

INFORMÁCIÓBIZTONSÁGI POLITIKA

MSZ ISO/IEC 27001:2023 alapján

A 4iG Informatikai Zrt. vezetősége elkötelezett, hogy a szolgáltatásokat a legmodernebb technológiák felhasználásával, magas színvonalon, biztonságosan működő termékekkel és folyamatosan lássa el, az ehhez szükséges információbiztonsági folyamatokat és azokhoz szükséges erőforrásokat biztosítsa. A Társaság által kezelt adatok és információk összessége kiemelt értéket képviselő vagyonelem, melyet védeni kell a különböző fenyegetések ellen, ezért a Társaság törekszik, hogy e vagyonelem tekintetében is időben állandóan megvalósuljon annak bizalmassága, sértetlensége, rendelkezésre állása. Az üzletmenet folytonosság biztosítása érdekében a Társaság az összes szükséges információvédelmi intézkedést megteszi, minden adatkezelési folyamatát az adatvédelmi és az információbiztonsági elvárásoknak megfelelően alakítja ki.

Jelen Információbiztonsági Politika (a továbbiakban IBP vagy Információbiztonsági Politika) célja magas szinten támogatni (és szabályozni) a Társaság alapfeladatainak zavartalan ellátásához szükséges adatvédelmi és információbiztonsági alapelveket.

A Társaság a működése és az általa nyújtott szolgáltatások teljesítése során elkötelezett a vonatkozó törvényi, valamint az irányadó szabványokban foglalt előírásoknak való maximális megfelelés iránt, így különösen az MSZ ISO/IEC 27001 szabványban meghatározott iránymutatásoknak való megfelelés iránt, azáltal, hogy magára nézve a hivatkozott törvényeket és szabványokat kötelezően alkalmazandónak ismeri el.

A 4iG Informatikai Zrt. felső vezetése az IBP-ben megfogalmazott elvek és követelmények teljesítését várja el a Társaság összes munkatársától, beszállítótól és minden egyéb érdekelt féltől. Az IBP hatálya kiterjed a Társaság valamennyi folyamatára és szervezeti egységre, így különösen a Társaság elektronikus információs rendszereire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, a környezeti infrastruktúra elemeit és objektumait, a papír alapú dokumentumokat, továbbá minden eljárására, melyek hatással lehetnek a 4iG Csoport adatvagyonára.

Célkitűzések

A Társaság az összes tevékenysége, szolgáltatása és folyamata során mind a belső üzemeltetés során, mind az ügyfelek, partnerek felé törekszik az elvártaknak megfelelő bizalmasság, sértetlenség és rendelkezésre állás biztosítására az információbiztonság tekintetében.

Alapelvek

A **védelem teljes körűségének** alapelvét be kell tartani. Az elvet érvényesíteni kell az összes rendszerlemre, a fizikai-logikai és az adminisztratív védelmi intézkedésekre is.

Zártság alapelvén belül biztosítani kell, hogy a fenyegetések ellen meglévő védelmi intézkedések megvalósításra kerültek és azok szerves egységet alkotnak.

A **védelem kockázatarányosságának** alapelve, hogy a védelem mértéke és a költségei a kockázatokkal arányosak legyenek. A védelmi intézkedések költségvonzatának és szigorúságának összhangban kell állnia a védett adat értékével és a bekövetkező kár nagyságával. Célkitűzés a minimális költséggel elért maximális védelmi képesség.

A **védelem folytonosságának** alapelve, hogy az informatikai rendszerek bevezetése során kialakított védelmi képességét a rendszer teljes életciklusa alatt folyamatosan biztosítani és fejleszteni kell.

Audit

A Társaság rendszeres ellenőrzésekkel megbizonyosodik arról, hogy a politikában kitűzött célok megvalósulnak-e és a vonatkozó utasításokat és eljárásokat az érintettek betartják-e. Amennyiben az előírásokkal ellentétes folyamatot, vagy munkavállalói magatartást tapasztal, úgy megteszi a szükséges intézkedést a probléma kiküszöbölése érdekében.

Budapest, 2026. május 13.

Radó Gábor

4iG Informatikai Zrt. vezérigazgató