**Prehlásenie vedenia spoločnosti Pow-en, a.s. k oblasti informačnej bezpečnosti**

V spoločnosti Pow-en, a.s. je bezpečnosť informácií kľúčovým prvkom na udržanie dôvery našich zákazníkov, partnerov i zamestnancov. Bezpečnosť informácií je charakterizovaná ako zachovanie dôvernosti, integrity a dostupnosti informácií, pričom:

- dôvernosť je zabezpečenie toho, že informácia nie je dostupná alebo nie je odhalená neoprávneným jednotlivcom, entitám alebo procesom,
- integrita je zabezpečenie presnosti a úplnosti informácie a metód jej spracovania,
- dostupnosť je zabezpečenie toho, že informácia je prístupná a uplatniteľná na žiadosť oprávneného jednotlivca, entity alebo procesu.

Pre jej podporu a zabezpečenie dobrého mena spoločnosti, spokojnosti zákazníkov a všetkých ďalších zainteresovaných strán sa rozhodlo pre zavedenie, podporu a zlepšovanie systému riadenia bezpečnosti informácií (ISMS) podľa medzinárodnej normy ISO/IEC 27001:2022.

Systém riadenia informačnej bezpečnosti platí pre všetky oblasti činností Pow-en, a.s., týkajúce sa služieb dodávky inteligentných meracích zariadení a dodávky elektrickej energie a plynu vrátane poskytovania služby zákazníckeho portálu.

Vedenie Pow-en, a.s., vyjadruje svoj zámer Záväzkom k zásadám bezpečnosti informácií:

- rešpektovať všetky legislatívne predpisy, štandardy a normy súvisiace s ochranou bezpečnosti informácií a osobných údajov;
- zabezpečiť integráciu požiadaviek systému riadenia informačnej bezpečnosti do procesov organizácie;
- zabezpečiť dostupnosť zdrojov potrebných na vybudovanie, zavedenie, prevádzku, monitorovanie, preskúmanie, udržiavanie, zlepšovanie a riadne dokumentovanie systému riadenia informačnej bezpečnosti;
- dodržiavať povinnosti v oblasti kybernetickej bezpečnosti v súlade so stratégiou kybernetickej bezpečnosti a určenými bezpečnostnými politikami a postupmi;
- podporovať relevantné riadiace úlohy na preukázanie ich vedúcej úlohy v oblastiach ich zodpovednosti a personál na prispievanie efektívnosti systému riadenia informačnej bezpečnosti;
- komunikovať význam efektívneho riadenia bezpečnosti informácií;
- presadzovať bezpečnostné opatrenia, ktoré vedú k ochrane aktív spoločnosti a aktív jej zverených na základe identifikácie a hodnotenia rizík;
- zabezpečovať systematické vzdelávanie zamestnancov v oblasti bezpečnosti informácií;
- pravidelne hodnotiť súlad ISMS a zvyšovať jeho účinnosť.

V Bratislave 10.09.2026

.....

Generálny riaditeľ