Verzia: 2, platí od 10.03.2023

Politika informačnej bezpečnosti

Vedenie spoločnosti **IFT InForm Technologies, a.s.** sa zaväzuje chrániť **dôvernosť, integritu a dostupnosť** informačných aktív v rámci celej organizácie. Dodržiavanie tohto záväzku je dlhodobo nutné pre získanie a udržanie konkurenčnej výhody, ziskovosti, súladu s právnymi a zmluvnými záväzkami a imidžu spoľahlivej a dôveryhodnej firmy. Za týmto účelom spoločnosť zaviedla a prevádzkuje **systém riadenia informačnej bezpečnosti** (SRIB) podľa normy **ISO/IEC 27001:2013**. Systém riadenia pokrýva všetky priestory v sídle spoločnosti v Bratislave, všetky informačné systémy a ostatné informačné aktíva.
Hlavný dôraz je pritom kladený na ochranu aktív súvisiacich s:

- dodržiavaním zmluvných a legislatívnych záväzkov,
- ochranou osobných údajov a súkromia,
- ochranou duševného vlastníctva,
- zabezpečením dát organizácie,
- riadením kontinuity v prípade havárií a napadnutia.
- zabezpečením správnych a objektívnych výsledkov monitorovania zákazníckych systémov.

Vedenie spoločnosti si je vedomé, že iba technické opatrenia nepostačujú na minimalizovanie všetkých existujúcich hrozieb, a preto bude aktívne formovať a zlepšovať bezpečnostné povedomie zamestnancov.
Na dôkaz dodržiavania požiadaviek normy sa spoločnosť podrobuje pravidelným externým auditom vykonávaným akreditovaným certifikačným orgánom.
Všetci zamestnanci musia konať v súlade s touto politikou a postupmi vyplývajúcimi zo zavedeného systému riadenia informačnej bezpečnosti. Spoločnosť zaviedla transparentné disciplinárne opatrenia pre prípady porušovania schválených bezpečnostných opatrení.

Hodnotenie bezpečnostných rizík

Zachovanie bezpečnosti informačných aktív je v súlade s obchodnými cieľmi spoločnosti. Systém riadenia informačnej bezpečnosti slúži ako nástroj na znižovanie súvisiacich rizík na akceptovateľnú úroveň. Posudzovanie rizík je základom účinného fungovania systému a podkladom pre účelné vynakladanie zdrojov. Vykonáva sa podľa potreby, no najmenej 1x ročne.
Výsledky posúdenia rizík sú predkladané vedeniu spoločnosti, ktoré rozhoduje o kritériách pre akceptovanie rizík a schvaľuje zostatkové riziká.

Zvládanie bezpečnostných incidentov a havarijných stavov

V spoločnosti je zavedený systém sledovania a ohlasovania bezpečnostných incidentov. Všetci zamestnanci sú poučovaní o tom, ako reagovať, ak zaznamenajú podozrivú aktivitu.

Vyhodnocovanie účinnosti systému riadenia informačnej bezpečnosti

Na hodnotenie účinnosti zavedeného systému riadenia máme zavedené postupy monitorovania a interných auditov. Účinnosť systému riadenia informačnej bezpečnosti je vyhodnocovaná vedením spoločnosti aspoň 1x ročne.

Bratislava, marec 2023

Ing. Jozef Lezo

Člen predstavenstva