
Směrnice pro řešení bezpečnostních incidentů

Verze: 1.0

Platnost od: 20. 01. 2026

Schválil: Fleet Manager / Vedení

---

1. Účel

Tato směrnice stanovuje závazný postup pro identifikaci, hlášení a řešení událostí, které mohou ohrozit telemetrická data, integritu firmwaru telemetrických jednotek nebo dostupnost služeb monitoringu vozového parku.

Cílem je zajistit rychlou reakci, minimalizaci škod a soulad s právními a regulatorními požadavky (např. GDPR, zákon o kybernetické bezpečnosti).

2. Klasifikace incidentů

Pro rychlou eskalaci se incidenty dělí do tří úrovní:

Úroveň	Popis	Příklad z risk register
Nízká	Událost bez dopadu na data zákazníků nebo provoz	Krádež SIM karty bez zneužití dat (RISK-NET-01)
Střední	Částečný výpadek služeb nebo podezření na pokus o útok	Expirace SSL certifikátu, opakované neúspěšné VPN pokusy (RISK-NET-02 / RISK-NET-03)
Vysoká	Únik dat, převzetí kontroly nad jednotkou, ransomware	Únik API klíčů, neautorizovaná změna FW, BOLA zranitelnost (RISK-API-01 / RISK-FW-01 / RISK-API-02)

3. Postup řešení incidentu (6 kroků)

Krok 1: Detekce a hlášení

- **Zdroje:** Automatizovaný monitoring (ELK/SIEM), hlášení od zákazníka, upozornění od etického hackera.

- **Akce:** Každý zaměstnanec nebo dodavatel, který zaznamená anomálii (např. hromadné odpojování jednotek), okamžitě informuje Technický dohled.
- **Eskalační linka 24/7:** Pro hlášení kritických incidentů (úroveň Vysoká) mimo pracovní dobu je zřízena pohotovostní linka: **+420 XXX XXX XXX**.

Krok 2: Analýza a potvrzení

- **Cíl:** Rozlišit technickou závadu od bezpečnostního incidentu.
- **Akce:** Technický dohled ověří logy (viz RISK-IRM-02) a klasifikuje incident podle výše uvedených úrovní.

Krok 3: Zadržení (Containment)

- **Cíl:** Zabránit dalšímu šíření škody.
- **Příklady:** Odpojení kompromitované VPN, rotace API klíčů, dočasné zablokování přístupu konkrétního uživatele.

Krok 4: Odstranění a obnova

- **Akce:**
    - Obnova dat ze „studené zálohy“ v případě logického poškození (RISK-BACK-02).
    - Nasazení opraveného firmwaru s digitálním podpisem (RISK-FW-01).
    - Ověření funkčnosti systému po zásahu.

Krok 5: Ohlašovací povinnost

Zákonné požadavky při vysokých incidentech:

- **ÚOOÚ:** Hlášení úniku osobních údajů do 72 hodin (např. vlastníci vozů, řidiči).
- **NÚKIB:** Hlášení významného kybernetického incidentu.
- **Zákazníci:** Informování dotčených zákazníků o rozsahu incidentu.

Krok 6: Poučení z incidentu

- **Akce:** Do 7 dnů po vyřešení incidentu tým provede Root Cause Analysis (RCA).
- **Výsledek:** Zapsán do Registru rizik jako nové riziko nebo aktualizace stávajícího.

4. Kontaktní matice

Role	Odpovědnost	Kontakt
Technický dohled	Prvotní analýza logů, containment incidentu	admin@telemetrie-firma.cz
Fleet Manager	Krizové řízení, komunikace se zákazníky	manager@telemetrie-firma.cz
Externí IT (Backend)	Obnova serverů, kontrola SLA dodavatele	support@gxtdm.eu
Krizová linka 24/7	Hlášení kritických incidentů mimo prac. dobu	+420 XXX XXX XXX
Úřad (ÚOOÚ)	Hlášení úniku dat (GDPR)	posta@uoou.cz / Datová schránka
NÚKIB	Hlášení kybernetického útoku	cert@nukib.cz

5. Auditní důkaz a reporting

Pro účely shody s ISO 27001 (zejména články 9.1 Monitorování a 10.2 Neshody a nápravná opatření) organizace povinně udržuje následující záznamy:

- **Kniha incidentů:** Centrální registr všech událostí. Každý záznam musí obsahovat:
    - Čas detekce a čas nahlášení.
    - Časovou osu (Auditní stopu): Chronologický záznam každého kroku v procesu hlášení a řešení (kdo, kdy a co udělal – interně i externě).
    - Způsob vyřešení a konečnou klasifikaci.
- **Interní „Incident Flash Report“:** Dokument sloužící k okamžitému informování Fleet Managera a vedení společnosti u incidentů úrovně „Vysoká“.

Poznámka: Tento report musí být odeslán a potvrzen vedením před jakýmkoliv ohlášením incidentu externím orgánům (ÚOOÚ, NÚKIB) nebo veřejným prohlášením.

- **RCA záznamy (Root Cause Analysis):** Hloubková analýza příčin u závažných incidentů, včetně seznamu implementovaných nápravných opatření, která zabrání opakování incidentu.
- **Záznamy o testování:** Dokumentace o provedených simulacích incidentů (min. 1× ročně). Obsahuje scénář (např. „Únik API klíče“), seznam účastníků a vyhodnocení reakce.