V politike informačnej bezpečnosti sa stanovené záväzky definujú ako záväzné povinnosti, ktoré musia dodržiavať všetci zamestnanci spoločnosti MTS, spol. s r.o., dodávatelia, externí partneri, aby zabezpečili účinnú ochranu informácií a správnu prevádzku informačných systémov. Vedenie spoločnosti MTS, spol. s r.o. sa zaviazalo implementovať požiadavky TISAXU, a tým efektívne udržiavať a neustále zlepšovať informačný systém manažérstva, v rozsahu stanovených základných pilierov:

1. Zásady informačnej bezpečnosti

- **Dôvernosť:** Informácie musia byť prístupné iba tým osobám, ktoré majú oprávnenie na ich prístup;
- **Integrita:** Informácie musia byť presné, úplné a nepoškodené;
- **Dostupnosť:** Informácie musia byť dostupné oprávneným používateľom v potrebnom čase.

2. Zodpovednosti a úlohy

- **Vedenie spoločnosti:** Zodpovedá za implementáciu politiky informačnej bezpečnosti a dohľad nad jej dodržiavaním;
- **Zamestnanci**: Musia dodržiavať pravidlá a postupy týkajúce sa bezpečnosti informácií, firemný mail je zakázane používať na súkromné účely;
- **Externí partneri, dodávatelia:** Musia podpisovať zmluvu o mlčanlivosti a ochrane informácií, ak majú prístup k firemným dátam;
- **Členovia bezpečnostného výboru:** Tento výbor je zodpovedný za strategické rozhodovanie, monitorovanie dodržiavania bezpečnostných politík a pravidiel a za zaisťovanie ochrany kritických informácií a systémov organizácie.

3. Riadenie rizík

- Spoločnosť MTS bude pravidelne vykonávať hodnotenie rizík týkajúcich sa bezpečnosti informácií;
- Na základe hodnotenia rizík budú stanovené opatrenia na zmiernenie hrozieb.

4. Kontrola a prístup

- **Autentifikácia:** Všetci používatelia musia používať silné heslá s 2-faktorovým overením prihlásenia a iné metódy autentifikácie pri prístupe k informačným systémom;
- **Prístupové práva:** Prístup k citlivým informáciám bude obmedzený na osoby s relevantnými oprávneniami;
- **Monitorovanie:** Všetky aktivity v informačných systémoch budú monitorované s cieľom identifikovať a reagovať na bezpečnostné incidenty;
- **Fyzickú bezpečnosť:** Prístup je na základe identifikačných kariet a do zabezpečených priestorov (napr. serverovne, niektorých kancelárii) je obmedzený fyzický prístup len pre poverené osoby.

Dokument je duševným vlastníctvom organizácie MTS, spol. s r.o. Bez výslovného súhlasu manažmentu nesmie byť kopírovaný a rozširovaný tretím osobám. Dokument po vytlačení stráca aktuálnosť údajov a je považovaný za neriadený výtlačok. Originál je na intranete spoločnosti.

5. Zabezpečenie IT infraštruktúry

- **Šifrovanie:** Citlivé informácie musia byť šifrované počas prenosu aj ukladania;
- **Zálohovanie:** Všetky kritické dáta budú pravidelne zálohované;
- **Antivírusová ochrana:** Všetky zariadenia a servery musia byť chránené aktualizovaným antivírusovým softvérom.

6. Školenie a vzdelávanie

- Všetci zamestnanci spoločnosti MTS budú pravidelne školení v oblasti informačnej bezpečnosti, aby pochopili hrozby a správne reagovali na bezpečnostné incidenty.

7. Reakcia na incidenty

- **Spoločnosť MTS** má zavedený postup na identifikáciu, reakciu a riešenie bezpečnostných incidentov;
- **Oznamovanie incidentov:** Všetky incidenty, ako je podozrenie na únik dát alebo pokus o útok, musia byť hlásené kombináciou telefonickej a písomnej formy, takže pre urgentnosť riešenia incidentu musí byť každý incident nahlásený na telefonicky na čísle +421 905 881 808 a mailom na: incident@mts.sk.

8. Zabezpečenie dodávateľov

- Dodávatelia, ktorí majú prístup k firemným informáciám, musia byť riadne vybraní a zaväzujú sa k dodržiavaniu bezpečnostných politík spoločnosti MTS.

9. Prehodnocovanie politiky

- Politika informačnej bezpečnosti bude pravidelne revidovaná, aby sa zabezpečila jej aktuálnosť v súlade s novými hrozbami, technológiami a právnymi predpismi.

V Krivej, dňa 21.02.2025

Schválené Generálnym riaditeľom spoločnosti MTS, spol. s r.o.

.....
Ing. Peter Laurinčík
CEO

Dokument je duševným vlastníctvom organizácie MTS, spol. s r.o. Bez výslovného súhlasu manažmentu nesmie byť kopírovaný a rozširovaný tretím osobám. Dokument po vytlačení stráca aktuálnosť údajov a je považovaný za neriadený výtlačok. Originál je na intranete spoločnosti.