Információbiztonsági politika

A JAKO Kft etikai, jogi és szakmai kötelessége annak biztosítása, hogy a birtokában lévő információk megfeleljenek a bizalmasság, a sértetlenség és a rendelkezésre állás elveinek. Biztosítanunk kell, hogy az általunk tárolt információkat, vagy amely információkért felelősek vagyunk, megóvjuk a nem megfelelő közzétételtől; biztosítjuk, hogy pontos, időszerű és azonosítható legyen; és elérhető legyen azok számára, akiknek hozzáféréssel kell rendelkezniük. Cégünk információbiztonsági politikája biztosítja a keretet, amelyen belül mindezeket az elveket figyelembe vesszük.

A JAKO Kft olyan integrált irányítási rendszert működtet, amely az információbiztonság vonatkozásában megfelel az ISO/IEC 27001:2013 szabvány és a TISAX követelményeinek.

Jelen politikai nyilatkozat a vállalat minden dolgozója számára irányadó, és kiterjed a vállalat teljes működésére.

A JAKO Kft. legfőbb célkitűzései:

(1) A vállalat és érdekelt felelei üzleti-, személyes-, és szellemi tulajdonjoghoz köthető adatainak és információinak széleskörű védelme, a bizalmasságuk, sértetlenségük és rendelkezésre állásuk biztosítása, összhangban valamennyi érdekelt fél elvárásaival és az alkalmazható jogszabályi és egyéb szabályozó követelményekkel.

(2) A felmerülő kockázatokkal arányos védelmi intézkedések, jól működő, biztonsági eljárások, biztonságos információs rendszerek, eszközök és infrastruktúra, továbbá magasan képzett munkatársak alkalmazása.

(3) A felhasználóink számára a mindennapos tevékenységük részeként a lehető legmagasabb fokú információbiztonság elérése. Ennek érdekében rendszeres információbiztonsági ismeretekkel kapcsolatos képzések nyújtása a személyzet számára, hogy teljesíteni tudják szerepüket az információbiztonsági követelmények teljesítésében.

(4) Információbiztonság irányításunk hatékonyságának rendszeres ellenőrzése és értékelése belső információbiztonsági auditokkal és jelentésekkel, melyek eredményeit a folyamatok és eljárások folyamatos javításához céltudatosan használunk.

(5) A potenciális információbiztonsági kockázatok megállapítása, értékelése és csökkentése, megfelelő technikák alkalmazásával. Az információbiztonság lehetséges fenyegetésének és védelmi lehetőségének figyelembevétele a kockázatkezelési folyamatban.

(6) A beszállítók és ellátási láncuk információbiztonsági kockázatainak hatékony kezelése.

A felső vezetés támogatja az információbiztonsággal kapcsolatos megelőző intézkedéseket és ezt a vezetői feladatai között kezeli.

……	……
Andreas Koch	Molnár Gábor
Ügyvezető	Minőségir. vezető

Készítette: Andreas Koch 2021.07.01, Rev.0
Utolsó felülvizsgálat: Molnár Gábor 2023.09.13