Tolna Megyei Balassa János Kórház

INFORMÁCIÓBIZTONSÁGI POLITIKA

NYILVÁNOS

Szekszárd, 2023.03.14

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

Dokumentum leíró adatok	
Szervezet neve:	Tolna Megyei Balassa János Kórház
Dokumentum címe:	Információbiztonsági Politika
Adatosztályozás besorolás:	Nyilvános
Állomány neve:	Információbiztonsági Politika
Állapot:	Végleges
Verzió:	v1.0
A dokumentum leírása:	Információbiztonsági elkötelezettség kinyilvánítása az Intézmény vezetősége által

Dokumentum változásai

Verzió:	Dátum:	Készítette:	Jóváhagyta:	A változások leírása:
v1.0	2022.08.10	Závoda Ferenc	**Dr. Németh Csaba**	**Teljes tartalom előállítása**

2023 MÁRC. 14.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Bén Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

TARTALOMJEGYZÉK

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

1. ÁLTALÁNOS RENDELKEZÉSEK / PREAMBULUM

A biztonság erősítése és fenntartása érdekében az Intézmény kiadja az Információbiztonsági Politikáját, aminek betartása és ismerete minden érintett számára kötelező, és amelynek karbantartása, folyamatos felülvizsgálata, szükség esetén módosítása az informatikai biztonsági vezető (információbiztonsági felelős: IBF) feladata.

(2) Amennyiben az Intézmény informatikai rendszereiben, vagy a vonatkozó jogszabályokban jelentős változások következnek be, akkor az IBP-t felül kell vizsgálni és módosítani kell. A módosítások, felülvizsgálatok kezdeményezése és a módosítások elvégzése az IBF feladata. A módosításokat a Főigazgató hagyja jóvá.

(3) Az IBP-t az Intézmény minden munkatársával éves rendszeres Információbiztonsági oktatás keretében ismertetni kell, az Intézmény honlapján kell folyamatosan elérhetővé tenni.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

2. AZ INFORMÁCIÓBIZTONSÁGI POLITIKA

Az Intézmény vezetősége elkötelezett, hogy az Intézmény a működése és a nyújtott szolgáltatásai területén a partnerei, ügyfelei és saját adatai védelmét, és az érdekelt felek információbiztonsági elvárásainak való folyamatos megfelelést meghatározó elemként kezeli.

Az Intézmény által kezelt adatok és információk összessége kiemelt értéket képviselő vagyonelem, melyet védeni kell a különböző fenyegetések ellen, ezért az Intézmény törekszik, hogy e vagyonelemek tekintetében is időben állandóan megvalósuljon annak

- bizalmassága,
- sértetlensége,
- rendelkezésre állása.

Az Intézmény által nyújtott szolgáltatásokat magas színvonalon, modern és biztonságosan működő technológiával nyújtja, ahol felügyelt információbiztonsági folyamatokkal biztosítja a kezelt adatok, információk sértetlenségét, bizalmasságát és rendelkezésre állását.

Üzletmenet-folytonosságának biztosítása és alapfeladatainak zavartalan ellátása érdekében minden szükséges információ- és adatvédelmi intézkedést megtesz, adatkezelési, információvédelmi folyamatait az adatvédelmi az információbiztonsági elvárásoknak megfelelően alakítja ki.

Az Intézmény működése és az általa nyújtott szolgáltatások teljesítése során elkötelezett a vonatkozó törvényi, valamint az irányadó szabványokban foglalt előírásoknak való maximális megfelelés iránt, így különösen az 41_2015. (VII. 15.) BM rendeletben meghatározott iránymutatásoknak való megfelelés iránt, azáltal, hogy magára nézve a hivatkozott törvényeket és szabványokat kötelezően alkalmazandónak ismeri el.

Az Intézmény vezetése az Információ Biztonsági Politikában (IBP) megfogalmazott elvek és követelmények teljesítését várja el az összes munkatársától, beszállítóitól és minden egyéb érdekelt féltől.

2.1 HATÁLYA

Az IBP hatálya kiterjed az Intézmény valamennyi folyamatára és szervezeti egységére, így különösen az elektronikus információs rendszereire, mely magában foglalja

- az adathordozókat,
- alkalmazásokat,
- szoftvereket,
- hardver elemeket,
- a környezeti infrastruktúra elemeit és objektumait,
- a papír alapú dokumentumokat,

továbbá minden eljárására, melyek hatással lehetnek az Intézmény adatvagyonára.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

2.2 ALAPELVEI

Az információbiztonság folyamatos magas színvonalú fenntartása érdekében az alábbi alapelvek figyelembe vételével információbiztonsági irányítási rendszert (IBIR) vezet be és üzemeltet.

Az IBIR célja, hogy biztosítsa az Intézmény kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető, mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

Az Intézmény az információbiztonság területén az alábbi alapelveket érvényesíti:

1. **Hitelesség**: az adat legyen megbízható és egyértelműen azonosítható
2. **Bizalmasság:** az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
3. **Sértetlenség:** a tárolt adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapítható (letagadhatatlanság), illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
4. **Rendelkezésre állás:** az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.
5. **Információ teljessége**: Logikailag összefüggő adatokat a konzisztencia biztosításával egységesen kell kezelni.
6. **A védelem teljes körűsége:** az erre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:
    a) az összes rendszerelemre;
    b) a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén;
    c) a központi, illetve a végponti informatikai eszközökre és környezetükre.
7. **A védelem zártsága:** az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.
8. **A védelem kockázatarányossága:** a védelem mértéke és költségei a felmért kockázatokkal arányosak. Cél a szükséges és elégséges védelmi költséggel elért maximális védelmi képesség.
9. **A védelem folyamatossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és kockázati viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

Az informatikai rendszerek minden eszköz és humán tényezőjére felmérést kell végezni, hogy meg lehessen határozni a fenyegetettségek teljes körét és a hozzájuk kapcsolódó kockázatokat. A feltártakra szabályzatokban kell a tevékenységeket meghatározni.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

2.3 SZEREPE

Az információbiztonság az Intézmény életében az informatika nélkülözhetetlenné válásával egyre határozottabban jelenik meg. Ma már nem az a kérdés kell-e, hanem hogy miként lehet a leggazdaságosabban megvalósítani, a leghatékonyabban működtetni. Ez csak úgy lehetséges, ha az Információbiztonsági Politika:

a) Az első számú vezető elkötelezettségét élvezi és támogatja minden érintett vezető,
b) Az Intézmény terveivel összhangban, a többi biztonsági területtel (Vagyonbiztonság, Üzembiztonság) szinergiában valósítják meg és működtetik,
c) Kellőképpen kommunikált, oktatott,
d) Beépül a szervezet mindennapi életébe, a működési folyamatokba,
e) Része a szervezeti kultúrának, a dolgozók tudatos viselkedésének,
f) A biztonsági intézkedések, funkciók működése ellenőrzött és visszacsatolt, a hiányosságok szankcionáltak,
g) A szervezetben megfelelően képviselik az információbiztonság kérdését, van kijelölt szerepkör, szervezeti egység a menedzselésére.

2.4 CÉLJA

Az Intézmény tulajdonát képező, illetve jogszerűen kezelésében lévő infokommunikációs eszközökkel kezelt adatvagyon védelmét szolgáló irányelvek meghatározása.

Az adatok, valamint az adatok előállítására, kezelésére és tárolására szolgáló eszközök, rendszerek biztonságos működéséhez szükséges szabályzatok előállításához a megfelelő irányelveket, az a 2011. évi CXII. törvényben és a 2015. évi CXXIX. törvényben foglaltakat az Információbiztonság Tárcaközi Bizottsága (ITB) útmutatása alapján egységbe foglalja, annak érdekében, hogy a teljeskörű adatvédelem megvalósításra kerüljön.

Az Információbiztonsági politikában megfogalmazott irányelvek összhangban vannak az adatvédelemmel kapcsolatos törvények alapelveivel. Az informatikai rendszerekkel kapcsolatos alapelvek érintik:

- A személyes adathoz kapcsolódó irányelveket
- Egészségügyi adatokhoz kapcsolódó irányelveket
- Az intézményi adatokhoz kapcsolódó irányelveket
- Az adatfeldolgozás és tárolás munkafolyamatait
- Az adathozzáférés, jogosultság témakörét

Az Intézmény kezelésében (többek között személyes adatok, egészségügyi adatok) lévő adatvagyon a vonatkozó törvények alapján védettnek minősül, míg a tulajdonában lévőről saját hatáskörben a biztonsági besorolás kialakításával rendelkezik.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

Célja továbbá

a) biztosítani az adatok előállításának, megőrzésének, visszanyerésének folyamatosságát
b) ellenőrizhetővé tenni az adatok előállításának, megőrzésének, visszanyerésének folyamatát
c) biztosítani az adatokhoz az illetékességnek megfelelő hozzáférést
d) megelőzni, vagy lehetetlenné tenni az adatok tartalmának illetéktelenek által történő hozzáférését
e) az Intézmény informatikai rendszerei által kezelt információk hitelességének, sértetlenségének, rendelkezésre állásának, funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetése
f) az ügyfél, partneri, munkatársi, szerződéses, és egyéb üzleti információk bizalmasságának megőrzése, különös tekintettel az ügyfelek bizalmas adatainak biztonságos kezelésére.
g) az ügyfeleknek biztosított szolgáltatások jól definiált és magas minőségű információbiztonságának folyamatos biztosítása
h) az alkalmazott támogató informatikai, illetve információtechnológiai rendszerek információbiztonságának, illetve információtechnológiai biztonságának fenntartása, beleértve a jogszabályi követelmények előírásainak megfelelő biztosítását is
i) az ügyfeleknek nyújtott szolgáltatások üzemeltetése és fejlesztése érdekében alkalmazott támogató folyamatokra, illetve információtechnológiai rendszerekre vonatkozó mindenkori jogszabályi és egyéb szabályozási követelményeknek való megfelelőség folyamatos biztosítása

Az IBP célja, hogy irányelveket adjon a biztonságért felelős vezető részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntések meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

2.5 ESZKÖZEI

Az Intézmény a célok eléréséhez és fenntartásához alapvető eszköznek tekinti:

a) A szervezeti, üzleti és szolgáltatás működés folyamatos fejlesztését, a korszerű technológiák bevezetését, és alkalmazását;
b) A szolgáltatások folyamatos fejlesztését a szabályozási követelmények, az ügyfelek és a piac igényei alapján;
c) Folyamatos továbbképzéssel a legmagasabb szakmai kompetencia vagy színvonal elérését;
d) A feladatok és megbízások elvégzéséhez szükséges erőforrások felmérését és biztosítását;
e) Megfelelő és megbízható beszállítók, alvállalkozók kiválasztását és alkalmazását, amelyek elfogadják és teljesítik az információbiztonsági követelményeket;
f) A munkavégzés során – törekvéseink ellenére is - bekövetkező hibák kijavítását;
g) A tevékenységekre vonatkozó szakmai, adat- és információvédelmi, és egyéb jogszabályi követelmények – és ezek változásainak – folyamatosan figyelemmel kísérését, és azok maradéktalan betartását;
h) A védendő ügyfél és saját információs-, illetve adatvagyon fenyegetettségének és azok biztonsági kockázatainak rendszeres, legalább évente történő felülvizsgálatát és újraértékelését, majd ennek megfelelően az információvédelmi előírások és eljárások aktualizálását;
i) A szolgáltatások feltételeinek folyamatos biztosításához a következő – kiemelkedő kockázatúnak értékelt – incidens kategóriák elfogadhatatlannak tartását és legnagyobb veszélynek értékelését:
    - az ügyfelek adatainak beleegyezés nélküli nyilvánosságra kerülése;
    - adatvesztések, amelyek mentésekből nem állíthatók vissza;
    - hálózati betörés a támogató és szolgáltató informatikai, információtechnológiai rendszerekbe.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu

3. ZÁRADÉK

Jelen dokumentum aktualitásának megtartása érdekében rendszeres karbantartást igényel, 3 évente felül kell vizsgálni, kivéve az alábbi eseteket:

- Jogszabályi
- Funkcionális
- Biztonságtechnológiai
- Működési

változások állnak be. Ez esetben a fenti változások bármelyike, mint indukáló tényező szükségessé teszi ezen dokumentum, illetve a teljes szabályozási dokumentumrendszer felülvizsgálatát.

Tolna Megyei Balassa János Kórház, 7100, Szekszárd, Béri Balogh Ádám u. 5-7, Telefon: +36 74 501 500, email: info@tmkorhaz.hu