
Politika řízení změn (Change Management Policy)

Verze: 1.0

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / Vedoucí IT

Vazba na ISO/IEC 27001:2022:

- A.8.31 – Správa změn
 - A.8.29 – Bezpečný vývoj (návaznost)
-

1. Účel

Účelem této politiky je zajistit, aby veškeré změny v informačních systémech byly řízeny, dokumentovány, posouzeny z hlediska bezpečnosti a schváleny před nasazením do produkčního prostředí, s cílem minimalizovat riziko výpadků a incidentů.

2. Klasifikace změn

Změny jsou rozděleny podle rizika a dopadu na provoz:

Typ změny	Popis	Schvalovatel
Standardní	Rutinní, nízkorizikové úkony (např. aktualizace AV, běžná údržba OS)	IT Administrátor
Normální	Změny s dopadem na funkčnost nebo bezpečnost (API, VPN, FW)	Fleet Manager + IT
Nouzová	Kritické zásahy nutné k odvrácení incidentu	Fleet Manager (ex-post)

3. Proces řízení změn

Každá normální změna prochází těmito kroky:

- **Žádost o změnu (RFC):** Popis změny, důvod, bezpečnostní dopady a vazba na rizika.
- **Posouzení a schválení:** Schválení odpovědnou osobou dle klasifikace změny.
- **Testování:** Ověření funkčnosti a bezpečnosti v testovacím prostředí.

- **Nasazení:** Provedení změny v plánovaném čase s minimalizací dopadu.
- **Rollback plán:** Definovaný postup návratu do původního stavu.

4. Specifické požadavky pro telemetrické systémy

- **Integrita firmwaru (RISK-FW-01):** Firmware telemetrických jednotek musí být digitálně podepsán. Nasazení nepodepsaného FW do produkce je zakázáno.
- **Bezpečnost API (RISK-API-02):** Změny API podléhají kontrole zranitelností (např. BOLA) a jsou hodnoceny v rámci procesu správy zranitelností.
- **Síťová konfigurace:** Změny APN, VPN nebo firewallových pravidel vyžadují schválení Fleet Managerem.

5. Nouzové změny

Nouzové změny mohou být provedeny okamžitě za účelem ochrany systému nebo dostupnosti služby. Dokumentace, testování a formální schválení musí být doplněny nejpozději do 24 hodin po zásahu.

6. Odpovědnosti

- **Žadatel (Vývojář / Administrátor):** Připravuje RFC, zajišťuje testování a rollback plán.
- **Fleet Manager:** Posuzuje obchodní a bezpečnostní rizika a schvaluje významné změny.
- **IT Administrátor:** Provádí technickou realizaci změn a zajišťuje jejich evidenci.

7. Auditní důkazy

Pro účely auditu jsou uchovávány:

- Záznamy RFC v ticketingovém systému nebo provozním deníku.
- Doklady o testování změn.
- Evidence verzí firmwaru a digitálních podpisů.