INFORMATIKAI BIZTONSÁGI SZABÁLYZAT (IBSZ)

1. módosítás

Jóváhagyom:

Dr. Trombitás Zoltán

főigazgató

Módosítások	
Dátuma	**Leírása**

1. AZ INFORMATIKAI BIZTONSÁGI SZABÁLYZAT CÉLJA

Az informatikai biztonsági szabályzat (a továbbiakban: IBSZ) alapvető célja, hogy a Pest Megyei Flór Ferenc Kórház (a továbbiakban: PMFFK vagy Kórház) informatikai rendszere alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és a jogosulatlan nyilvánosságra hozatalát.

AZ IBSZ TOVÁBBI CÉLJA SZABÁLYOZNI

a) az adatvédelem és adatbiztonság informatikai feltételeinek megteremtését.
b) az üzemeltetett informatikai rendszerek rendeltetésszerű használatát;
c) az üzembiztonságot szolgáló karbantartást és fenntartást;
d) az elektronikus adat- és titokvédelemre vonatkozó védelmi intézkedések szabályozása;
e) az adatok informatikai feldolgozását;
f) az adatok feldolgozása és kezelése során az illetéktelen felhasználásból származó hátrányos következmények minimális mértékre való csökkentését, megszüntetését;
g) az adatállományok tartalmi és formai épségének megőrzését;
h) az alkalmazott programok és adatállományok dokumentációinak nyilvántartását;
i) a munkaállomásokon lekérdezhető adatok körét;
j) az adatállományok biztonságos mentését;
k) az informatikai rendszerek zavartalan üzemeltetését;
l) a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását;

2. FONTOSABB FOGALMAK, MEGHATÁROZÁSOK

INFORMATIKAI BIZTONSÁGI FELELŐS (IBF)

Az elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján a PMFFK Főigazgatója által kijelölt azon személy, aki felelős az elektronikus információs rendszerek biztonságáért.

3. HIVATKOZÁSOK

KÜLSŐ DOKUMENTUMOK

- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK Irányelve a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.
- 331/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak az érintett hozzájárulá-sával tekinthet be a munkavállaló munkahelyi e-mail címén történő levelezésébe.
- 570/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak akkor ismerheti meg a munkavállaló internet-használatával kapcsolatos adatait, ha előzetesen felhívta a figyelmét az ezzel kapcsolatos korlátozásra és az ellenőrzés lehetőségére.
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 171/2010. (V.13.) Kormányrendelet a kormányzati informatika koordinációjáról és a kapcsoló-dó eljárási rendről
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 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 sérülékenységvizsgálat lefolytatásának szabályairól
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről; érintett szakaszok: 1.§ 1.,2.,2.§
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról; érintett szakaszok: 2.§ (1), 7.§ (1)-(6)
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről; érintett szakaszok: 2. §és 3. számú melléklet
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról; érintett szakaszok: 1.§,2.§ (1),5.§-12.§, 14.§-16.§
- 319/2010. (XII. 27.) Korm. rendelet az egészségbiztosítási szervekről; érintett szakaszok: 4.§ (1)
- 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról; érintett szakaszok: 1. számú melléklet
- 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

- 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 sérülékenységvizsgálat lefolytatásának szabályairól
- 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; érintett szakasz: 6. §
- 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; érintett szakaszok: 1-2. számú melléklet

BELSŐ DOKUMENTUMOK

- INT13 Adatvédelmi szabályzat
- INT14 Informatika
- INT 16 Leltározási szabályzat
- INT 35 Iratkezelési szabályzat
- INT-40 Vezetékes és Rádiótelefonok használatának szabályzata
- INT-45 A közérdekű adatok megismerésére irányuló kérelmek intézésének ls a kötelezően közzéteendő adatok nyilvánosságra hozatalának szabályzata

KAPCSOLÓDÓ SZABVÁNYOK ÉS AJÁNLÁSOK

- MSZ-ISO/IEC 27001:2006;
- MSZ ISO/IEC 17799:2006;
- Magyar Informatikai Biztonsági Ajánlások (Közigazgatási Informatikai Bizottság 25. számú Ajánlása);
- A MABISZ biztonságtechnikai ajánlása B/I. pontja szerinti teljes mechanikai, fizikai védelem;
- A MABISZ biztonságtechnikai ajánlása C/I/2. pontja szerinti részleges elektronikai jelzőrend-szer;
- A MABISZ biztonságtechnikai ajánlása C/II. pontja szerinti beléptető rendszer.

5. ADATOKKAL VÉGZETT TEVÉKENYSÉGEK

5.1. és 5.2 FELELŐSSÉGEK, HATÁSKÖRÖK AZ INFORMATIKAI BIZTONSÁG TERÜLETÉN

A PMFFK FŐIGAZGATÓJA

Az elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján gondoskodik az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,
b) biztosítja a Pest Megyei Flór Ferenc Kórházra irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,
c) kijelöli az elektronikus információs rendszer biztonságáért felelős személyt,
d) meghatározza a Kórház elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az informatikai biztonsági szabályzatot,

A PMFFK DIO OSZTÁLYVEZETŐJE

Felelős az informatikai rendszerek működésének és az elektronikus információs rendszerek biztonságának szervezeti szintű megvalósításáért, összehangolásáért, valamint folyamatos működtetéséért.
A DIO osztályvezetőjének jelen szabályozással kapcsolatban feladatai:

a) az Informatikai rendszer jelen Szabályzatnak megfelelő működtetése;
b) az általa érzékelt vagy tudomására jutott kockázatokról a Főigazgató tájékoztatása;
c) az informatikai üzemeltetést érintő minden dokumentum és utasítás elkészítése.

Az IBSZ szabályzatgazdája a DIO osztályvezetője, feladata legalább 2 évente, de szükség szerint soron kívül aktualizálni jelen szabályzatot.

A DIO osztályvezetője az informatikai rendszerek működésének és az elektronikus információs rendszerek biztonságának szervezeti szintű megvalósításával járó feladatait a Főigazgató közvetlen irányítása alatt látja el.
A DIO osztályvezetője jogosult:

d) az Informatikai rendszer teljes körű ellenőrzésére,
e) az informatikai üzemeltetést érintő szabályzatok, utasítások és dokumentumok előterjesztésére, véleményezésére.

A KÓRHÁZ MINDEN MUNKATÁRSA

A PMFFK minden felhasználója felelős a jelen Szabályzatban a szakterületére meghatározott informatikai biztonsági előírások betartásáért és betartatásáért.
A Kórház minden munkatársa köteles :

a) a Szabályzatban előírt ellenőrzések és az auditok sikeres megvalósítását elősegíteni és támogatni;
b) az Informatikai rendszer használata közben tapasztalt, a megszokottól eltérő működés esetén azt a közvetlen felettesének, illetve a DIO osztályvezetőnek vagy az IBF részére köteles jelezni.
c) hozzájárulni, hogy a DIO osztályvezetője előzetes bejelentés nélkül – a személyiségi jogok tiszteletben tartása mellett – ellenőrizheti az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok betartását.

FELHASZNÁLÓI HOZZÁFÉRÉSEK

d) Felhasználói nevek és jelszavak kiadása és karbantartása a DIO feladata, melyet a Munka- és Bérügyi osztály vagy az érintett gyógyító osztály vezetőjének papír alapú vagy elektronikus megkeresésére végez el.
e) Minden felhasználó kötelessége a saját jelszavának megvédése, azt harmadik fél részére nem adhatja át.