
Směrnice pro mobilní zařízení a koncové body (Mobile Device & Endpoint 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.7.9 – Mobilní zařízení a práce na dálku
- A.8.19 – Zabezpečení koncových bodů

---

1. Účel

Účelem této směrnice je stanovit závazná pravidla pro bezpečné používání koncových a mobilních zařízení, která přistupují k telemetrickému systému, backendovým službám nebo interní síti organizace, a minimalizovat rizika spojená s jejich ztrátou, odcizením nebo kompromitací.

2. Povinné bezpečnostní standardy koncových bodů

Koncová zařízení nesmí být připojena k firemním systémům, pokud nesplňují následující požadavky:

- **Šifrování disku:** Povinné plné šifrování systémového disku (např. BitLocker, FileVault).
- **Ochrana proti malwaru:** Aktivní a centrálně spravovaný AV/EDR nástroj dle *Politiky ochrany proti malwaru*.
- **Aktualizace:** Operační systém a kritické aplikace musí mít aplikovány aktuální bezpečnostní záplaty.
- **Uzamykání obrazovky:** Automatické uzamčení zařízení po maximálně 5 minutách neaktivity.

3. Pravidla pro mobilní zařízení (smartphone / tablet)

Mobilní zařízení používaná pro firemní účely musí splňovat:

- **Autentizace:** Povinné zabezpečení PINem (min. 6 číslic), silným heslem nebo biometrikou.
- **Zákaz kompromitovaných zařízení:** Používání zařízení s jailbreakem nebo rootem je zakázáno.

- **Oddělení dat:** Firemní data musí být logicky oddělena od soukromých (např. pracovní profil, MDM).

4. Vzdálený přístup a práce v terénu

Vzhledem k práci techniků v terénu a přístupu k telemetrii platí:

- **Povinnost VPN:** Přístup k backendu, administraci nebo konfiguraci jednotek je povolen výhradně přes šifrovanou VPN.
- **Veřejné sítě:** Přístup k administrativním systémům přes veřejné Wi-Fi je zakázán bez aktivní VPN.
- **Fyzická ochrana:** Zařízení nesmí být ponechána bez dozoru na veřejných místech nebo ve vozidlech na viditelném místě.

5. Postup při ztrátě nebo odcizení zařízení

Při ztrátě nebo odcizení zařízení je uživatel povinen:

1. **Okamžité hlášení:** Nahlásit událost IT Administrátorovi bezodkladně, nejpozději do 2 hodin.
2. **Vzdálená opatření:** IT Administrátor provede blokaci přístupů a vzdálené smazání firemních dat (pokud je technicky možné).
3. **Změna přístupových údajů:** Okamžitá revokace VPN certifikátů a změna souvisejících hesel.

Postup je koordinován dle *Směrnice pro řešení bezpečnostních incidentů*.

6. Odpovědnosti

- **Zaměstnanec / uživatel:** Odpovídá za fyzickou ochranu zařízení a dodržování této směrnice.
- **IT Administrátor:** Odpovídá za konfiguraci bezpečnostních politik, MDM/EDR, VPN přístupů a monitoring stavu zařízení.
- **Fleet Manager:** Schvaluje nákup zařízení a přidělení oprávnění pro vzdálený přístup.

7. Auditní důkazy

Organizace uchovává následující záznamy:

- Evidence koncových a mobilních zařízení.
- Reporty z MDM a EDR nástrojů.
- Záznamy o blokaci nebo vyřazení ztracených zařízení.