Vnitropodniková směrnice ISMS Politika

Politika systému řízení bezpečnosti informací (ISMS)

MiCoS SOFTWARE s.r.o.

1. Úvod

Vedení společnosti MiCoS SOFTWARE s.r.o. považuje systém řízení bezpečnosti informací (ISMS) za nedílnou součást podnikatelského záměru a strategického řízení. ISMS zahrnuje provoz, rozvoj a neustálé zlepšování bezpečnosti informací napříč všemi procesy a je integrován do organizační struktury, plánování a správy zdrojů.

Cílem této politiky je chránit všechna informační aktiva společnosti, zajistit důvěrnost, integritu a dostupnost informací a minimalizovat rizika, která by mohla ohrozit naše služby, pověst či důvěru našich klientů.

2. Kontext a účel

MiCoS SOFTWARE s.r.o. působí na trhu informačních technologií od roku 1991. Neustále se vyvíjíme, reagujeme na technologické trendy a potřeby našich zákazníků. Řízení bezpečnosti informací chápeme jako klíčový prvek zajištění dlouhodobé spokojenosti zákazníků a obchodních partnerů.

Tato politika stanovuje závazky, zásady a rámec pro řízení bezpečnosti informací v souladu s normou ČSN EN ISO/IEC 27001:2023 a platí pro všechny zaměstnance, dodavatele, smluvní partnery a další zainteresované strany, které zpracovávají nebo mají přístup k informacím společnosti.

3. Závazek vedení

Vedení společnosti se zavazuje, že:

- poskytne potřebné zdroje pro zavedení, udržování a neustálé zlepšování ISMS,
- bude uplatňovat zásady důvěrnosti, integrity a dostupnosti informací,
- zajistí plnění právních, regulačních a smluvních požadavků, včetně požadavků GDPR,
- bude prosazovat program zvyšování povědomí o informační bezpečnosti mezi zaměstnanci,

- zajistí, aby ISMS poskytoval zákazníkům a partnerům jistotu při nakládání s jejich informacemi a daty,
- bude podporovat profesionální přístup k informační bezpečnosti vůči všem třetím stranám.

4. Zásady bezpečnosti informací

Společnost MiCoS SOFTWARE s.r.o. uplatňuje tyto hlavní zásady:

1. Ochrana důvěrnosti, integrity a dostupnosti všech informačních aktiv.
2. Identifikace a řízení rizik souvisejících s informačními aktivy a službami.
3. Přístupová kontrola a používání vhodných autentizačních mechanismů.
4. Školení a zvyšování povědomí o bezpečnosti u všech zaměstnanců a spolupracovníků.
5. Řízení bezpečnostních incidentů – jejich rychlá detekce, hlášení a náprava.
6. Pravidelné kontroly, audity a revize bezpečnostních opatření.

5. Ochrana osobních údajů

Společnost se zavazuje chránit osobní údaje v souladu s platnými právními předpisy, zejména nařízením GDPR, a uplatňovat vhodná technická a organizační opatření k ochraně soukromí jednotlivců.

6. Odpovědnosti

- Vedení společnosti: stanovuje strategii a cíle ISMS, schvaluje tuto politiku a zajišťuje potřebné zdroje.
- Vedoucí pracovníci: odpovídají za implementaci politiky v rámci svých oddělení a dohled nad dodržováním zásad.
- Všichni zaměstnanci a spolupracovníci: jsou povinni dodržovat stanovené zásady, interní předpisy a podílet se na udržování bezpečného prostředí.

7. Přezkoumání a aktualizace politiky

Tato politika je pravidelně přezkoumávána vedením minimálně jednou ročně a vždy po významných změnách v organizaci, legislativě, technologii nebo v hodnocení rizik. O všech verzích a změnách je vedena dokumentovaná historie.

Tato směrnice nabývá účinnosti dnem 9.4.2025

V Ostravě dne 9.4.2025