1. melléklet

A Pillér Informatikai Nonprofit Kft. Informatikai Biztonsági Politikája

1. A Pillér Nkft. teljes mértékben elkötelezett a társaság információbiztonsága iránt, az elektronikus információs rendszerei által kezelt információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására érdekében.

2. Figyelemmel a fentiekre a Pillér Nkft. vezetősége elkötelezett az informatikai biztonság megvalósításához szükséges erőforrások biztosítása iránt. Ennek érdekében beépíti az információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrásokat az éves üzleti tervben.

3. A megfelelő szintű információbiztonság, a kockázatarányos védelem kialakítása a vezetők feladata és kötelezettsége. A védelem mértéke és annak költségei arányosak legyenek a felmért kockázatokkal. A védelem kialakításánál az észszerűen elérhető legkisebb kockázatra kell törekedni.

4. A Pillér Nkft. elektronikus információs rendszeri által gyűjtött, tárolt, feldolgozott, továbbított és megjelenített adatok védelméről gondoskodni kell bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából. Úgy kell megvalósítani, hogy az elektronikus információs rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint megvalósuljon a zárt szabályozási ciklus.

   4.1. a védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés ellen a megelőző védelmi intézkedések, a kockázatokkal arányos módon megvalósulnak, mind az adminisztratív, fizikai, logikai védelem területén és ezek szerves egységet alkotnak,

   4.2. a védelem akkor kockázatarányos, ha az elektronikus információs rendszerben kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak, célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség,

   4.3. a védelem folytonossága úgy biztosítható, hogy az elektronikus információs rendszer fejlesztése és megvalósítása során kialakított védelmi képességek a rendszerből történő kivonásig (a rendszer teljes életciklusa alatt) folytonosan biztosított a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel,

   4.4. a zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelem biztosítja a szabályozás, az érvényesítés, az ellenőrzés és a védelmi intézkedések, valamint szankciók zárt folyamatát.

5. Az informatikai biztonság területén létrehozott szabályozó rendszer a Pillér Nkft. munkavállalóin kívül a társasággal kapcsolatba kerülő más személyeknek/gazdálkodó szervezeteknek is bemutatja azokat az alapelveket és normákat, amelyeket a Pillér Nkft. -e körben követ, és elvár mind a munkavállalóitól, mind a vele kapcsolatba kerülő más személyektől/szervezetektől.

6. Az informatikai biztonság megteremtése elsődlegesen a Pillér Nkft. vezetőinek a feladata, mindazonáltal az informatikai rendszerek, alkalmazások és eszközök biztonságáért és hatékony felhasználásáért valamennyi munkavállaló felelős.

7. A Pillér Nkft. elkötelezett olyan védelmi eljárások és előírások alkalmazása iránt, amelyek garantálják a Pillér Nkft. hatékony működését katasztrófahelyzet esetén is.

8. Az informatikai rendszereket, alkalmazásokat és eszközöket a bennük kezelt adatok jellemzői (érzékenység, bizalmasság stb.) alapján, a hatályos jogszabályok figyelembevétele mellett biztonsági osztályba kell sorolni.

9. A Pillér Nkft. adatkezelése, informatikai rendszereinek, alkalmazásainak és eszközeinek a használata minden esetben jogszabályokon alapul és a jogszabályok adta keretek között valósul meg. Ezt biztosítják a Pillér Nkft. rendelkezéseiben rögzített előírások is.
10. A Pillér Nkft. által üzemeltetett és használt informatikai rendszerek, alkalmazások és eszközök biztonságát a kockázatarányosság, a szükséges és elégséges védelem elve alapján kell garantálni.
11. A Pillér Nkft. által az informatikai rendszerekben és alkalmazásokban kezelt adatokra vonatkozóan olyan védelmi megoldásokat és eljárásokat kell alkalmazni, amelyek lehetővé teszik a hozzáférések akár utólagos ellenőrzését és a jogosulatlan hozzáférések felderítését, valamint a felelősök személyének megállapítását.