
Směrnice čistého stolu a čisté obrazovky (Clear Desk & Clear Screen Directive)

Verze: 1.0
Platnost od: 27. 01. 2026
Garant procesu: Fleet Manager / Vedoucí IT

Vazba na ISO/IEC 27001:2022:

- A.7.7 – Čistý stůl a čistá obrazovka

---

1. Účel

Účelem této směrnice je minimalizovat riziko neoprávněného přístupu k informacím, jejich ztráty nebo kompromitace během pracovní doby i mimo ni. Směrnice se vztahuje na fyzické dokumenty, paměťová média i zobrazování informací na obrazovkách a displejích.

2. Pravidla čistého stolu (fyzický prostor)

- **Opouštění pracoviště:** Při každém opuštění pracovního místa (včetně krátkodobého) musí být veškeré citlivé dokumenty a paměťová média uloženy mimo dohled nepovolaných osob.
- **Konec pracovní doby:** Po skončení pracovní doby nesmí zůstat na pracovním stole žádné dokumenty obsahující citlivé nebo důvěrné informace (např. konfigurační listy jednotek, seznamy řidičů, přístupové údaje). Dokumenty musí být uloženy v uzamykatelných zásuvkách nebo skříních.
- **Tisková zařízení:** Dokumenty nesmí být ponechány v tiskárnách, kopírkách nebo skenerech. Uživatel je povinen vyzvednout tiskové výstupy bezprostředně po jejich vytvoření.
- **Bílé tabule a flipcharty:** Informace obsahující technické, provozní nebo bezpečnostní detaily musí být po ukončení jednání neprodleně odstraněny.

3. Pravidla čisté obrazovky (digitální prostor)

- **Uzamykání stanice:** Uživatel je povinen při každém opuštění pracovního místa uzamknout obrazovku zařízení (**Win + L** / **Cmd + Ctrl + Q**).
- **Automatický zámek:** Všechna koncová zařízení musí mít aktivní automatický zámek obrazovky po **maximálně 5 minutách neaktivity**, v souladu se Směrnicí pro mobilní zařízení a koncové body.

- **Viditelnost obrazovky:** V prostředích s pohybem třetích osob musí být obrazovky umístěny tak, aby nebylo možné nahlížet na zobrazovaná data z veřejně přístupných míst.
- **Sdílení obrazovky:** Při online schůzkách je povoleno sdílet pouze konkrétní aplikace nebo okna. Sdílení celé plochy je zakázáno, pokud by mohlo dojít k neúmyslnému zobrazení citlivých informací.

4. Správa hesel a fyzických klíčů

- **Hesla:** Je přísně zakázáno uchovávat hesla nebo autentizační údaje v čitelné podobě (např. na papírcích, v sešitech nebo na monitoru).
- **Fyzické klíče:** Klíče od uzamykatelných skříní a zásuvek s citlivým obsahem nesmí být ponechány v zámcích ani volně dostupné na pracovním stole.

5. Odpovědnosti

- **Zaměstnanec:** Odpovídá za dodržování pravidel na svém pracovišti i při práci mimo prostory organizace.
- **Fleet Manager:** Odpovídá za zajištění vhodných uzamykatelných úložných prostor pro zaměstnance.
- **IT Administrátor:** Odpovídá za technické vynucení automatického uzamykání obrazovek prostřednictvím centrálních politik.

6. Kontrola a dohled

- **Namátkové kontroly:** Garant procesu nebo jím pověřená osoba provádí namátkové kontroly dodržování této směrnice, zejména po skončení pracovní doby.
- **Porušení směrnice:** Opakované nebo závažné porušení je klasifikováno jako bezpečnostní incident a řešeno v souladu s disciplinárními postupy organizace.

7. Auditní důkazy

Organizace uchovává:

- Záznamy o provedených kontrolách pracovišť.
- Konfigurační politiky automatického uzamykání obrazovek.
- Záznamy o školení zaměstnanců v oblasti informační bezpečnosti.