DEKLARACE
POLITIKY INFORMAČNÍ BEZPEČNOSTI

Východiskem Politiky informační bezpečnosti (dále jen PIB) je potřeba zajistit nerušené plnění strategických a ekonomických cílů společnosti IPEX zahrnující i ochranu informačních aktiv a zájmů našich zákazníků/obchodních partnerů a všech relevantních zainteresovaných stran. Naplnění PIB je realizováno implementovaným systémem řízení informační bezpečnosti (ISMS) a je postaveno na osobní angažovanosti, zodpovědnosti a aktivitě nejen řídících, tj. všech zaměstnanců společnosti.

Cílem ISMS je především zabezpečit adekvátně k rizikům dostupnost, integritu a důvěrnost informací při všech činnostech souvisejících s předmětem podnikání společnosti. Nedělitelnou součástí je řízení shody s regulatorními a legislativními požadavky.

Bezpečnost ve společnosti řídí předseda představenstva. Pro zajištění výkonu bezpečnostních funkcí ve společnosti jsou stanoveny bezpečnostní role. Role jsou vykonávány pracovníky společnosti nebo jsou zajištěny službami externích subjektů. Celý ISMS je 1x ročně revidován managementem

Strategickými záměry jsou:

- Při budování ISMS vycházet především z mezinárodních norem ISO/IEC skupiny 2700 (27001, 27002, 27005, 27011). Opatření v oblasti bezpečnosti informací jsou aplikována v těchto oblastech:
    - Organizace bezpečnosti informací
    - Bezpečnost lidských zdrojů
    - Řízení aktiv
    - Řízení přístupu
    - Kryptografie
    - Fyzická bezpečnost a bezpečnost prostředí
    - Bezpečnost provozu
    - Bezpečnost komunikací
    - Akvizice a údržba systémů
    - Dodavatelské vztahy
    - Řízení incidentů bezpečnosti informací
    - Aspekty řízení kontinuity činností organizace
    - Soulad s požadavky
- Dodržovat platnou legislativu ve všech oborech činnosti a podporovat a chránit obchodní a technické procesy obchodních partnerů, informace o partnerech a informace partnerů.
- Trvalou pozornost věnovat racionalizaci a zdokonalování ISMS (aplikace metody P-D-C-A) tak, aby docházelo k optimalizaci činností a nákladů.

Bezpečnost je realizována tak, aby byla ekonomicky smysluplná a nebránila společnosti v dosahování jejích cílů. Rizika se hodnotí z hlediska vlivu na dosahování cílů společnosti, dodržení úrovně poskytovaných služeb ze smluvních ujednání a z hlediska možných finančních a jiných dopadů na společnost.

Proces řízení rizik je základním nástrojem předcházení škod. Prioritně jsou zvládána vysoká rizika v souvislostech možných dopadů, významu zabezpečovaných aktivit a možností společnosti uvolnit potřebné zdroje.

Systém řízení je podroben soustavnému monitorování, vyhodnocování stavu bezpečnosti a zavádění adekvátních nápravných opatření.

Preferuje se prevence bezpečnostních incidentů. Incidenty, které se přesto stanou, jsou vyšetřeny a analyzovány. Poté jsou navržena a provedena opatření s cílem zabránit opakovanému výskytu incidentů.

Bezpečnostní povědomí je ve společnosti soustavně upevňováno. Povinnosti a pravidla jsou školeny. Kvalifikace pracovníků pověřených výkonem bezpečnostních rolí je managementem systematicky pěstována a kontrolována.