

Politika bezpečnosti informací

PCS spol. s r. o. je obchodní společností založenou na znalosti vyspělých technologií objektové bezpečnosti, detekce nebezpečných předmětů, ochrany dat v informačních systémech, měřících zařízení a speciálních fyzikálně-chemických analytických metod.

S ohledem na využívání vyspělých technologií při zpracování dat a obecně široký záběr společnosti v oblasti bezpečnostních aplikací musíme klást i důraz na bezpečnost a řízení přístupu k vnitřním informacím a informacím zákazníků. Tím přispíváme nejen ke zvýšení úrovně zabezpečení dat, s nimiž společnost a její zaměstnanci pracují, ale k celkovému upevnění důvěryhodnosti společnosti. V tomto směru vnímá důvěryhodnost vedení společnosti jako přidanou hodnotu pro zákazníka, který vnímá zázemí společnosti jako bezpečné, je spokojen s poskytnutou službou, vrací se a svěřuje společnosti realizaci náročných technologických a bezpečnostních řešení.

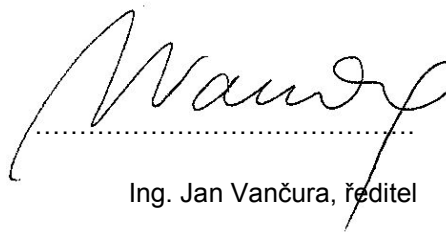
Sledujeme trvale nejnovější bezpečnostní hrozby i trendy v oblasti obrany proti nim a zajišťujeme tak prostředky pro plnění cílů v oblasti bezpečnosti informací a jejich pravidelným přezkoumáním směřujeme společnost k trvalému zvyšování efektivity systému řízení bezpečnosti informací.

Systém řízení bezpečnosti informací je vystavěn na následujících zásadách:

- ochrana dat smluvních partnerů,
- zajištění ochrany osobních údajů v souladu s platnou legislativou,
- vytváření a prosazování systému řízeného přístupu k informacím,
- provádění stálé identifikace bezpečnostních rizik, incidentů a přijímání účinných opatření pro zlepšování bezpečnosti informací,
- zajišťování systematického vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací,
- zpracovávání opatření pro zachování kontinuity činnosti pro případy závažného výpadku v oblasti informací, pravidelné přezkušování a ověřování těchto opatření,
- zabezpečování informačních systémů, internetu, elektronické pošty a dalších způsobů výměny informací přístupných veřejnosti,
- zabezpečování systému fyzického přístupu do prostor,
- nepřetržité zajišťování dostupnosti, spolehlivosti a integrity dat,
- prosazování politiky bezpečného pracoviště, tzn. dodržování zásady čistého stolu, prázdné obrazovky a odpadkového koše bez zabezpečených informací,
- dodržování bezpečnostních pravidel pro přenosná počítačová zařízení a jiné nosiče informací,
- zajišťování spolehlivé kontroly celé interní sítě proti působení zlomyslného softwaru, spolehlivé chránění a zálohování informací,
- sdělování a výměnu informací s třetí stranou provádět pouze na základě zákona, nebo na základě smlouvy uzavřené v písemné formě.

Tato politika je ve společnosti rozpracována do pracovních postupů a pravidel se stanovením odpovědností jednotlivých zaměstnanců.

V Praze dne 24. dubna 2013



Ing. Jan Vančura, ředitel