
Politika řízení přístupu (Access Control Policy)

Verze: 1.0

Platnost od: 20. 01. 2026

Garant procesu: Fleet Manager / IT Administrátor

Vazba na ISO 27001:2022: A.5.15 – A.5.18, A.8.2 – A.8.5

---

1. Účel

Zajistit, aby přístup k telemetrickým datům, backendu a nastavení jednotek měli pouze autorizovaní uživatelé a aby tento přístup odpovídal jejich pracovní roli.

Politika reaguje zejména na rizika: **RISK-USR-01, RISK-USR-02, RISK-NET-03, RISK-API-02**.

2. Základní principy

- **Need-to-know:** Přístup pouze k informacím nutným pro vykonání práce.
- **Least privilege:** Minimální oprávnění nutná k úkolu (např. zákazník může číst data, ale nemůže měnit firmware).
- **Segregation of Duties:** Vývoj kódu API nesmí schvalovat a nasazovat kód sám bez nezávislé kontroly.

3. Identifikace a autentizace

3.1. Politika hesel (RISK-USR-01)

- **Minimální délka:** 12 znaků.
- **Složitost:** velká/malá písmena, číslice, speciální znaky.
- **Historie:** Zákaz opakování posledních 5 hesel a používání snadno odhadnutelných řetězců.

3.2. Vícefaktorové ověřování – MFA (RISK-NET-03, RISK-USR-01)

MFA je **povinné** pro:

- Administrátorské přístupy do backendu.
- VPN přístupy.
- Administrátorské zákaznické účty v aplikaci Fleet Monitoring.

Metody a správa:

- Povolené metody: TOTP aplikace, hardwarové tokeny. SMS je povolena pouze jako záložní metoda.
- **Povinnost revize:** Pololetní revize nastavení MFA (kontrola metod, odstranění neaktivních autentizátorů a vynucená obnova/přenastavení tokenů u administrátorských účtů).

4. Správa přístupů k telemetrickému API (RISK-API-02)

- **Objektová autorizace (BOLA):** Každý požadavek ověřuje SessionID uživatele vůči VehicleID. Přístup k datům jiného vozidla se automaticky blokuje a loguje.
- **API klíče:** Nesmí být natvrdo zapsány v kódu (hardcoded). Rotace probíhá minimálně 1× ročně.

5. Životní cyklus uživatelských účtů (RISK-USR-02)

Fáze	**Pravidlo / Lhůta**
Zřízení účtu	Pouze na základě písemně schválené žádosti odpovědnou osobou.
Změna oprávnění	Musí být nastavena do **24 h** od schválení změny.
Zrušení účtu	Blokace v den ukončení poměru; hlášení odchodu zákazníka do **24 h**.
Pravidelná revize	Kvartální kontrola; neaktivní účty (>90 dní) jsou automaticky deaktivovány.

6. Vzdálený přístup a VPN

- Správcovský přístup je povolen výhradně přes **šifrovanou VPN s aktivním MFA**.
- Přímý přístup k telemetrickým jednotkám z veřejného internetu je **zakázán** (komunikace probíhá pouze přes privátní APN).

7. Auditní důkazy a logování

Pro potřeby auditu a zpětné dohledatelnosti organizace zajišťuje:

- **Logování změn (Audit Trail):** Automatický záznam změn oprávnění (vytvoření, smazání, změna role). Log je chráněn proti smazání a uchováván **min. 12 měsíců**.
- **Aktuální seznam uživatelů:** Evidence uživatelů a jejich přiřazených RBAC rolí.
- **Logy autentizace:** Záznamy z autentizačního serveru (úspěšná i neúspěšná přihlášení).
- **Záznamy o revizích:** Protokoly z kvartálních revizí účtů a pololetních revizí MFA podepsané Fleet Managerem.