

Hesla a 2FA pro úředníka

Co musí vědět každý, kdo se přihlašuje do systémů obce

Souhrn pravidel pro hesla a vícefaktorovou autentizaci podle § 8 vyhl. 410/2025 Sb. a doporučení NÚKIB.



Načíst
na webu

Délka hesla podle § 8 vyhl. 410/2025

Délka rozhoduje, ne složitost. „kvetinacemodryslon“ je silnější než „Pondeli2024!“.

- NÚKIB doporučuje minimálně 16 znaků.
- Záonné minimum (§ 8 odst. 4 vyhl. 410/2025, **jen bez MFA**): 12 uživatelé / 17 administrátoři / 22 technická aktiva.
- Pro pamatovaná hesla: **frázové heslo** ze 4–6 náhodných slov.
- **Žádné** předvídatelné vzorce (velké na začátku, číslo na konci, O→0).

Vícefaktorové ověření (MFA) — § 8 odst. 2

S MFA útočník heslo nezneužije ani po úniku. Vyhláška: „alespoň dva různé typy faktorů“.

Zapněte pro: **e-mail, datovou schránku, VPN, cloudové služby, administrátorské účty.**

Aplikaci (Authenticator/Authy) preferujte před SMS. Když systém MFA neumí, **vymáhejte nápravu smluvně.**

Správce hesel + co NIKDY

Použijte **správce hesel** (Bitwarden, KeePass, 1Password) — jedno hlavní heslo, zbytek dělá software.

NIKDY: lepit na monitor, sdílet s kolegou, posílat e-mailem/SMS, používat 1 heslo na víc účtů, měnit „periodicky“ bez důvodu. Při podezření na kompromitaci: **bezodkladná změna** (§ 8 odst. 5 písm. d).