (továbbiakban IBS) célja, a Szent Rókus Kórház és Intézményei Informatikai Biztonsági Politikájában (továbbiakban IBP) meghatározott alapelveknek megfelelően, az intézmény által kezelt információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, az IBS –ben meghatározott stratégiai folyamatok, tevékenységek alapján, valamint az elemzésekben feltárt biztonsági kockázatok csökkentése, az informatikai biztonság növelése.

Az intézmény megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti az informatikai biztonsági stratégiát, amely meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését.

Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

A Rókus Kórház információs rendszereinek biztonsági osztályai alapján felállított cselekvési tervek végrehajtása során kerülnek elérésre. A cselekvési tervekben rövid, közép, és hosszabb távon végrehajtandó feladatok kerülnek meghatározásra, amelyek alapján az intézmény meghatározza az informatikai biztonsági stratégia felülvizsgálatának és frissítésének gyakoriságát. Az informatikai biztonsági stratégiának illeszkednie kell a szervezet más stratégiáihoz (így különösen a költségvetési és humánerőforrás tervezéshez, fejlesztéshez), jövőképéhez.

3.Az IBS személyi, tárgyi, területi hatályai

Személyek tekintetében jelen Rendszerinformatikai Biztonsági Stratégia vonatkozik a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, a munkatörvénykönyvéről szóló 2012. évi I. törvény alapján alkalmazott személyekre, továbbá érvényesíteni kell azt a Szent Rókus Kórház és Intézményeivel szerződött, üzleti kapcsolatba került harmadik személyekkel és szervezetekkel létesített egyéb jogviszonyokban is.

Tárgyi hatálya vonatkozik az adathordozókra, informatikai alkalmazásokra, alap- és felhasználó szoftverekre, az informatikai hálózat aktív és passzív elemeire (környezeti infrastruktúrára) és az intézmény objektumaira.
Az IBS területi hatálya kiterjed a tárgyi hatálya lá tartozó informatikai erőforrások üzemelési és használati helyszíneire.

4. Az IBS helye az intézet szabályzati, szabályozási struktúrájában

Az IBS a szabályozási hierarchia (irányelvek - szabályozások - eljárásrendek - kézikönyvek) köztes szintjén helyezkedik el és ilyen módon hatással van a teljes szabályozási struktúrára. Ismerete és betartása minden munkatársra kötelező érvényű. A biztonsági stratégia a cselekvési tervekben rögzített részletezéssel meghatározza a biztonságpolitikai célok megvalósításának módszerét, eszközrendszerét, ütemezését. Az Információ Biztonsági Politika, majd az erre épülő Informatikai Biztonsági Stratégia elkészítése, karbantartatása és folyamatos felülvizsgáltatása az Informatikai biztonsági felelős feladata. A jelen IBS-ben megfogalmazottak megfelelnek a hazai jogszabályoknak.

5. Az informatikai biztonsági stratégia készítésénél alkalmazott alapelvek

Az IBS ben az alábbi stratégiai alapelvek és célkitűzések kerülnek megfogalmazásra, az Informatikai Biztonsági Stratégia azáltal hat vissza a Szent Rókus Kórház és Intézményei működésére, hogy az informatikai biztonság hiánya az intézmyény fő tevékenységének ellátása (betegellátás) terén súlyos veszteségeket okozhat, ezáltal az informatikai biztonsági kockázat egyértelműen működési kockázattá válik. Az informatikai biztonság teremti meg a szakmai folyamatok folytonosságát – kiemelten a betegellátási folyamatok teljes láncolatát – és a kiszolgáló informatikai rendszerek biztonságos működésének feltételeit.

Az alkalmazott alapelvek az intézmény IBP meghatározott alapevek.

5. 1. A védelem teljes körűségének alapelve:

A teljes körűségre vonatkozó alapelvet a fizikai, a logikai es az adminisztratív védelem területen a következő három dimenzióban kell érvényesíteni:

a) az összes rendszerelemre,
b) a rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén,
c) mind a központi, mind a végponti informatikai eszközökre és környezetükre.

5. 2. A védelem zártságának alapelve:

A zárt védelem akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések megvalósításra kerültek, és azok szerves egységet alkotnak.

5. 3. A védelem kockázat arányosságának alapelve:

A védelem mértéke és költségei a felmért kockázatokkal arányos legyen. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség. A védelem folytonosságának alapelve: az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

5. 4. A védelem folytonosságának alapelve:

Az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

6. Az IBS készítésekor feltárt, az intézmény működését tekintve releváns, elsődleges kockázati tényezők

Az intézmény vezetése célul tűzi ki, hogy a kockázatokkal arányos védelem biztosítása érdekében rendszeres kockázatelemzést végez.

A fenyegetések, gyenge pontok a nem elviselhető kockázati tényezők azonosítását elvégzi és kockázat kezelési tervet készít. A kialakítandó védelmi intézkedésekhez felelőst, határidőt rendel.

A kockázat alapú helyzetfelmérés eredményeinek összefoglalása:

A szerverszobába való belépés fizikailag nem szabályozott, nincs tűz,- vízjelző rendszer kialakítva, a szerverek szünetmentes áramellátása nem biztosított.
Az informatikai hálózat a szakrendelő területén elavult, a napi folyamatos adatforgalom kiszolgálása nem alkalmas (100 MB/s gerinchálózat), elavult, működési ciklusának végén járó, nem VLAN kompatibilis aktív eszközök működnek a hálózatban, ezért sem a működési biztonság nem kielégítő, sem a hálózatok szegmentálása nem megoldott.
Nincs központilag menedzselhető felhasználó kezelési rendszer. (Címtár, jogosultság kezelés. AD, LDAP, VPN)

Nincs központilag menedzselhető vírusvédelmi megoldás.

Nincs központilag menedzselhető adatmentési megoldás. (Pl. Veeam.)

A webszerver és a levelező szerver külső tárhelyen működik.

A kulcsfontosságú informatikai rendszerek támogatásához nem áll rendelkezésre elegendő backup szerver támogatás.

A PACS rendszer tárolási kapacitása bővítésre szorul, a PACS vezérlő szoftver verziócseréje elengedhetetlen. Az archiváláshoz központi, független tárolási megoldással nem rendelkezik a Rókus Kórház. Az informatikusok folyamatos szakmai képzése, illetve a felhasználók folyamatos oktatása nem kielégítő mértékű.

BCP (munkamenet folytonosság) biztosításához a normál munkaidőn túli informatikai ügyelet megszervezése, intézkedési terv kialakítása javasolt.

7. Megvalósítandó stratégiai feladatok

Elérni kívánt célok:

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben megfogalmazott feladatok az intézmény erőforrásainak figyelembevételével történő maradéktalan teljesítése a kapcsolódó végrehajtási rendeletekben meghatározott módon és határidőre, valamint az ennek megfelelő cselekvési terv végrehajtása.

Az ISO 27001:2014 ajánlásaihoz, mint információ biztonsági szabványhoz való közelítés az informatikai biztonság területén, a Szent Rókus Kórház és Intézményei jogszabály által meghatározott feladataival és Informatikai Biztonsági Politikájával összhangban.

Az IBS –nek olyan célokat – rövid, közép és hosszú távú -kell meghatároznia (összhangban az IBP –vel) amelyek az informatikai rendszereinkben tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állását kockázatokkal arányosan biztosítják a Szent Rókus Kórház és Intézményei számára. Az informatikai rendszer teljes területén megvalósított egyenszilárd, zárt, teljes körű, folyamatos és kockázatokkal arányos védelem biztosításával.

Az informatikai biztonság megvalósítása során, a piacon rendelkezésre álló technikai lehetőségek feltárása, — azok rövid és hosszú távon egyaránt — a kívánt biztonság elérése érdekében történő szem előtt tartása, a fejlesztésekben történő beépítése. Az informatikai rendszerek konszolidálása mellett a védelmi rendszerek teljes körű kiépítése, az adatok biztonsági besorolásának megfelelő szintre emelése minden alkalmazásban.

A Szent Rókus Kórház és Intézményei folyamatos, non-stop működésének biztosítása érdekében a Kórház kritikus területeire kiterjedő Üzletmenet-folytonossági és katasztrófa elhárítási terv elkészítése és alkalmazása, rendszeres tesztekkel, frissítésekkel és oktatásokkal.

7. 1. Rövid távú feladatok:

Szerver helyiség(ek) kialakítása, amely(ek) rendelkezik(nek) behatolás védelemmel és tűz, víz, áramellátás kimaradás esetére megfelelő védelmi megoldással.

A szerverközpontba való belépéseket regisztráló beléptető rendszer kiépítése, valamint benntartózkodási napló bevezetése. A web-és levelező szerver az intézet informatikai hálózatába való áttelepítése.

Olyan központi szerver – hardver és szoftver – beszerzése és alkalmazása, amely lehetővé teszi minden munkaállomáson egyedi, személyre szabott belépési rendszer kialakítását, ami központilag menedzselhető és minden munkaállomáson egyedi, személyre szabott belépési rendszer kialakítása, amely központilag menedzselhető. Ehhez a megfelelő hardver és szoftver eszközök beszerzése, szinten tartása, a működtetésre alkalmas humánerőforrás biztosítása. A PACS rendszervezérlő szoftverének frissítése.

Belső informatikai képzések szervezése.

7. 2. Közép távú feladatok:

Informatikai határvédelem területén a külső adatkapcsolatok és az internet irányában az intézmény kockázati szintjének megfelelő védelem (tűzfal, szabályrendszerek) magasabb biztonsági szinten való megoldása, amely összhangban van a NISZ által megkövetelt biztonsági előírásokkal.

Belső, információs rendszerek közötti kommunikáció magasabb biztonsági szintnek megfelelő módon történjen, szabványos megoldásokkal (pl.HL7, API) megvalósítása. Az egyes rendszerek szeparációjának hardveres, szoftveres és logikai megoldásokkal való támogatása.

Az intézmény kockázati tényezőinek figyelembe vételével megfelelő színvonalú, folyamatosan karbantartott, központilag menedzselhető biztonsági alkalmazások bevezetése, amelyek alkalmasak a rosszindulatú szoftverek elleni védelemre és lehetővé teszik a megfelelő logolással a számítógépes rendszerekben végzett tevékenységek lekövetését. A PACS rendszer archív kapacitásának jelentős bővítése, a háttértároló redundaciájának biztosítása.

7. 3. Hosszú távú feladatok:

Teljes mértékű virtualizáció az alkalmazás szerverek tekintetében. Folyamatosan rendelkezésre álló backup szerver beszerzése.

Olyan informatikai hálózat kialakítása és folyamatos karbantartása, amely megfelel az intézet információs igényeinek és az üzemeltetés biztonságának. A szükséges működési igényeket kielégítő optikai gerinchálózat kiépítése, korszerű aktív hálózati eszközök alkalmazása, a hálózati csomópontok megfelelő fizikai védelme és üzemeltetési folytonosság (pl. intézeti szintű szünetmentes áramellátás ezekhez az eszközökhöz) biztosítása, logikai hálózat-szeparáció különös tekintettel a különleges adatok forgalmának védelmére.

Nagybiztonságú, területileg elszeparált archiváló rendszer beszerzése. (Hardver és szoftver)

8. A stratégia megvalósításának feltételei, kritikus sikertényezők

A Rókus Kórház számára az információbiztonság sikeres megvalósítása során kritikus tényezők a következők:

a biztonsági szabályzó környezet pontos meghatározása, a vezetőség elkötelezettsége, a biztonsági követelmények, a kockázatbecslés és a kockázatkezelés megértése és helyes alkalmazása,

a biztonság hatékony menedzselése valamennyi vezető és alkalmazott felé, gondoskodás a kellő oktatásról és képzésről, átfogó, mindenre kiterjedő és kiegyensúlyozott mérési módszer alkalmazása

a biztonság menedzselés teljesítőképességének értékeléséhez és a helyesbítési javaslatok visszacsatolásához, a kockázatarányos anyagi források rendelkezésre állásának biztosítása.

9. Értelmező rendelkezések

Az IBS-ben használt fogalmak és definíciók értelmezése az Ibtv., és az információs önrendelkezési jogról és az információszabadságról szóló hatályos 2011. évi CXII. törvény fogalmaival és definícióival azonosak.

10. Szabályozáshoz kapcsolódó/hivatkozott külső és belső minőségirányítási dokumentumok

MSZ EN ISO/IEC 27001:2014

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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
- MF-01 Minőségirányítási dokumentumok készítése, módosítása és kezelése, külső dokumentumok figyelemmel kísérése
- Informatikai Biztonsági Politika
- Informatikai Biztonsági Szabályzat
- Intézményi kockázatelemzés (A FEUVÉ alapján.)
- Cselekvési terv (Az IBS –el összhangban készülő dokumentum)

11. Az IBS időbeli hatálya, felülvizsgálata

Az IBS 2019. január 1–jével lép hatályba, egyúttal minden korábbi – szabályzatokban és egyéb dokumentumokban kiadott-, az informatikai stratégiára vonatkozó szabályozás érvényét veszti.

Az IBS-t rendszeresen, de legalább kétévente felül kell vizsgálni. A felülvizsgálat az EIRF feladata.

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.

MEGISMERÉSI NYILATKOZAT

A Szent Rókus Kórház és Intézményei **Információ Biztonsági Stratégia** *(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.	
BÁTORI JÓZSEF	INFORM. OV.	2018. 12. 21.	
Kanis István	informatikus	2018. 12. 21	
BUGARSZKIVÉ S. GIZELLA	ÁPOLÁSI IGAZGATÓ	2018. 12. 27	
BERECZ LÁSZLÓNÉ	MIR munkatárs	2018. 12. 27	
[illegible]	[illegible]	2018. 12. 27.	
LACZKOVSZKI EMESE	PÉNZÜGYI ÜGYINTÉZŐ	2018. 12. 27.	
MADARAS DÓRA	FINANSZ. ELŐNDÍ	2018. 12. 27.	
Patkó Tünde	gazdálkodó	2018. 12. 27.	
Knob Veronika	adminisztrátor	2018. 12. 27	Knob Veronika
Keller Sándorné	adminisztrátor	2018. 12. 27	
DEDJÁN ZOLTÁN	ANYAG- ÉS ESZKÖZGAZD.	2018. 12. 27	
KARCSAI ÉVA	HUMÁNERŐ	2018. 12. 27.	
Bakáné Török Erzsi	humánerő. ü.	2018. 12. 27.	
CZEMPEL MÁRIA	MINŐSÉGÜGYI MUNKATÁRS	2018. 12. 27	
KARPÁTI ZOLTÁN	MIR. VEZ	2018. 12. 27.	
KÁLLAI ANETT	IGAZGATÁSI KOORDINÁTOR	2018. 12. 27	