POLITIKA SYSTÉMU ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI (ISMS)

Prohlášení vedení společnosti

Vedení společnosti G – DATA servis, spol. s r.o. si plně uvědomuje, že informace a datová infrastruktura představují jeden z klíčových pilířů jejího podnikání a důvěry zákazníků. Proto se zavazuje vytvářet, udržovat a neustále zlepšovat Systém řízení informační bezpečnosti (ISMS) podle mezinárodní normy ČSN EN ISO/IEC 27001.

Cílem je chránit informace zpracovávané společností před jakýmkoliv ohrožením, ať již úmyslným nebo neúmyslným, zajistit důvěrnost, integritu a dostupnost informací a současně zachovat přiměřenou míru efektivity a hospodárnosti.

Tato politika vyjadřuje závazek vedení společnosti k odpovědnému nakládání s informacemi, k plnění všech legislativních, smluvních a regulačních požadavků a k rozvoji bezpečnostního povědomí všech zaměstnanců i spolupracovníků.

Společnost působí v oblasti informačních technologií a poskytuje služby včetně správy IT infrastruktury, cloudových a síťových řešení, podpory uživatelů a instalace bezpečnostních systémů. Při těchto činnostech klade důraz na kvalitu a spolehlivost poskytovaných služeb, ochranu informací zákazníků a dlouhodobou důvěru klientů.

Vedení společnosti zajišťuje potřebné zdroje, podporu a kompetence k naplnění požadavků této politiky a k udržování účinného systému řízení informační bezpečnosti a kvality.

A. Východiska a principy informační bezpečnosti

1. Informace jsou pro společnost jedním z nejcennějších aktiv. Jsou uchovávány nejen v informačních systémech a dokumentech, ale i ve znalostech a zkušenostech zaměstnanců – jejich ochranu proto chápeme komplexně, technicky, organizačně i personálně.
2. Informační bezpečnost chápeme jako součást firemní kultury a každodenní praxe. Každý zaměstnanec nese odpovědnost za bezpečné nakládání s informacemi a aktivně přispívá k jejich ochraně.
3. Ochrana informací se týká nejen interních dat společnosti, ale i údajů zákazníků, partnerů a dodavatelů, které jsou nám svěřeny.
4. Informační bezpečnost řešíme v úzké souvislosti s ochranou osobních údajů (GDPR) a s požadavky dalších souvisejících právních předpisů.

B. Kybernetická bezpečnost a řízení rizik

1. Společnost chápe kybernetickou bezpečnost jako nedílnou součást ISMS. Otázka nezní, zda útoky přijdou, ale jak často a s jakými dopady — proto usilujeme o minimalizaci pravděpodobnosti incidentu a zmírnění jeho následků.
2. Vycházíme z principů řízení rizik podle ČSN EN ISO/IEC 27005. Nebezpečí spojená s provozem informačních technologií jsou pravidelně analyzována a přehodnocována, přičemž přijatá opatření odpovídají míře rizika i ekonomické přiměřenosti.
3. Inspirujeme se v platné i připravované legislativě kybernetické bezpečnosti, zejména ve směrnici NIS 2 a českém zákoně o kybernetické bezpečnosti a navazujících vyhláškách.
4. Ověřování a zlepšování systému probíhá průběžně prostřednictvím interních auditů, přezkoumání vedením a externích kontrol podle normy ISO 19011.
5. Při zabezpečení IT prostředků využíváme moderní technické prostředky, osvědčené postupy a osobní zkušenosti odborníků.
6. U každého opatření zvažujeme poměr mezi přínosem a náklady. Uplatňujeme princip „rozumné dostatečnosti“ – chápeme, že není možné zcela eliminovat všechna rizika, ale vyvažujeme míru bezpečnosti s potřebami firmy, zákazníků a efektivitou nákladů.

7. Při poskytování služeb zákazníkům jsou zásady informační bezpečnosti uplatňovány i v procesech správy IT infrastruktury, vzdáleného přístupu, zálohování a údržby systémů, aby byla zajištěna ochrana informací klientů i interních dat společnosti.

C. Zaměstnanci, povědomí a odpovědnost

1. Člověk je nejdůležitějším, ale zároveň i nejzranitelnějším prvkem systému.
2. Zaměstnanci jsou pravidelně, cíleně a opakovaně školeni a informováni o zásadách bezpečnosti informací, svých povinnostech a postupech při vzniku bezpečnostních incidentů, aby byli schopni účinně předcházet hrozbám a přispívali k celkové úrovni bezpečnosti společnosti.
3. Zaměstnanci přistupují ke své práci zodpovědně z hlediska bezpečnosti informací, kvality poskytovaných služeb a péče o zákazníky a aktivně upozorňují na zjištěné nebo podezřelé bezpečnostní události.
4. Společnost podporuje otevřenou komunikaci o bezpečnostních tématech, aby se prevence stala přirozenou součástí firemní kultury.
5. Každý zaměstnanec je veden k odpovědnému chování a vědomí, že bezpečnost začíná u jednotlivce.

D. Závazek vedení a přezkoumání politiky

Tato politika je závazkem vedení společnosti G – DATA servis, spol. s r.o., že bude:

- uplatňovat zásady a požadavky systému řízení informační bezpečnosti podle ČSN EN ISO/IEC 27001,
- zajišťovat jejich plnění všemi zaměstnanci i spolupracujícími subjekty,
- respektovat veškeré právní a smluvní požadavky České republiky a Evropské unie,
- průběžně zlepšovat účinnost systému řízení a podporovat bezpečnostní i kvalitativní povědomí napříč firmou,
- přezkoumávat politiku společně pro systém řízení informační bezpečnosti a kvality nejméně jednou ročně nebo při významných změnách.

Politika ISMS je základem pro stanovování cílů v oblasti bezpečnosti informací a kvality.

Je zveřejněna všem zaměstnancům a partnerům a je dostupná i veřejnosti na webových stránkách společnosti.

V Praze dne 1. 9. 2025
Peter Dobiáš
ředitel společnosti