

Prohlášení vedení společnosti Pow-en a. s. k oblasti informační bezpečnosti

Ve společnosti Pow-en a. s. je bezpečnost informací klíčovým prvkem k udržení důvěry našich zákazníků, partnerů i zaměstnanců. Bezpečnost informací je charakterizována jako zachová ní důvěrnosti, integrity a dostupnosti informací, přičemž:

- důvěrnost je zajištění toho, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům,
- integrita je zabezpečení přesnosti a úplnosti informace a metod jejího zpracování,
- dostupnost je zajištění toho, že informace je přístupná a použitelná na žádost oprávněného jednotlivce, entity nebo procesu.

Pro její podporu a zajištění dobrého jména společnosti, spokojenosti zákazníků a všech dalších zainteresovaných stran se rozhodlo pro zavedení, podporu a zlepšování systému řízení bezpečnosti informací (ISMS) podle mezinárodní normy ISO/IEC 27001:2022.

Systém řízení informační bezpečnosti platí pro všechny oblasti činností Pow-en, a.s., týkající se služeb dodávky inteligentních měřících zařízení a dodávky elektrické energie a plynu včetně poskytování služby zákaznického portálu.

Vedení Pow-en a. s., vyjadřuje svůj záměr Závazkem k zásadám bezpečnosti informací:

- respektovat všechny legislativní předpisy, standardy a normy související s ochranou bezpečnosti informací a osobních údajů;
- zajistit integraci požadavků systému řízení informační bezpečnosti do procesů organizace;
- zajistit dostupnost zdrojů potřebných pro vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a řádné dokumentování systému řízení informační bezpečnosti;
- dodržovat povinnosti v oblasti kybernetické bezpečnosti v souladu se strategií kybernetické bezpečnosti a určenými bezpečnostními politikami a postupy;
- podporovat relevantní řídicí role k prokázání jejich vůdčí role v oblastech jejich odpovědnosti a personál k přispívání efektivnosti systému řízení informační bezpečnosti;
- komunikovat význam efektivního řízení bezpečnosti informací;
- prosazovat bezpečnostní opatření, která vedou k ochraně aktiv společnosti a aktiv jí svěřených na základě identifikace a hodnocení rizik;
- zajišťovat systematické vzdělávání zaměstnanců v oblasti bezpečnosti informací;
- pravidelně hodnotit soulad ISMS a zvyšovat jeho účinnost.

V Bratislavě 1 0. SEP 2026

.....
Generální ředitel