



# PANNON GUARD BIZTONSÁGI SZOLGÁLTATÓ ZRT.

4026 Debrecen Hatvan utca 39. 2/3.

## Biztonságpolitika

A Pannon Guard Zrt. vezetése és minden alkalmazottja tudatában van annak, hogy az üzletvitel során tudomására jutott információk pontossága, teljessége, bizalmasságának és sértetlenségének megőrzése, amellyel vevői és saját érdekeit szolgálja, szerződéses kötelezettségeinek eleget téve – alapvető elsődleges szerepet játszik a Zrt. életében, a piacvezetői helyzet megszerzésében, megtartásában.

Emiatt a Zrt. minden dolgozójának és alvállalkozójának kötelessége és érdeke, hogy tevékenysége, valamint az alkalmazott hardver és szoftver eszközök mindenkor megfeleljenek a vonatkozó érvényes jogszabályoknak. A Zrt. vezetősége elkötelezte magát arra, hogy értékes eszközeinek – beleértve munkatársait és az információhordozó és feldolgozó eszközöket és a vevőik által rájuk bízott értékeinek, információinak – a szükséges és elégséges védelmet biztosítja.

Mindezek érdekében a Pannon Guard Zrt. vezetése kialakítja és fenntartja az Információbiztonság Irányítási Rendszerét. Vállalja, hogy Információbiztonság Irányítási Rendszerét rendszeresen átvizsgálja, teszteli, a belső és külső igényeknek megfelelően folyamatosan fejleszti.

A kockázatok minimalizálása érdekében folyamatosan ellenőrzi, szükség szerint módosítja a kockázat értékelés szempontjait, és a kockázat menedzselési, intézkedési tervét.

A Zrt. vezetése biztosítja, hogy

- minden dolgozó megismerje az Pannon Guard Zrt. Információbiztonság Irányítási Rendszerének általános szabályait, továbbá a munkakörre érvényes jogosultsági és felelősségi szabályokat,
- a szervezet Információbiztonság Irányítási Rendszere és a Zrt. munkatársainak ilyen irányú oktatása révén, a jogosultsági és felelősségi szabályoknak a Zrt. minden dolgozója és alvállalkozója eleget tudjon tenni,
- az Információbiztonság Irányítási Rendszer változtatása esetén, minden dolgozója megfelelő oktatásban részesüljön annak érdekében, hogy az Információbiztonság Irányítási Rendszer az első bekezdésben foglalt cél elérését mindenkor lehetővé tegye,
- a megfelelő védelmi rendszer kiépítésével a számítógépes vírusok és kártevők kiszűrhetőek legyenek és a számítógépes rendszer működését, ne veszélyeztessék, a Zrt. eszközeit rossz célra ne használhassák, azzal ne élhessenek vissza,
- csak jogtiszt szoftverek kerüljenek használatra,
- a biztonsági incidenseket a dolgozók jelentsék,
- az Információbiztonság Irányítási Rendszer működtetése révén az üzletmenet folyamatosága mindenkor biztosítva legyen.