Control Pro Mérnöki Szolgáltató Kft.

INFORMÁCIÓBIZTONSÁGI POLITIKA

Hatályba lépés időpontja: 2026.05.01.

VERZIÓKEZELÉS

Verzió	Dátum	Fejezet(-ek)	Módosítás oka, lényege
1.0	2026.05.01.	teljes	jóváhagyás
1.1	2026.06.23.	több pont	pontosítás, testreszabás

INFORMÁCIÓBIZTONSÁGI POLITIKA

Az Információbiztonsági politika célja, hogy a Control Pro Mérnöki Szolgáltató Kft. teljes egészére megfogalmazza azt a vezetői szándékot, amely a szervezet és a szervezet informatikai rendszerei által kezelt adatok és információk biztonságának megőrzésére irányulnak.

A Control Pro Kft. ipari automatizálási, energetikai és SCADA rendszerekkel kapcsolatos mérnöki szolgáltatásokat nyújt, amelyek kritikus infrastruktúrák működését támogathatják. Ennek megfelelően az információbiztonság kiemelt jelentőségű az üzletmenet folytonossága és az ügyfélbizalom fenntartása szempontjából.

A Control Pro Mérnöki Szolgáltató Kft. az informatikai biztonság területén az alábbi biztonsági alapelveket érvényesíti:

- Bizalmasság: az információt védeni kell a jogosulatlan hozzáféréstől, közzétételtől. Meg kell akadályozni, hogy üzleti titok a versenytársak birtokába kerüljön, az üzleti információk bizalmassága sérüljön.
- Sértetlenség: biztosítani kell, hogy az információ mindig pontos, teljes, valamint érvényes az üzleti értékeknek és várakozásoknak megfelelően.
- Rendelkezésre állás: biztosítani kell, hogy az üzleti folyamatokhoz szükséges információ hozzáférhető legyen most és a jövőben. Biztosítani kell a szükséges erőforrások védelmét is.
- Biztonsági kockázat: a jelentős kárértéket képviselő veszélyforrásokra védelmi intézkedésekkel szükséges a kockázatot elviselhető mértékűre csökkenteni az esetek többségében.
- A védelem teljeskörűsége: a fizikai, a logikai és az adminisztratív védelmet a következő három dimenzióban kell érvényesíteni:
    - az összes rendszerelemre,
    - a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén,
    - a központi, illetve a végponti informatikai eszközökre és környezetükre.
- A védelem zártsága: a Társaság által meghatározott kockázati érték felett az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.
- A védelem kockázatarányossága: a védelmi célkitűzések és informatikai biztonsági követelmények teljesítése érdekében biztosítani kell a kellő, észszerű, költséghatékony, kockázatokkal arányos védelmi intézkedések és kontrollok – a mindenkori rendelkezésre álló erőforrásoknak megfelelő – alkalmazását.
- A védelem folyamatossága: a kialakított védelmi intézkedéseket a folyamatosan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fenn kell tartani.

A Társaság az alapelvek figyelembe vételével tervezte meg, alakította ki, működteti és fejleszti információbiztonsági irányítási rendszerét annak érdekében, hogy a kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az ezeket veszélyeztető mindenkori

fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét biztosítsa logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

A Társaság vezetése elkötelezett, és kiemelten fontos feladatnak tartja a szervezet elektronikus információs rendszerei és a bennük tárolt adatok védelmét, és az ellenőrző folyamatok kialakításával, rendszeres kontrolltevékenységekkel és az információbiztonság folyamatokba integrálásával fejleszti a biztonsági szintet.

A Társaság vezetése elkötelezett aziránt, hogy az elvárások megfelelő, korszerű és biztonságos adatkezelés valósuljon meg.

Az információbiztonsági irányítási rendszer működtetéséért az ügyvezető által kijelölt információbiztonsági felelős (ISMS felelős) tartozik felelősséggel.

A Társaság elkötelezett az információbiztonsági irányítási rendszer folyamatos fejlesztése mellett, a kockázatértékelések, auditok és vezetőségi átvizsgálások alapján.

A Társaság vezetése, minden munkatársa és szerződéses partnere felelős a kezelésükre bízott adatokra vonatkozó információbiztonsági alapelvek, elvárások betartásáért, ezekről az alapelvekről, elvárásokról rendszeres oktatásban részesül, és az elvárásoknak, alapelveknek megfelelően védi a kezelt adatokat.

Kelt: Budapest, 2026.06.23.

Jován Zoltán

ügyvezető