
Směrnice bezpečnosti provozu (Operations Security Directive)

Verze: 1.0

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / IT Administrátor

Vazba na ISO/IEC 27001:2022:

- A.8.1 – Provozní postupy a odpovědnosti
- A.7.4 – Fyzické monitorování bezpečnosti
- A.8.20–A.8.22 – Síťová bezpečnost (doplněno implicitně)

---

1. Účel

Účelem této směrnice je stanovit provozní bezpečnostní pravidla pro telemetrické jednotky, síťovou komunikaci a backendovou infrastrukturu s cílem zajistit dostupnost, integritu a důvěrnost telemetrických dat.

2. Fyzická bezpečnost telemetrických jednotek

(Reakce na RISK-DEV-02, RISK-NET-01) S ohledem na provoz zařízení v mobilním prostředí platí následující pravidla:

- **Zabezpečení instalace:** Telemetrické jednotky (DEV-01) jsou instalovány v uzamykatelných rozvaděčích lokomotivy nebo na místech s omezeným fyzickým přístupem.
- **Ochrana SIM karet:** SIM karty jsou umístěny uvnitř jednotek a mechanicky zajištěny proti neoprávněnému vyjmutí.
- **Detekce manipulace:** Systém generuje alarm při ztrátě napájení, odpojení jednotky nebo dlouhodobé ztrátě konektivity, což může indikovat neoprávněný zásah.

3. Síťová bezpečnost a komunikace

(Reakce na RISK-DEV-01)

- **Izolace komunikace:** Komunikace mezi jednotkami a backendem probíhá výhradně přes privátní APN nebo jiný izolovaný komunikační kanál. Management rozhraní jednotek nesmí být dostupné z veřejného internetu.

- **Monitoring konektivity:** Dostupnost jednotek je monitorována kontinuálně. Výpadek více než 5 % aktivní flotily je klasifikován jako bezpečnostní událost a řešen dle Směrnice pro řešení bezpečnostních incidentů.
- **Správa certifikátů:** IT Administrátor vede evidenci TLS certifikátů a zajišťuje jejich obnovu nejpozději 30 dní před expirací.

4. Řízení změn v provozu

(Vazba na A.8.31 – Správa změn)

- **Testování změn:** Veškeré změny konfigurace backendu, sítě nebo firmware jsou před nasazením ověřeny v testovacím prostředí.
- **Evidence změn:** Zásahy do produkčního prostředí (např. aktualizace firmware FW-01, změny konfigurace) jsou dokumentovány v provozním deníku nebo ticketovacím systému.

5. Údržba a provozní revize

- **Fyzická kontrola zařízení:** V rámci pravidelných technických revizí lokomotiv je kontrolována neporušenost jednotek, kabeláže a upevnění zařízení.
- **Revize logů:** IT Administrátor provádí minimálně kvartální revizi provozních a přístupových logů backendu za účelem identifikace anomálií, které nebyly zachyceny automatickým monitoringem.

6. Odpovědnosti

- **System Specialist / Údržba:** Odpovídají za fyzickou instalaci, integritu a základní kontrolu telemetrických jednotek.
- **IT Administrátor:** Odpovídá za provoz backendu, síťovou bezpečnost, správu certifikátů a dohledové systémy.
- **Fleet Manager:** Odpovídá za koordinaci provozu, schvalování změn s dopadem na služby a eskalaci incidentů.

7. Auditní důkazy

Pro účely interních a externích auditů jsou evidovány:

- Provozní deníky a záznamy o změnách v infrastruktuře.
- Protokoly o instalaci a zabezpečení jednotek.
- Monitoring reporty dostupnosti a konektivity flotily.