
Směrnice pro práci z domova (Home Office Directive)

Verze: 1.0

Platnost od: 27. 01. 2026

Garant procesu: Fleet Manager / Vedoucí IT

Vazba na ISO/IEC 27001:2022:

- A.7.8 – Práce na dálku (Teleworking)
- A.7.9 – Mobilní zařízení a práce na dálku

---

1. Účel

Účelem této směrnice je stanovit závazné podmínky pro výkon práce mimo prostory organizace (zejména z domova) tak, aby nedošlo ke snížení úrovně ochrany informačních aktiv, telemetrických dat ani backendových systémů.

2. Obecné podmínky a schvalování

- **Schválení:** Práce z domova je povolena pouze po schválení přímým nadřízeným a pouze u pozic, kde to povaha práce umožňuje.
- **Pracovní prostředí:** Zaměstnanec je povinen zajistit prostředí, které minimalizuje riziko nahlížení nepovolaných osob na obrazovku nebo klávesnici zařízení.
- **Zákaz BYOD:** Přístup k produkčním systémům, telemetrickým datům a administraci je povolen výhradně z firemních zařízení spravovaných IT oddělením.

3. Technická bezpečnostní opatření

Při práci z domova musí být splněna všechna následující pravidla:

- **VPN + MFA:** Každé připojení k interním systémům nebo administraci telemetrie musí probíhat přes šifrovaný VPN tunel s povinným vícefaktorovým ověřením.
- **Zabezpečení domácí sítě:** Domácí Wi-Fi síť musí být chráněna minimálně standardem WPA2/WPA3 se silným heslem. Připojení přes otevřené nebo veřejné sítě bez VPN je zakázáno.
- **Stav zařízení:** Zařízení musí být v souladu s *Politikou ochrany proti malwaru* (aktivní EDR, aktuální signatury, platné aktualizace OS).

4. Ochrana informací a komunikace

- **Důvěrná komunikace:** Hovory o bezpečnostních nebo technických detailech nesmí probíhat v přítomnosti třetích osob.
- **Fyzické dokumenty:** Dokumenty obsahující citlivé údaje nesmí být likvidovány v běžném odpadu; musí být bezpečně skartovány nebo vráceny k likvidaci do sídla organizace.
- **Zákaz sdílení zařízení:** Firemní zařízení nesmí být zapůjčována ani používána jinými osobami.

5. Incidenty a technická podpora

- **Hlášení incidentů:** Jakékoliv podezření na bezpečnostní incident (phishing, kompromitace účtu, ztráta EDR ochrany) musí být okamžitě hlášeno dle *Směrnice pro řešení bezpečnostních incidentů*.
- **Vzdálená podpora:** IT podpora je poskytována výhradně prostřednictvím schválených nástrojů a pouze se souhlasem uživatele.

6. Odpovědnosti

- **Zaměstnanec:** Odpovídá za dodržování této směrnice a fyzickou ochranu zařízení v místě práce.
- **Vedoucí IT:** Odpovídá za technické zajištění VPN, MFA a dohled nad vzdálenými přístupy.
- **Fleet Manager:** Schvaluje práci z domova a zajišťuje informovanost zaměstnanců o bezpečnostních pravidlech.

7. Auditní důkazy

Organizace uchovává:

- Logy VPN přístupů (uživatel, čas, zdrojová IP).
- Záznamy o MFA autentizaci.
- Podepsané dohody o práci na dálku.