BEZPEČNOSTNÁ
POLITIKA INFORMÁCIÍ

CIELE BEZPEČNOSTNEJ POLITIKY

Naším prvoradým cieľom je postarať sa o dôvernosť, integritu a dostupnosť všetkých vlastných a zákazníckych údajov pre bezproblémové zaistenie našich podnikateľských aktivít. Touto politikou deklarujeme všetkým obchodným partnerom, zamestnancom, verejnej a štátnej správe, ako aj širokej verejnosti schopnosť celého Skrivanek Holding SE efektívne chrániť informácie, hmotný i nehmotný majetok vlastný aj nám zverený v súlade s legislatívnymi požiadavkami vo všetkých krajinách, kde pôsobíme a našimi bezpečnostnými predpismi.

ZÁSADY A PRINCÍPY BEZPEČNOSTI INFORMÁCIÍ 1/3

Zaväzujeme sa:

Dodržiavať a napĺňať legislatívne predpisy pre oblasť bezpečnosti informácií vo všetkých krajinách, kde naša skupina pôsobí.

Zaisťovať dostupnosť informácií v čase a mieste podľa potrieb spoločnosti, ale len tým, ktorí ich potrebujú pre svoju pracovnú činnosť. Tým je zachovávaná dôvernosť informácií na základe stanovených kategórií - verejné, interné, dôverné, osobné.

SKRIVANEK

PREHLÁSENIE MANAŽMENTU

Skrivanek je popredný poskytovateľ jazykových služieb v oblasti prekladov a tlmočenia vrátane lokalizácie a DTP služieb a jazykovej výučby v Slovenskej republike a v ďalších 13 krajinách na celom svete.

Vedenie spoločnosti Skrivanek Holding SE vyhlasuje túto Bezpečnostnú politiku informácií ako rámec pre smerovanie spoločnosti na poli ochrany bezpečnosti informácií. Zámerom vedenia je podporovať vytýčené ciele a princípy tejto politiky.

ZÁSADY A PRINCÍPY BEZPEČNOSTI INFORMÁCIÍ 2/3

Zaväzujeme sa tiež:

Riadiť integritu a životný cyklus informácií od okamihu ich vzniku cez odovzdávanie a užívanie až po ich likvidáciu.

Vzdelávať a rozvíjať našich zamestnancov, dodávateľov a partnerov v oblasti bezpečnosti informácií.

Porušenie pravidiel informačnej bezpečnosti je považované za hrubé porušenie interných predpisov a zmluvných vzťahov.

CERTIFIKÁCIA BEZPEČNOSTNEJ POLITIKY

Na presadzovanie politiky je v spoločnosti zavedený a rozvíjaný systém manažmentu bezpečnosti informácií podľa ISO/IEC 27001:2013. Táto medzinárodná norma pre systémy riadenia bezpečnosti informácií zaisťuje ochranu proti potenciálnym bezpečnostným hrozbám, ako sú napr. kybernetické zločiny, zneužitie osobných údajov, vandalizmus/terorizmus, požiar/poškodenie, zneužitie a krádež údajov, vírusový útok.

TÜV NORD
TÜV NORD CERT GmbH
ISO 27001

ZÁSADY A PRINCÍPY BEZPEČNOSTI INFORMÁCIÍ 3/3

Ďalej sa zaväzujeme:

Stanovovať prijaté bezpečnostné opatrenia podľa princípu posúdenia závažnosti vyhodnotených rizík, ich dopadov a ekonomickej náročnosti opatrení.

Pravidelným monitorovaním, prehodnocovaním rizík, riadením bezpečnostných udalostí a incidentov pomocou nápravných a preventívnych opatrení zvyšovať účinnosť nášho systému manažmentu bezpečnosti informácií.

2020 - **2024**