
Politika informační bezpečnosti (ISMS)

Verze: 1.0

Datum revize: 20. 01. 2026

Vlastník: Fleet Manager / Vedení společnosti

---

1. Účel

Účelem této politiky je zajistit ochranu telemetrických dat, integrity firmwaru telemetrických jednotek a dostupnosti backendové infrastruktury. Vzhledem k našemu zaměření na monitoring vozového parku (lokomotiv) je prioritou prevence neautorizovaného přístupu k jednotkám a zajištění kontinuity služeb (SLA) pro naše zákazníky.

Tento dokument je **hlavním nadřazeným dokumentem** celého systému řízení bezpečnosti informací (ISMS). Všechny ostatní směrnice, procesy a politiky jsou mu podřízeny a rozvádějí jeho principy do detailů.

2. Rozsah působnosti

Tato politika je závazná pro všechny zaměstnance, externí dodavatele a zákazníky přistupující k našim systémům:

- **Aktivum DEV:** Telemetrické jednotky a jejich nastavení.
- **Aktivum FW/API:** Firmware jednotek a rozhraní pro přenos dat.
- **Aktivum SYS/NET:** Backendová infrastruktura, VPN přístupy a SIM konektivita.
- **Aktivum DAT/USR:** Data z provozu a uživatelské účty.

3. Bezpečnostní opatření (Reakce na rizika)

3.1. Bezpečnost telemetrických zařízení a sítí

(Reakce na RISK-DEV-01, NET-01)

- **Privátní spojení:** Pro komunikaci s jednotkami musí být využívána výhradně privátní APN/VPN. Vzdálený přístup k nastavení jednotek přes veřejný internet je zakázán.
- **Autentizace:** Jsou zakázána výchozí hesla. Každá jednotka musí mít unikátní a silné přístupové údaje.
- **SIM karty:** SIM karty musí být v jednotkách fyzicky zabezpečeny. Provoz na SIM kartách je monitorován a omezen pouze na nezbytný datový tarif (prevence zneužití při krádeži).

3.2. Integrita firmwaru a softwaru

(Reakce na RISK-FW-01)

- **Digitální podepisování (Code Signing):** Každý firmware (např. LOKO01) musí být před distribucí digitálně podepsán vývojářem. Jednotka nesmí přijmout ani nainstalovat binární soubor, jehož integrita nebyla ověřena veřejným klíčem.

3.3. Řízení přístupu a API

(Reakce na RISK-API-01, API-02, NET-03)

- **Autorizace (BOLA):** API musí při každém volání ověřovat nejen identitu uživatele, ale i jeho oprávnění k danému objektu (např. ID lokomotivy). Zákazník A nesmí mít přístup k datům Zákazníka B.
- **Vícefaktorové ověřování (MFA):** Pro všechny administrátorské přístupy přes VPN a pro správu zákaznických účtů je povinné zavedení MFA.
- **Správa relací:** Webové aplikace musí implementovat automatické odhlášení po 15 minutách neaktivity a zabezpečené příznaky (Secure/HTTPOnly) pro cookies.

3.4. Zálohování a obnova dat

(Reakce na RISK-DAT-01, BACK-02)

- **Strategie záloh:** Musí být definovány parametry RPO (bod obnovy) a RTO (doba obnovy).
- **Imutabilní zálohy:** Kromě real-time replikace (Hot Standby) musí být prováděny denní "studené" zálohy (snapshots), které jsou chráněny proti okamžitému přepisu logickou chybou nebo ransomwarem.

3.5. Správa uživatelů a "Ghost Users"

(Reakce na RISK-USR-02)

- **Revize přístupů:** Kvartálně probíhá revize aktivních uživatelských účtů.
- **Smluvní povinnost:** Zákazníci jsou povinni nahlásit odchod své pověřené osoby do 24 hodin pro okamžitou deaktivaci účtu.

4. Monitoring a řešení incidentů

(Reakce na RISK-IRM-01, VULN-01, IRM-02)

- **Centralizované logování:** Veškeré přístupy k API a administrátorské zásahy jsou logovány do centrálního systému (SIEM/ELK). Logy musí obsahovat informaci o tom, ke kterému konkrétnímu aktivu (lokomotivě) bylo přistupováno.

- **Vulnerability Management:** Pravidelně (min. měsíčně) probíhá skenování zranitelností API a backendu. Kritické chyby musí být odstraněny do 48 hodin.
- **Incident Response:** Společnost udržuje aktuální kontaktní matici (včetně kontaktů na ÚOOÚ a NÚKIB) pro případ kybernetického útoku nebo úniku dat.

5. Odpovědnosti

Role	Odpovědnost
Fleet Manager	Odpovídá za schválení této politiky a alokaci zdrojů pro nápravná opatření v registru rizik.
IT / Vývoj	Odpovídají za technickou implementaci (Code Signing, VPN, MFA, API autorizace).
Zaměstnanci	Odpovídají za dodržování politiky silných hesel a hlášení podezřelých aktivit.

6. Sankce

Porušení této politiky je považováno za porušení pracovních povinností a může vést k disciplinárnímu řízení, v závažných případech až k ukončení pracovního poměru nebo smluvního vztahu.