Politika bezpečnosti informací (ISMS)

ORSIA, spol. s r.o. je dodavatelem aplikačního programového vybavení v oblasti informačních technologií. Kromě návrhu, vývoje, realizace a implementace informačních systémů, zpracovává také ekonomické agendy jak pro vlastní potřeby, tak i externím zákazníkům, které podléhají zákonu o ochraně osobních údajů. Pro účinné zpracování informací a jejich dostatečnou ochranu přijala a schválila dne 13. 12. 2023 rada vedení společnosti tuto politiku bezpečnosti informací:

a) Závazek vedení

Vedení provádí pravidelné periodické monitorování a vyhodnocování analýz bezpečnostních rizik a přijímá odpovídající opatření vedoucí k omezení jejich vlivu.
V rámci celé organizace zajišťuje neustálé zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti informací, zamezení jejich modifikace, zneužití a ztráty informací) v souladu s obecně závaznými právními předpisy a smluvními požadavky.
Způsob zpracování informací je definován souborem vnitřních předpisů a dokumentovaných postupů, které jsou vedením podporovány, prosazovány a sdělovány všem zaměstnancům.
Náklady na zajištění bezpečnosti informací musí být vynakládány efektivně, tzn. aby odpovídaly významu a ceně informací.

b) Hlavní zásady práce s informacemi a způsob jejich zabezpečení

- Zajistit ochranu osobních údajů v souladu s platnou legislativou.
- Začleňovat zabezpečení informací do odpovědnosti za práci.
- Zajišťovat vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací.
- Zabezpečovat informace při zaměstnání na dálku.
- Provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací.
- Vytvářet a prosazovat systém řízeného přístupu k informacím a omezit přístup k informacím (používání hesel).
- Prosazovat a zajišťovat politiku bezpečného pracoviště.
- Provádět kontrolu připojení a směrování sítě.
- Vytvářet a prosazovat bezpečnostní pravidla pro přenosná počítačová zařízení a jiné nosiče informací.
- Zajišťovat spolehlivou antivirovou kontrolu celé interní sítě a zabezpečit celou síť proti působení každého zlomyslného SW.
- Zajišťovat pravidelné zálohování dat a ty ukládat na bezpečném místě.
- Udržovat systém způsobu používání informačních aktiv a bezpečných oblastí.

c) Následky porušení informační politiky

- Každý zaměstnanec, kterému byl umožněn přístup k informačním prostředkům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti.
- Přijatá a schválená politika a související bezpečnostní dokumentace je závazná pro všechny uživatele s přístupem k informacím, a to bez ohledu na zastávanou funkci, pozici či roli v organizaci.
- Všichni uživatelé nesou v souladu s platnou legislativou a předpisy svůj díl zodpovědnosti za dodržení, případně porušení pravidel s nimiž byli seznámeni.
- Porušování těchto pravidel ze strany zaměstnanců organizace je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen.
- Všichni zaměstnanci jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou, a upozornit na ně v souladu s příslušnými vnitřními předpisy.
- Příčiny porušení informační politiky se musí analyzovat a přijímat účinná opatření.

V Ústí nad Orlicí dne 25. 3. 2024

Ředitel Ing. Vlastimil Matějka

ORSIA spol. s r.o.
Čs. armády 1181
562 01 Ústí nad Orlicí
IČO: 150 30 261, DIČ: 273-15030261