POLITIKA KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

1. PROHLÁŠENÍ VEDENÍ

Vedení společností ABRA Software a.s. a ABRA Software s.r.o. si uvědomuje, že informace, zákaznická data, zdrojové kódy, obchodní know-how a digitální infrastruktura představují zásadní hodnotu a klíčový předpoklad dlouhodobé stability, důvěryhodnosti a konkurenceschopnosti obou společností.

Ochrana informací a zajištění bezpečného a spolehlivého fungování informačních systémů jsou proto nedílnou součástí strategického řízení společností. Kybernetická a informační bezpečnost je chápána jako integrální součást řízení rizik, kvality poskytovaných služeb a odpovědnosti vůči zákazníkům, zaměstnancům, obchodním partnerům i příslušným orgánům veřejné správy.

Za účelem systematického řízení této oblasti společnosti zavádějí, udržují a rozvíjejí systém řízení kybernetické a informační bezpečnosti (Cyber and Information Security Management System – CISMS) jako jednotný a konzistentní rámec řízení napříč oběma právními entitami.

2. ZÁSADY ŘÍZENÍ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI

Systém řízení kybernetické a informační bezpečnosti vychází z principu ochrany důvěrnosti, integrity a dostupnosti informací a z principu přiměřeného a systematického řízení rizik. Bezpečnostní opatření jsou navrhována a implementována na základě identifikace a vyhodnocení rizik s ohledem na význam informačních aktiv, charakter poskytovaných služeb a regulatorní prostředí České republiky a Slovenské republiky.

Informace jsou chráněny bez ohledu na jejich formu či nosič, ať již jsou zpracovávány v informačních systémech, cloudových prostředích, dokumentech, databázích nebo představují znalosti a zkušenosti zaměstnanců. Zvláštní pozornost je věnována ochraně zákaznických dat, osobních údajů, zdrojových kódů a dalších citlivých informací, které mají zásadní význam pro podnikání společností.

Bezpečnost je integrována do procesů vývoje, provozu a poskytování softwarových produktů a služeb. Součástí řízení je rovněž zajištění kontinuity činností, schopnost včasné detekce a řešení bezpečnostních událostí a systematické posilování odolnosti vůči kybernetickým hrozbám.

CISMS je budován a provozován v souladu s požadavky normy ISO/IEC 27001:2022 a současně podporuje plnění právních, regulatorních a smluvních požadavků v oblasti kybernetické bezpečnosti a ochrany osobních údajů vyplývajících z právních předpisů České republiky, Slovenské republiky a přímo použitelných právních aktů Evropské unie. Jednotný rámec řízení umožňuje konzistentní a systematický přístup k bezpečnosti napříč oběma společnostmi a zajišťuje jejich připravenost reagovat na budoucí legislativní změny.

3. LIDÉ, ODPOVĚDNOST A KULTURA BEZPEČNOSTI

Úroveň kybernetické a informační bezpečnosti je dána nejen technickými a organizačními opatřeními, ale především odpovědným přístupem zaměstnanců. Každý zaměstnanec je povinen nakládat s informacemi v souladu s touto politikou a souvisejícími interními předpisy a přispívat k ochraně informačních aktiv v rozsahu své role.

Odpovědnosti za řízení kybernetické a informační bezpečnosti jsou jasně vymezeny a integrovány do řídicích a rozhodovacích procesů na všech úrovních řízení. Společnosti zajišťují, aby tato politika byla přiměřeným způsobem komunikována zaměstnancům a aby jí zaměstnanci rozuměli v kontextu své pracovní činnosti. Politika je současně dostupná relevantním zainteresovaným stranám v rozsahu odpovídajícím jejich roli a vztahu ke společnostem.

Společnosti podporují systematické vzdělávání, rozvoj bezpečnostního povědomí a otevřenou komunikaci o bezpečnostních tématech, včetně včasného hlášení bezpečnostních událostí a incidentů, a vytvářejí prostředí, ve kterém je bezpečnost přirozenou součástí každodenního rozhodování.

4. ZÁVAZEK VEDENÍ A NEUSTÁLÉ ZLEPŠOVÁNÍ

Vedení společností se zavazuje vytvářet podmínky pro efektivní fungování CISMS, poskytovat odpovídající zdroje pro jeho provoz a rozvoj a pravidelně hodnotit jeho výkonnost a přiměřenost. Součástí tohoto závazku je stanovování bezpečnostních cílů, jejich vyhodnocování a podpora neustálého zlepšování systému v návaznosti na vývoj hrozeb, technologického prostředí i podnikatelských aktivit společností.

Tato politika je závazná pro všechny zaměstnance a osoby jednající jménem společností ABRA Software a.s. a ABRA Software s.r.o. a tvoří základní rámec pro stanovování bezpečnostních cílů, bezpečnostní strategie a navazujících interních předpisů.

V Praze, dne 9. 3. 2026

Za ABRA Software a.s.

Petr Havelka

ABRA Software a.s.
Digitální podpis
23.03.2026 15:44:49

Za ABRA Software s.r.o.

David Rožek

ABRA Software s.r.o.
Digitální podpis
23.03.2026 17:06:46