Információbiztonsági Politika

A Yigsoft Kft. célja, hogy szolgáltatásait mind a szoftverfejlesztés, mind a mindennapi működés során a legmodernebb technológiák felhasználásával, magas színvonalon és a biztonságos működést támogató megoldásokkal biztosítsa, az ehhez szükséges információbiztonsági folyamatok és erőforrások rendelkezésre álljanak. A Társaság működése során kiemelt fontosságúnak tekinti az IT rendszerek és a rendszerekben kezelt adatok védelmét, amelyet a lefektetett információbiztonsági alapelvek szerint működő környezetben biztosít.

A vezetés és a munkatársak elkötelezettek az információbiztonsági követelményeknek való megfelelés iránt, a Társaság ennek megfelelően tervezi meg, alakítja ki, működteti és fejleszti az Információbiztonsági Irányítási Rendszerét (IBIR) annak érdekében, hogy a kezelésében lévő információs vagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az IT rendszerek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető mindenkori fenyegetések kockázataival arányos, zárt, teljeskörű és folytonos, a rendszerek teljes életciklusára kiterjedő védelmet biztosítsa logikai, fizikai és adminisztratív védelmi intézkedések alkalmazásával.

Az elszámoltathatóság, a bizalmasság és a sértetlenség elveiből fakadóan a Yigsoft Kft. meg kíván felelni a jelen kor követelményeinek eleget tévő, információbiztonságra vonatkozó elvárásoknak, ezért a hatáskörében működő IT rendszerek tervezésére, bevezetésére, üzemeltetésére és ellenőrzésére vonatkozó feladatokat úgy végzi vagy végezteti, hogy a rendszerek védelme a jogszabályi előírásoknak, az Ügyfelek igényeinek, az üzletmenet folytonossági elvárásoknak megfeleljen, valamint a védelem költsége a releváns kockázatokkal arányos legyen.

A kitűzött cél elérése érdekében a Társaság:

- megtervezi az Információbiztonsági Irányítási Rendszerét, gondoskodik az esetleges információbiztonsági incidensek hatékony kezeléséről és arról, hogy a zavarok okozta kár minimális legyen; a tanulságok alapján folyamatosan fejleszti a folyamatait,
- oktatásokkal és figyelemfelhívó kampányokkal növeli a felhasználók biztonságtudatossági szintjét,
- megelőző tevékenységet folytat, megelőző intézkedéseket alkalmaz az információs vagyon bizalmassági, sértetlenségi és rendelkezésre állási szintjének fenntartása érdekében, az üzleti tevékenységek folytonosságának megszakadását eredményező események hatásának csökkentése céljából,
- rendszeres felülvizsgálatokkal megbizonyosodik a kialakított folyamatok működési hatékonyságáról, valamint a kitűzött célok megvalósulásáról.

Budapest, 2023.03.01.

Hambalkó Bence

Ügyvezető