Bezpečnostná politika

1. Riadenie informačnej bezpečnosti

Vedenie spoločnosti **RKnet, s. r. o.** so sídlom I. Houdeka 1941/45, Ružomberok 034 01, IČO: 48 065 838, zapísaná v Obchodnom registri Okresného súdu Žilina, Oddiel: Sro, vl. č. 63410/L (ďalej len „Spoločnosť"), ktorá pôsobí v oblasti telekomunikačných služieb, sa zaväzuje chrániť **dôvernosť, integritu a dostupnosť** fyzických a elektronických informačných aktív v rámci celej organizácie.

Za týmto účelom spoločnosť zaviedla a prevádzkuje vlastný **systém riadenia informačnej bezpečnosti (SRIB).** Systém geograficky pokrýva centrálu v Ružomberku, Ludrovej a čiastočne aj v Likavke, ako aj všetky externe umiestnené zariadenia. Z funkčnej stránky slúži SRIB na ochranu všetkých informačných systémov, dát a súvisiacich fyzických a elektronických zariadení.

Vedenie spoločnosti si je vedomé, že samotné technické opatrenia nie sú dostačujúce na minimalizovanie existujúcich hrozieb, a preto vytvára podmienky na zlepšovanie **bezpečnostného povedomia** spolupracovníkov a zamestnancov, napríklad formou školení, účasťou na odborných konferenciách, výstavách a podobne.

Pre účinné riadenie informačnej bezpečnosti je menovaný **Manažér informačnej bezpečnosti** – **Bc. Miroslav Jurečka.**

Všetci zamestnanci a spolupracovníci vystupujúci v mene spoločnosti musia konať v súlade s touto politikou a postupmi, ktoré vyplývajú zo zavedeného SRIB. Rovnako tak spolupracujúce **tretie strany** musia dodržiavať bezpečnostné záväzky vyplývajúce z požiadaviek informačnej bezpečnosti.

Táto bezpečnostná politika je prehodnocovaná vedením spoločnosti minimálne 1x ročne.

2. Hodnotenie bezpečnostných rizík

Zachovanie bezpečnosti informačných aktív je v súlade s obchodnými cieľmi spoločnosti. **Analýza rizík je základom fungovania SRIB a podkladom pre účelné**

vynakladanie zdrojov. Vykonáva sa podľa potreby, no najmenej 1x ročne. Vedenie spoločnosti rozhoduje o kritériách pre akceptovanie rizík a schvaľuje zostatkové riziká.

3. Reakcia na bezpečnostné incidenty a havarijné situácie

Aby dokázala Spoločnosť správne reagovať na neželané bezpečnostné udalosti, zaviedla systém sledovania a ohlasovania bezpečnostných incidentov. Všetci zamestnanci sú poučovaní o tom, ako reagovať a koho informovať, ak zaznamenajú podozrivú aktivitu. Riešenie havarijných situácií je testované aspoň 1x ročne. Získané skúsenosti sú zapracované do havarijného plánu.

4. Hodnotenie a zlepšovanie stavu informačnej bezpečnosti

Účinnosť informačnej bezpečnosti je sledovaná zavedeným systémom monitorovania a internými auditmi. Hodnotenie informačnej bezpečnosti vykonáva vedenie spoločnosti aspoň 1x ročne.

Táto bezpečnostná politika nadobúda účinnosť dňa: 04.03.2015.

.....
Bc. Miroslav Jurečka
RKnet, s. r. o.