BEZPEČNOSTNÍ
POLITIKA INFORMACÍ

CÍLE BEZPEČNOSTNÍ POLITIKY

Naším prvořadým cílem je postarat se o důvěrnost, integritu a dostupnost všech vlastních a zákaznických dat pro bezproblémové zajištění našich podnikatelských aktivit. Touto politikou deklarujeme všem obchodním partnerům, zaměstnancům, veřejné a státní správě i široké veřejnosti schopnost celé Skřivánek Holding SE efektivně chránit informace, hmotný i nehmotný majetek vlastní i nám svěřený v souladu s legislativními požadavky ve všech zemích, kde působíme, a našimi bezpečnostními předpisy.

ZÁSADY A PRINCIPY BEZPEČNOSTI INFORMACÍ 1/3

Zavazujeme se:

dodržovat a naplňovat legislativní předpisy pro oblast bezpečnosti informací ve všech zemích, kde naše skupina působí,

zajišťovat dostupnost informací v čase a místě podle potřeb společnosti, ale pouze těm, kteří je potřebují pro svoji pracovní činnost. Tím je zachovávána důvěrnost informací na základě stanovených kategorií – veřejné, interní, důvěrné, osobní.

SKŘIVÁNEK

PROHLÁŠENÍ MANAGEMENTU

Skřivánek je přední poskytovatel jazykových služeb v oblasti překladů a tlumočení, včetně lokalizace a DTP služeb, a jazykové výuky v České republice a v dalších 13 zemích po celém světě.

Vedení společnosti Skřivánek Holding SE vyhlašuje tuto Bezpečnostní politiku informací jako rámec pro směřování společnosti na poli ochrany bezpečnosti informací. Záměrem vedení je podporovat vytyčené cíle a principy této politiky.

ZÁSADY A PRINCIPY BEZPEČNOSTI INFORMACÍ 2/3

Zavazujeme se také:

Řídit integritu a životní cyklus informací od okamžiku jejich vzniku, přes předávání a užívání až po likvidaci,

vzdělávat a rozvíjet naše zaměstnance, dodavatele a partnery v oblasti bezpečnosti informací.

Porušení pravidel informační bezpečnosti je považováno za hrubé porušení interních předpisů a smluvních vztahů.

CERTIFIKACE BEZPEČNOSTNÍ POLITIKY

K prosazování politiky je ve společnosti zaveden a rozvíjen systém managementu bezpečnosti informací podle ISO/IEC 27001:2013. Tato mezinárodní norma pro systémy řízení bezpečnosti informací zajišťuje ochranu proti potenciálním bezpečnostním hrozbám, jakými jsou např. kybernetické zločiny, zneužití osobních údajů, vandalismus / terorismus, požár / poškození, zneužití a krádež dat, virový útok.

TÜV NORD
TÜV NORD CERT GmbH
ISO 27001

ZÁSADY A PRINCIPY BEZPEČNOSTI INFORMACÍ 3/3

Dále se zavazujeme:

přijímaná bezpečnostní opatření stanovovat na principu posouzení závažnosti vyhodnocených rizik, jejich dopadů a ekonomické náročnosti opatření,

pravidelným monitorováním, přehodnocováním rizik, řízením bezpečnostních událostí a incidentů prostřednictvím nápravných a preventivních opatření zvyšovat účinnost našeho systému managementu bezpečnosti informací.

2020 - **2024**