FŐVÁROSI VÍZMŰVEK

A FŐVÁROSI VÍZMŰVEK ZRT. INFORMÁCIÓBIZTONSÁGI POLITIKÁJA

Célok

Az Információbiztonsági Politika fő célja annak garantálása, hogy az információs rendszerek és azok adatainak védelme a lehető legmagasabb szintű legyen a leginkább költséghatékony módon. A védelmi politikával az FV Rt. biztosítja, hogy az informatikai rendszerek és az adatok rendelkezésre állnak, bizalmasan kezeltek és sértetlenek.

A védelem azt jelenti, hogy lépéseket teszünk annak érdekében, hogy megakadályoz-zuk a behatolást, a rendszerek feltörését, a szándékos vagy véletlen hibázást. A védelem továbbá tervekkel rendelkezik a károk kijavítására is. A védelmi intézkedések kialakításakor figyelembe kell venni a védendő rendszerek sajátosságait, a vállalat anyagi lehetőségeit és az üzletmenet folytonosságának követelményeit.

Alkalmazási kör

A védelmi politika az FV Rt. összes információs rendszerére és teljes informatikai infrastruktúrájára érvényes.

Felelősségi kör

Az információs rendszereink védelméért minden munkavállaló felelős.

Ezen általános felelősségi körön belül az alábbi speciális felelősségi köröket lehet megkülönböztetni:

Informatikai szervezet

Az Informatikai, BPR és ingatlangazdálkodási igazgató felelős az információbiztonsági politika kialakításáért és a betartatásáért.
Figyelemmel kíséri, hogy a Felhasználók és az Informatikai szakemberek a politikát a gyakorlatban is megvalósítják-e. Ennek során garantálnia kell, hogy:

- A szükséges eljárások, irányelvek, útmutatók elkészüljenek.
- Az informatikai szakemberek által nyújtott védelemi szolgáltatások megfeleljenek a biztonsági politikának. Kötelező jelleggel!
- A védelem szintje meghatározásra kerüljön, a tervet folyamatosan karbantartsák, megvalósítását mérjék és ellenőrizzék.
- A vállalati alkalmazásokhoz és az adatokhoz, való hozzáféréshez titoktartási megállapodást kell aláírni.
- A hozzáférési jogok személyre szabottak, azokat harmadik félre átruházni tilos.
- A személyes jelszavakat titokban kell tartani. Ennek érdekében a felhasználóknak tilos a jelszavakat bármilyen formában közzétenni.
- A személyes jelszavakat legalább 2 havonta meg kell változtatni.
- A számítógépektől csak az éppen futó alkalmazások lezárása után szabad eltávozni.
- Szigorúan tilos hamis azonosítót vagy más személy hozzáférési jogát használni, megpróbálni megkerülni a jelszóhasználatot vagy betörni az információs rendszerbe.
- A vállalattól történő kilépés esetén minden a kilépő által használt jelszót érvényteleníteni kell, valamint kulcsot, anyagot és belépőkártyát vissza kell szolgáltatni.
- Szigorúan tilos kárt okozó vagy közfelháborodást, előidéző szoftvert felhasználni vagy terjeszteni.
- A védendő rendszerek leltára elkészüljön.
- A belső és külső felhasználók listája jogosultságukkal együtt kialakításra kerüljön, és ezt a listát folyamatosan frissítsék is.
- Minden egyes munkavállaló felelőssége egyénileg legyen meghatározva.
- Rendszeresen legyenek az informatikai védelemmel kapcsolatos tájékoztatók, előadások.

A fenti feladatokat az Informatikai Igazgató megbízásából az Adatbiztonsági Felügyelő valósítja meg.

Budapest, 2010. július 1.

Keszler Ferenc
vezérigazgató

Felhasználók

A felhasználóknak be kell tartaniuk a védelmi előírásokat és a mindenkire nézve kötelező irányelveket. A következő előírásokra külön hangsúlyt kell helyezni:

- A munkahelyen a felhasználók rendelkezésére bocsátott informatikai eszközöket és adatokat kizárólag munkával kapcsolatos célokra szabad felhasználni.
- Csak a vállalat által megvásárolt és telepített szoftvert szabad használni.

Informatikai szakemberek

Az informatikai szakembereknek szigorúan tartaniuk kell magukat a fent említett biztonsági folyamatok és vezetési irányelvek betartásához. Továbbá, a rendszerhez való szélesebb körű hozzáféréssel rendelkező informatikai szakembereknek formálisan is vállalniuk kell, hogy a rendszereket az etikai kódexben foglaltaknak megfelelően szigorúan csak munkahelyi célokra használhatják.
Az információs rendszerek tulajdonosainak kérésére megfelelő védelmi szolgáltatásokat kell nyújtaniuk.
Az FV Rt. a rendszerek tulajdonosaival együtt felelősnek tartja őket a rájuk bízott rendszerekért. Az informatikai biztonság vonatkozásában különösen fontos feladatuk megbizonyosodni arról, hogy a rendszerek fizikai és szoftveres védelme a megkívánt szintnek megfelelő-e.

A fizikai védelemmel kapcsolatos követelmények:

- Korlátozott belépési jogosultság az informatikai eszközök és adattárolók elhelyezésére szolgáló épületekbe és helyiségekbe (korlátozott számú belépési pont, zárt ajtók, kulccsal vagy kártyával történő belépés).
- Adatok tárolására, archiválására szolgáló helyiségekben, valamint fontos berendezéseket tároló helyiségekben tűzeset megelőzésére, észlelésére és elhárítására szolgáló lépések megtétele.
- Lopás megelőzésére szolgáló lépések megtétele: a berendezések tárolására szolgáló helyiségek zárva tartása, fontos berendezések és adattároló eszközök elzárása munkaidőn kívüli időszakokban, könnyen elmozdítható berendezések biztonságos rögzítése.

A szoftvervédelemmel kapcsolatos követelmények:

- Az alkalmazások és adatok hatékony védelme.
- Mentések készítése annak érdekében, hogy a munka folyamatossága probléma esetén is fenntartható legyen.
- A mentések megfelelő védelme és külön helyiségben történő tárolása.
- Amennyiben egy adott alkalmazás működésképtelensége jelentősen befolyásolja a munkavégzést, helyettesítő megoldásnak kell rendelkezésre állnia.

Audit

Rendszeres ellenőrzésekkel meg kell bizonyosodni arról, hogy a politikában kitűzött célok megvalósulnak és a vonatkozó utasításokat és eljárásokat az érintettek betartják. Az ellenőrzések során talált hiányosságok szerepelnek a jegyzőkönyvekben.

A politikában megfogalmazott irányelvek megszegése

Mindenki, aki a biztonsági politika alkalmazásának megszegését észleli, köteles azt közvetlen vezetőjének azonnal jelenteni. A közvetlen vezető ezt követően értesíti a rendszer tulajdonosát és a védelemért felelős vezetőt.

A biztonsági politika irányelveinek megszegése a munkahelyi szabályokba foglalt szankciókat vonhatja maga után.

FŐVÁROSI VÍZMŰVEK