

Bezpečnostná politika spoločnosti okto—digital

Spoločnosť okto—digital s.r.o. si uvedomuje dôležitosť informačných systémov, ktoré prevádzkuje, význam údajov, ktoré sú v nich spracúvané, hodnotu majetku a technológií, ktoré používa pre svoju činnosť a povinnosť chrániť oprávnené záujmy svojich zákazníkov a všetkých osôb, s ktorými prichádza do kontaktu.

Z tohto dôvodu sa spoločnosť rozhodla zaviesť a udržiavať systém manažérstva informačnej bezpečnosti v súlade s požiadavkami normy ISO/IEC 27001:2022. Spoločnosť prijala a zaväzuje sa presadzovať a dosahovať tieto strategické ciele a princípy:

1. Riadiť informačnú bezpečnosť v súlade s požiadavkami štandardov ISO/IEC 27001, ISO/IEC 27002 a platnou legislatívou SR a EÚ.
2. Prijatť a implementovať Bezpečnostnú politiku, ktorej cieľom je vytvoriť predpoklady pre zaistenie primeranej úrovne informačnej bezpečnosti vo všetkých činnostiach a funkciách spoločnosti.
3. Chrániť práva a záujmy majiteľov, zákazníkov, zamestnancov a obchodných partnerov implementovaním efektívnych a účinných bezpečnostných mechanizmov a opatrení.
4. Zvyšovať bezpečnostné povedomie zamestnancov a systematicky ich viesť a motivovať k zlepšovaniu a dodržiavaniu bezpečnostných zásad pri práci.
5. Zabezpečiť dôvernosť, dostupnosť a integritu osobných údajov, obchodného tajomstva a iných citlivých informačných aktív spoločnosti, jej zákazníkov a obchodných partnerov pri ich spracúvaní.
6. Zaisťiť bezpečnosť, spoľahlivosť a kvalitu prevádzkovaných IS využívaním moderných informačných technológií a ich postupným zlepšovaním a zefektívňovaním.
7. Vytvoriť podmienky pre bezpečné umiestnenie jednotlivých komponentov IS v závislosti na ich dôležitosti a zabezpečiť ich fyzickú ochranu a ochranu pred vplyvmi okolitého prostredia.
8. Chrániť dobré meno spoločnosti a zabezpečiť vysoký etický štandard a kvalitu poskytovaných služieb.
9. Zabezpečiť hlásenie a riešenie bezpečnostných incidentov s dôrazom na prevenciu ich opätovného výskytu.
10. Zdokonaľovať systém manažérstva informačnej bezpečnosti, trvalo zlepšovať jeho efektívnosť a integritu v súlade s novými požiadavkami na poskytovanie služieb a vytvoriť organizačné podmienky pre zaistenie bezpečnosti IS.

Bezpečnostná politika je platná v rámci celej spoločnosti. Kontrola dodržiavania bezpečnostnej politiky prebieha formou interných auditov. Nedodržanie pravidiel a zásad uvedených

v bezpečnostnej politike a prijatých bezpečnostných opatrení je posudzované ako porušenie pracovnej disciplíny.

Schválil: Štefan Gembický, 29. 02. 2024