INFROMATIKAI BIZTONSÁGI POLITIKA

Az alábbi aláírások igazolják, hogy a jóváhagyók elolvasták, megértették és elfogadták a dokumentumot:

|  |  |  |  |
| --- | --- | --- | --- |
| **Név** | **Beosztás** | **Aláírás** | **Dátum** |
| **Jóváhagyó:** | ügyvezető |  |  |
| A szervezet vezetője igazolja, hogy a dokumentum megfelel a szervezet igényeinek. | | | |
| **Jóváhagyó:** | ügyvezető |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Jóváhagyás dátuma** | **Felülvizsgálati határidő** | **Adat kategória** | **Megőrzési idő** |
| 2018. május 25. | Szükség szerint | Belső - nem szabályozott | Az új verzió megjelenéséig, illetve módosítás időpontjáig |

**Tartalom**

[1 Bevezetés 3](#_Toc406486259)

[1.1 A dokumentum hatálya 3](#_Toc406486260)

[1.1.1 Szervezeti hatály 3](#_Toc406486261)

[1.1.2 Személyi hatály 3](#_Toc406486262)

[1.1.3 Tárgyi hatály 3](#_Toc406486263)

[1.2 Kötelező felülvizsgálat rendje 3](#_Toc406486264)

[1.3 Kapcsolódó dokumentumok 4](#_Toc406486265)

[2 Az informatikai biztonsági politika célja 5](#_Toc406486266)

[3 Alapelvek és védelmi célkitűzések 5](#_Toc406486267)

[4 Kapcsolódó elemek 5](#_Toc406486268)

[5 Kapcsolódó felelősségek 7](#_Toc406486269)

[6 Hivatkozások 7](#_Toc406486270)

[7 Dokumentum történet 7](#_Toc406486271)

# Bevezetés

Jelen dokumentum a **Firstmed-FMC Egészségügyi Szolgáltató Korlátolt Felelősségű Társaság** (székhelye: 1015 Budapest, Hattyú utca 14., cégjegyzékszáma: 01-09-958986, a továbbiakban TÁRSASÁG, vagy Társaság) informatikai biztonsági politikája.

## A dokumentum hatálya

### Szervezeti hatály

Az IBP hatálya kiterjed a TÁRSASÁG valamennyi szervezeti egységére, továbbá a TÁRSASÁGGAL szerződéses jogviszonyban álló valamennyi magánszemélyre, szervezetre, amelynek munkavállalói, vagy alvállalkozói az TÁRSASÁG által használt rendszerekhez, illetve az azokon tárolt adatokhoz hozzáféréssel rendelkeznek. A TÁRSASÁG kötelessége, hogy az érintetteknek legyen módjuk a rájuk vonatkozó elvárások és kötelezettségek megismerésére.

Az IBP-ben és a kapcsolódó szabályzatokban foglaltak érvényre juttatása érdekében a szabályozás előírásainak betartását minden olyan külső partnerrel kötött szerződésben és megállapodásban kötelezően elő kell írni, amelynek keretében a külső partner (beleértve annak munkavállalóit, alvállalkozóit, illetve az általa meghívott személyeket) a szabályozás hatálya alá eső helyen munkát végez, szállít vagy a TÁRSASÁG adataival, adatállományaival, rendszereivel, hálózatával, illetve hálózati eszközeivel bármiféle közvetlen, vagy közvetett kapcsolatban áll. Ezért a szerződés előkészítő szervezeti egység felelős.

### Személyi hatály

Az elfogadott IBP vonatkozik:

* a TÁRSASÁG valamennyi munkatársára,
* a TÁRSASÁGGAL szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási nyilatkozatok alapján.

A kapcsolódó szabályozások szellemének értelmében elsődlegesen a TÁRSASÁG feladata az irányítása alá tartozó szervezeti egységek esetében a szabályzatok betartásának ellenőrzése, szükség esetén szankciók alkalmazása.

### Tárgyi hatály

Az IBP tárgyi hatálya kiterjed a TÁRSASÁG által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a TÁRSASÁGNÁL keletkező, illetve felhasznált adatokat, információkat.

## Kötelező felülvizsgálat rendje

Az IBP annak elfogadásától a következő változat elfogadásáig marad érvényben.

Az IBP-ban előálló bármilyen változás verziószám változással jár, melyet a *Dokumentum történet* fejezetben fel kell vezetni, feltüntetve a verziószámot a kibocsátás napját és a változások rövid összefoglalását.

Az IBP felülvizsgálatára az alábbiak szerint kerül sor:

* 3 évente egy alkalommal, a belső felülvizsgálatok során,
* minden olyan esetben, amikor a leírtakhoz képest jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az Informatikai vezető feladatát jelenti.

## Kapcsolódó dokumentumok

Az IBP elkészítéséhez felhasznált dokumentumok

* Szervezeti és Működési Szabályzat [1]
* 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [2]
* Magyar Informatikai Biztonsági Ajánlások (MIBA) – Közigazgatási Informatikai bizottság [3]

# Az informatikai biztonsági politika célja

Az Informatikai Biztonsági Politika (a továbbiakban: IBP) a TÁRSASÁG akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések alkalmazására.

A dokumentum célja irányelveket adni a biztonságért felelős vezetők részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához. A szabályzatokban meghatározott védelmi intézkedéseknek minden esetben teljesíteniük kell az alábbi elvárásokat:

* teljes körűek, azaz a rendszer összes elemére kiterjednek,
* zártak, azaz minden fenyegetést figyelembe vesznek
* folytonosak, azaz a változó körülmények és követelmények mellett is megszakítás nélkül megvalósulnak.

# Alapelvek és védelmi célkitűzések

A TÁRSASÁG az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni:

* Hitelesség biztosítása, annak érdekében, hogy a TÁRSASÁG belső, vagy külső kapcsolataiban a partnerek kölcsönösen és kétségtelenül felismerjék egymást és ezt az állapotot a kapcsolat egész idejére változatlanul fenntartsák.
* Bizalmasság biztosítása a TÁRSASÁG által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a merevlemezen/szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók kezelése, valamint a kommunikáció során.
* Sértetlenség biztosítása a TÁRSASÁG teljes adatvagyonára vonatkozóan, az adatkezelés, adattárolás és a kommunikáció során.
* A TÁRSASÁGNÁL történő adatkezelések és feldolgozások során követelmény, hogy a pontos és helyes információkat dolgozzák fel, valamint az adatok sértetlenségének megőrzése a feldolgozás előtt, közben és után.
* Rendelkezésre állás fenntartása elsősorban a TÁRSASÁG adatvagyonára vonatkozóan, amelyet biztosítani kell mind a külső, mind pedig a belső adatkérések során.
* Működőképesség fenntartása a TÁRSASÁG informatikai rendszereire és rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a megfelelően képzett személyzetet és technikai feltételeket.

# Kapcsolódó elemek

A TÁRSASÁG vezetése elkötelezett, hogy olyan összetett védelmi környezetet alakítson ki, mely segítségével kellő biztonsággal, ugyanakkor rugalmassággal tudja kezelni a reá bízott és saját információkat. A védelmi környezet technológiai, szabályozási, ellenőrzési, dokumentálási funkciói révén megteremti a szervezet zárt, teljes körű, folyamatos és a kockázatokkal arányos információvédelmét, amely kiterjed:

**A szervezetbiztonságra:**

A TÁRSASÁG menedzselési keretrendszert állít fel, hogy a szervezeten belül ezzel kezdeményezze és ellenőrizze az információbiztonság megvalósítását.

Fenntartja az információ biztonságát akkor is, ha az információfeldolgozási felelősséget más szervezetnek alvállalkozásba adja át.

**Az információs vagyon osztályozása és ellenőrzésére:**

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

**Az emberi erőforrások (személyzet) biztonságára:**

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.

**Fizikai és környezeti biztonságára:**

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.

**Kommunikáció és az üzemeltetés irányítására:**

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.

**Hozzáférés-ellenőrzésre:**

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.

**Információs rendszerek beszerzésére, fejlesztésére, és fenntartására:**

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.

**Információbiztonsági incidensek kezelésére:**

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

**Az üzletmenet folyamatosságának menedzselésére:**

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

**Követelményeknek való megfelelőségre:**

A TÁRSASÁG határozott célja a törvényes, jogszabályoknak, szerződéses kötelezettségnek megfelelő információvédelem biztosítása.

# **Kapcsolódó felelősségek**

A TÁRSASÁG felügyeletében működő, és e szervezeteket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellégére és biztonságára vonatkozó törvényeknek megfelelően kell üzemeltetni. Ezek alapján a jogszerűen védett adatokra vonatkozóan olyan védelmi eljárásokat kell alkalmazni, amelyek ellenőrizhetővé teszik a folyamatokat, lehetővé teszik a szabálytalan cselekmények felderítését és a felelősség megállapítását.

Az informatikai rendszerekben adatot, információt és egyéb szellemi tulajdont a szervezet számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől. A védelemnek biztosítani kell az informatikai rendszer megbízható működését fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén.

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

# Hivatkozások

|  |  |  |
| --- | --- | --- |
| **No** | **Dokumentum azonosító** | **Dokumentum cím** |
| 1 | Társaság | Szervezeti és Működési Szabályzat |
| 2 | 2013. évi L. törvény | 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról |
| 3 | 25. számú ajánlás | Magyar Informatikai Biztonsági Ajánlások (MIBA) – Közigazgatási Informatikai bizottság |

# Dokumentum történet

|  |  |  |  |
| --- | --- | --- | --- |
| **Dátum** | **Verzió** | **Módosította** | **Módosítás oka** |
| 2018. május 25. | 1.0 | ügyvezető | Ez a dokumentum első változata |