POLITIKA INFORMAČNÍ BEZPEČNOSTI (2025 –2027)

skrivanek

PROHLÁŠENÍ VEDENÍ SPOLEČNOSTI

Společnost Skřivánek jako přední poskytovatel jazykových a technologických služeb vyhlašuje tuto Politiku informační bezpečnosti jako základní pilíř ochrany svých obchodních operací a zachování důvěry zúčastněných stran.

Díky zavedení a neustálému rozvoji našeho Systému řízení bezpečnosti informací (ISMS), který je v souladu s normou **ISO/IEC 27001:2022**, se zavazujeme:

- chránit naši společnost proti nově vznikajícím hrozbám, včetně kybernetické kriminality, rizik spojených s umělou inteligencí a zneužitím dat,
- zajišťovat soulad s platnými mezinárodními a místními předpisy a proaktivně reagovat na legislativní změny,
- prosazovat kulturu, v níž je bezpečnost prioritou, na všech úrovních organizace,
- poskytovat potřebné zdroje, vedení a strategický dohled k naplnění této politiky, jejímu pravidelnému vyhodnocování a sladění s globálními osvědčenými postupy.

CÍLE POLITIKY BEZPEČNOSTI

1. Posilovat opatření zaměřená na nové kybernetické hrozby včetně ransomwaru, phishingua útoků řízených umělou inteligencí.
2. Dosáhnout většího souladu s globálními i regionálními předpisy o ochraně údajů (např. GDPR, CCPA a nové místní požadavky).
3. Soustavně zdokonalovat postupy hodnocení rizik a reakce na incidenty podle osvědčených postupů v oblasti bezpečnosti informací.
4. Šířit kulturu informovanosti ohledně bezpečnosti mezi zaměstnanci, dodavateli i partnery.

PROHLÁŠENÍ VEDENÍ SPOLEČNOSTI

Naše závazky:

- **Dodržovat a prosazovat legislativu v oblasti informační bezpečnostive všech zemích**, kde působí naše společnost.
- **Zajistit dostupnost informací** v požadovaném čase a místě pro obchodní operace, přičemž přístup bude omezen podle zásady **nejnižší nutné úrovně oprávnění** (least privilege).
- Správně klasifikovat informace a nakládat s nimi na základě jejich citlivosti (veřejné, interní, důvěrné, osobní) společně s přísnými kontrolami přístupu na všech úrovních.
- **Posílit řízení přístupu** zavedením **vícefaktorového ověřování (MFA) a řízení přístupu na základě rolí (RBAC)** za účelem minimalizace rizik neoprávněného přístupu.
- **Spravovat integritu a životní cyklus** informací–od jejich vzniku, přes přenos, až po bezpečnou likvidaci –v souladu s mezinárodními normami.
- **Zajišťovat pravidelná školenía zavést povinné každoroční vzdělávací programy** přizpůsobené pracovním rolím, zaměřené na nové hrozby a bezpečné nakládání s daty, aby byli všichni v naší organizaci dobře informováni a připraveni na rizika.
- **Považovat porušení pravidel informační bezpečnosti za závažné porušení interních předpisů a smluvních závazků.**
- **Určovat bezpečnostní opatření na základě závažnosti rizik, jejich dopadů a nákladové efektivity**, aby byla ochrana přiměřenáaflexibilní.
- **Pravidelně monitorovat rizika, přehodnocovat hrozby a implementovat nápravná a preventivní opatření** k neustálému zlepšování ISMS.
- **Rozšířit schopnosti reakce na bezpečnostní incidenty, včetně detekce v reálném čase, hlášení a rychlých opatření** ke zmírnění dopadů a minimalizaci prostojů.
- Integrovat systémy založené na umělé inteligenci pro detekci hrozebareakce na ně, aby bylo možno rychleji zjistit narušení a zmírnit jeho dopady a současně zvýšit celkovou odolnost naší infrastruktury bezpečnosti informací.

Vydal: Anna Julie Skřivánková, 10. 4. 2025