POLITIKA INFORMAČNÍ BEZPEČNOSTI SPOLEČNOSTI Solutia, s.r.o.

Tato politika má za cíl informovat zákazníky a partnery společnosti i veřejnost o trvalém zájmu chránit všechna informační aktiva a aktiva využívaná na jejich zpracování vůči externím i interním hrozbám, jejich zneužití, prozrazení nebo zničení.

Základním smyslem systému informační bezpečnosti je zabezpečit kontinuální **integritu, dostupnost a důvěrnost datových a jiných aktiv**.

Vedení společnosti Solutia, s.r.o. si je vědomo odpovědnosti za neustálé zvyšování jistoty vlastních aktiv i aktiv našich klientů a ostatních partnerů a produktů poskytovaných stávajícím i novým zákazníkům společnosti s cílem maximálního uspokojení potřeb svých zákazníků. Proto se rozhodlo pro zavedení dokumentovaného systému managementu informační bezpečnosti podle modelu procesně orientovaného systému ČSN ISO/IEC 27001:2006.

Tuto Politiku informační bezpečnosti projednalo a schválilo vedení společnosti pro období červen 2011 až červen 2014 a slouží ke zvýšení celkové stability společnosti a ke zlepšení návratnosti investic. V rámci tohoto procesu bude věnovat společnost trvalou pozornost následujícím oblastem:

- **Zabezpečit soulad** našeho ISMS s obchodními požadavky našich zákazníků a partnerů i se zákony, vyhláškami a všemi relevantními předpisy. **Vyhnout se porušením jakýchkoliv zákonných, statutárních, regulačních nebo smluvních závazků** a jakýchkoliv bezpečnostních požadavků.
- **Řídit rozvoj informační bezpečnosti** uvnitř společnosti i na rozhraních s našimi zákazníky i partnery.
- **Dosáhnout, udržovat a zlepšovat přiměřenou ochranu aktiv** společnosti i našich zákazníků a partnerů. Proto je zkoumána a vyhodnocována situace z hlediska rizik (viz analýza bezpečnostních rizik), kde vedení rozhodne o rozdělení na akceptovatelná a neakceptovatelná a pro ně následně zavádí opatření.
- **Trvale zajistit**, aby bezpečnost a kompatibilita **byly integrální součásti našich informačních produktů.**

Klíčovými nástroji k dosažení zlepšování ve výše uvedených oblastech jsou především následující mechanismy:

- **Zabezpečit, že zaměstnanci, smluvní partneři a uživatelé v pozici třetích stran rozumějí svým odpovědnostem** a že jsou vhodní pro výkon rolí jim přidělených.
- **Obrana před neautorizovaným fyzickým přístupem, poškozením a ohrožováním prostoru a informací** společnosti.
- **Zabezpečení správného a bezpečného provozu prostředků** zpracovávajících informace.
- **Řízení přístupu** k informacím.

Všichni zaměstnanci společnosti, jakož i smluvní partneři a třetí strany, jsou zavázáni příslušnými smlouvami a dohodami zabezpečovat naplňování této politiky v praxi s aktivní podporou vedení naší společnosti, které tuto politiku schválilo. Dále je tato politika rozvinuta v Příručce Systému managementu bezpečnosti informací a v dalších řídicích dokumentech ISMS.

V Praze, dne 02. 07. 2011

Ing. Martin Stufi

ředitel společnosti