Bezpečnostní politika ISMS

Vedení společnosti Thein Security s.r.o. (dále jen společnost) přikládá velký význam zabezpečení informací, které jsou mu svěřeny do péče a se kterými zachází. Vnímá ochranu informací svých i informací svých klientů jako ucelenou a řízenou soustavu vyvážených opatření, jejichž cílem je přiměřeně chránit všechna důležitá aktiva. Prioritní je zejména ochrana osobních dat klientů zákazníků zpracovávaných společností z hlediska zákona na ochranu osobních údajů.

Základním úkolem je zajištění dostupnosti, integrity a důvěrnosti dat. Pro ochranu svých i svěřených informací společnost vybudovalo, udržuje a rozvíjí systém řízení bezpečnosti informací ve smyslu ČSN ISO/IEC 27001:2014. Systém řízení bezpečnosti informací vychází z cílů bezpečnosti informací a dále z určených a ohodnocených rizik.

Systém dále zahrnuje určení povinností a odpovědností spolu s vytvořením a dodržováním zdokumentovaných bezpečnostních zásad a postupů. Systém současně stanovuje rozsah kritérií hodnocení rizik a zahrnuje kontroly dodržování stanovených pravidel, definici zákonných, regulatorních a smluvních požadavků, vzdělávání pracovníků a postupy pro reakci na bezpečnostní incidenty.

Společnost se zavazuje na základě analýzy rizik plnit bezpečnostní opatření, v prioritách daných plánem zvládání rizik, a bezpečnostních požadavků v následujících oblastech:

- Organizační bezpečnost, která definuje odpovědnosti a rozsah systému řízení bezpečnosti.
- Bezpečnost lidských zdrojů, jejímž cílem je, aby se s důvěrnými informacemi seznamoval pouze pracovník k tomu určený, byl náležitě vybrán a svých povinností si byl vědom.
- Klasifikace a řízení aktiv určující způsob identifikace a ohodnocení aktiv, způsob klasifikace informací a způsob zacházení s nimi. Oblast postihuje i samotnou „Analýzu rizik“, včetně stanovení její struktury a kritérií hodnocení.
- Řízení přístupu, které definuje ochranu a kontrolu přístupu k informacím, službám a procesům.
- Kryptografie k ochraně důvěrnosti, autentičnosti a integrity informací.
- Fyzická bezpečnost a bezpečnost prostředí předcházející neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do informací Thein Security s.r.o. a do prostor, ve kterých se nacházejí zařízení Thein Security s.r.o.
- Bezpečnost provozu, které stanovuje postupy pro řádný a bezpečný provoz prostředků pro zpracování informací Thein Security s.r.o. a služeb s tím souvisejících
- Bezpečnost komunikací s cílem zajistit jejich ochranu a bezpečnost při vzniku, uchování i přenosu v rámci a mimo společnost.
- Akvizice, vývoj a údržba systémů, které definuje bezpečnostní pravidla vývoje a údržby systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
- Dodavatelské vztahy je třeba řídit také z hlediska dohodnuté úrovně bezpečnosti informací a dodávek služeb, týkajících se systému bezpečnosti informací.

- Řízení incidentů bezpečnosti, které stanovuje postupy reakce na poruchy pravidel, bezpečnosti a odolnosti systému ISMS.
- Řízení kontinuity činností organizace, které stanovují rámec prevence a reakce na krizové situace formou plnění plánů kontinuity.
- Zajištění souladu s požadavky, která rozpracovává konkrétní postupy v oblasti zajištění shody přijímaných opatření s legislativou a bezpečnostními technologickými požadavky.

Management společnosti trvale zajišťuje, že politika bezpečnosti informací:

a) Odpovídá záměrům společnosti,
b) Zahrnuje závazek k plnění požadavků a k neustálému zlepšování efektivnosti systému,
c) Poskytuje rámec pro stanovení a přezkoumání bezpečnostních cílů,
d) Je trvale přístupná a je sdělována a pochopena v organizaci při školeních zaměstnanců,
e) Je pravidelně přezkoumávána z hlediska kontinuity vhodnosti formou „Přezkoumání vedení“ společně se systémem řízení kvality.

Jednatelé společnosti

V Praze dne: 1. 1.2022