Information Security Management System

Vrcholová politika systému bezpečnosti informací

	Datum:	Jméno:	Podpis:
Vypracoval:	**12.1.2023**	**Ing. Vladimír Hampl**	
Ověřil:	**12.1.2023**	**Ing. Jiří Placht**	
Uvolnil:	**12.1.2023**	**MBI**	

1. Vrcholová politika ISMS

(1) Politika ISMS (Politika systému bezpečnosti informací) je plně podporována valnou hromadou společnosti, jednateli a vedením společnosti v čele s ředitelem společnosti.

2. Prohlášení vedení společnosti

(1) V souladu s požadavky ČSN ISO/IEC 27001:2014 vyhlásilo vedení společnosti Politiku bezpečnosti informací jako svůj závazek.

(2) Záměrem vedení je podporovat cíle a principy bezpečnosti informací.

3. Strategie v oblasti bezpečnosti informací

(1) Respektovat všechny právní předpisy, standardy, normy a doporučení související s činností firmy a procesy řízení bezpečnosti a ochrany informací.

(2) Trvale vytvářet podmínky k zajišťování všech zdrojů potřebných k zavedení, udržování a soustavnému zlepšování systému řízení bezpečnosti informací.

(3) Uplatňovat politiku založenou na principech důvěrnosti, dostupnosti a integrity informací, na dodržování právních a normativních předpisů a na smluvních požadavcích zainteresovaných stran.

(4) Zajistit bezpečnost informačních aktiv firmy pomocí přiměřených a odpovídajících opatření.

(5) Pravidelně hodnotit plnění cílů a cílových hodnot vycházejících z analýzy rizik a této politiky.

(6) Prezentovat profesionální přístup a postavení firmy přesným uplatňováním zásad informační bezpečnosti vůči smluvním partnerům a třetím stranám.

(7) Úroveň bezpečnosti nastavovat přiměřeně bezpečnostním rizikům a významu zajišťovaných aktivit. Rizika se hodnotí z hlediska vlivu na dosahování cílů firmy, na dodržení úrovně poskytovaných služeb a z hlediska možných finančních a jiných dopadů na firmu.

(8) Prioritně zvládat vysoká rizika v souvislostech možných dopadů, významu zabezpečovaných aktivit a možností firmy uvolnit potřebné zdroje. Proces řízení rizik je základním nástrojem předcházení škod.

(9) ISMS podrobovat soustavnému monitorování, vyhodnocování stavu bezpečnosti a zavádění adekvátních nápravných opatření. Preferuje se prevence bezpečnostních incidentů.

(10) Vědomí informační bezpečnosti je soustavně upevňováno a zaměstnanci jsou pravidelně proškolováni. Kvalifikace zaměstnanců pověřených výkonem bezpečnostních rolí je systematicky rozvíjena.

(11) Při realizaci cílů politiky ISMS očekává vedení firmy od každého zaměstnance:

- důsledné a přesné dodržování postupů stanovených interními dokumenty integrovaného systému řízení
- vysokou odpovědnost za jakost vlastní práce spočívající v předcházení chybám
- důslednou kontrolu výsledků své práce před jejich předáním spolupracovníkům nebo smluvním partnerům