POLITIKA INFORMAČNEJ BEZPEČNOSTI (2025 – 2027)

SKRIVANEK

VYHLÁSENIE VEDENIA SPOLOČNOSTI

Spoločnosť Skrivanek ako popredný poskytovateľ jazykových a technologických služieb vyhlasuje túto Politiku informačnej bezpečnosti ako základný pilier ochrany svojich obchodných operácií a zachovania dôvery zainteresovaných strán.
Vďaka zavedeniu a neustálemu rozvoju nášho Systému riadenia bezpečnosti informácií (ISMS), ktorý je v súlade s normou ISO/IEC 27001:2022, sa zaväzujeme:

- chrániť našu spoločnosť pred novovznikajúcimi hrozbami, vrátane kybernetickej kriminality, rizík spojených s umelou inteligenciou a zneužitím dát,
- zabezpečovať súlad s platnými medzinárodnými a miestnymi predpismi a proaktívne reagovať na legislatívne zmeny,
- presadzovať kultúru, v ktorej je bezpečnosť prioritou, na všetkých úrovniach organizácie,
- poskytovať potrebné zdroje, vedenie a strategický dohľad na naplnenie tejto politiky, jej pravidelné vyhodnocovanie a zosúladenie s globálnymi overenými postupmi.

CIELE POLITIKY BEZPEČNOSTI

1. Posilňovať opatrenia zamerané na nové kybernetické hrozby vrátane ransomvéru, phishingu a útokov riadených umelou inteligenciou.
2. Dosiahnuť väčší súlad s globálnymi i regionálnymi predpismi o ochrane údajov (napr. GDPR, CCPA a nové miestne požiadavky).
3. Neustále zdokonaľovať postupy hodnotenia rizík a reakcie na incidenty podľa overených postupov v oblasti bezpečnosti informácií.
4. Šíriť kultúru informovanosti o bezpečnosti medzi zamestnancami, dodávateľmi a partnermi.

ZÁKLADNÉ PRINCÍPY

Naše záväzky:

- Dodržiavať a presadzovať legislatívu v oblasti informačnej bezpečnosti vo všetkých krajinách, kde pôsobí naša spoločnosť.
- Zabezpečiť dostupnosť informácií v požadovanom čase a mieste pre obchodné operácie, pričom prístup bude obmedzený podľa zásady **najnižšej potrebnej úrovne oprávnení (least privilege)**.
- Správne klasifikovať informácie a nakladať s nimi podľa ich citlivosti (verejné, interné, dôverné, osobné) spolu s prísnymi kontrolami prístupu na všetkých úrovniach.
- Posilniť riadenie prístupu zavedením **viacfaktorového overovania (MFA)** a **riadenia prístupu na základe rolí (RBAC)** s cieľom minimalizovať riziká neoprávneného prístupu.
- Spravovať integritu a životný cyklus informácií – od ich vzniku, cez prenos, až po bezpečnú likvidáciu – v súlade s medzinárodnými normami.
- Zabezpečovať pravidelné školenia a zaviesť povinné každoročné vzdelávacie programy prispôsobené pracovným rolám, zamerané na nové hrozby a bezpečné nakladanie s dátami, aby boli všetci v organizácii dobre informovaní a pripravení na riziká.
- Považovať porušenie pravidiel informačnej bezpečnosti za závažné porušenie interných predpisov a zmluvných záväzkov.
- Určovať bezpečnostné opatrenia na základe závažnosti rizík, ich dopadov a nákladovej efektívnosti, aby bola ochrana **primeraná a flexibilná**.
- Pravidelne monitorovať riziká, prehodnocovať hrozby a implementovať **nápravné a preventívne opatrenia** pre neustále zlepšovanie ISMS.
- Rozšíriť schopnosti reakcie na bezpečnostné incidenty, vrátane detekcie v reálnom čase, hlásenia a rýchlych opatrení na zmiernenie dopadov a minimalizáciu prestojov.
- Integrovať systémy založené na **umelej inteligencii** pre detekciu hrozieb a reakcie na ne, aby bolo možné rýchlejšie zistiť narušenie, zmierniť jeho dopady a zároveň zvýšiť celkovú odolnosť infraštruktúry informačnej bezpečnosti.

Vydal: Anna Julie Skřivánková, 10. 4. 2025