

## **BEZPEČNOSTNÍ POLITIKA ISMS**

Společnost Colsys s.r.o. je dodavatel a systémový integrátor v oblasti bezpečnostních, slaboproudých a komunikačních technologií, AV technologií, silnoproudých a řídicích systémů. Tuto činnost zajišťujeme po celém území ČR a v zahraničí.

Společnost přikládá velký význam zabezpečení informací, které jsou jí svěřeny do péče a se kterými zachází. Vnímá ochranu informací svých i informací svých obchodních partnerů jako ucelenou a řízenou soustavu vyvážených opatření, jejichž cílem je přiměřeně chránit všechna důležitá aktiva. Prioritní je zejména komplexní ochrana technologických dat našich zákazníků, která jsou zpracovávána v rámci projekčních, instalačních a servisních dodávek jednotlivých systémů. Základním úkolem je zajištění dostupnosti, integrity a důvěrnosti dat.

Pro ochranu svých i svěřených informací společnost Colsys s.r.o. vybuodovala, udržuje a rozvíjí systém řízení bezpečnosti informací ve smyslu ČSN EN ISO/IEC 27001.

Systém řízení bezpečnosti informací vychází z cílů integrovaného systému řízení 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 kritéria hodnocení rizik a zahrnuje kontroly dodržování stanovených pravidel, definici zákonných, regulatorních a smluvních požadavků, vzdělávání pracovníků a postupy pro reakci na bezpečnostní incidenty.

Společnost Colsys s.r.o. se zavazuje na základě analýzy rizik plnit bezpečnostní opatření, v prioritách daných Plánem zvládnání rizik, a bezpečnostní požadavky v následujících oblastech:

- **Organizační bezpečnost**, která definuje odpovědnosti a rozsah systému řízení bezpečnosti.
- **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.
- **Bezpečnost lidských zdrojů**, jejímž cílem je, aby se s důvěrnými informacemi seznamoval pouze oprávněný pracovník.
- **Fyzická bezpečnost a bezpečnost prostředí** předcházející neautorizovanému přístupu, poškození, znehodnocení, zničení či jiným zásahům do informací společnosti a do prostor, ve kterých se nacházejí zařízení společnosti.
- **Řízení komunikací a řízení provozu**, které stanovuje postupy pro řádný a bezpečný provoz prostředků pro zpracování informací a služeb s tím souvisejících.
- **Řízení přístupu**, které definuje ochranu a kontrolu přístupu k informacím, službám a procesům.
- **Akvizice, vývoj a údržba systémů**, které definuje bezpečnostní pravidla vývoje a údržby systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu.
- **Zvládnání bezpečnostních událostí**, 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 či technologickými požadavky.

Společnost Colsys s.r.o. trvale zajišťuje, že politika bezpečnosti informací odpovídá záměrům společnosti, její požadavky jsou plněny a je kladen důraz na neustálé zlepšování systému řízení bezpečnosti informací. Politika bezpečnosti informací je společně s integrovaným systémem řízení pravidelně přezkoumávána a komunikována v rámci organizace formou školení zaměstnanců.

V Kladně dne: 5. 2. 2024

ředitel společnosti  
Ing. Pavel Hlavinka