Password Policy

Verze dokumentu: 2026-07-25
Kategorie: bezpecnost

Provozovatel: Kibios s.r.o., IČO 29814995, se sídlem Brněnská 305/32, 664 44 Ořechov.
Kontakt: info@kibios.com
Online verze: https://kibios.com/pravni/password-policy

Password Policy Verze: 1.0 Účinnost od: 4. 8. 2026 Společnost: Kibios s.r.o., Brněnská 305/32, 664 44 Ořechov, IČO 298 14 995

1. Účel a rozsah

Tato Password Policy stanoví pravidla pro tvorbu, používání a správu hesel ve společnosti Kibios s.r.o. Cílem je:

- snížit riziko kompromitace účtů,
- zajistit bezpečné ověřování uživatelů,
- podpořit ochranu systémů a dat klientů i Kibios.

Policy se vztahuje na:

- všechny uživatelské a administrátorské účty v systémech Kibios,
- přístupy k interním i klientským systémům, kde Kibios používá hesla.

2. Požadavky na hesla

Každé heslo musí splňovat minimálně:

- minimální délku 12 znaků,
- kombinaci velkých a malých písmen, číslic a speciálních znaků,
- nesmí obsahovat snadno uhodnutelné prvky (jméno, login, název firmy, běžná slova, jednoduché vzory typu „123456“, „password“).

U vysoce citlivých účtů (administrátorské, přístup k citlivým datům) lze požadovat další podmínky (delší hesla, složitější strukturu).

3. Unikátnost a opětovné použití hesel

- Hesla nesmí být znovu použita mezi různými systémy, zejména mezi pracovním a osobním prostředím.
- Hesla pro administrátorské účty musí být odlišná od hesel běžných uživatelských účtů stejné osoby.

4. Platnost a změna hesel

- Hesla mají definovanou dobu platnosti (např. max. 90 dní) pro vybrané citlivé účty; po uplynutí lhůty musí být heslo změněno.
- Heslo musí být bezodkladně změněno, pokud existuje podezření na kompromitaci (např. phishing, únik databáze hesel).

- Při odchodu zaměstnance nebo ukončení spolupráce jsou jeho hesla a účty zrušeny nebo změněny v souladu s Access Control Policy.

5. Ukládání a sdílení hesel

- Hesla se nesmí zapisovat v čitelné podobě (papír na stole, nešifrované soubory, běžné poznámkové aplikace).
- Pokud je nutné uchovávat hesla, používá se bezpečný password manager schválený Kibios.
- Sdílení hesel mezi osobami je zásadně zakázáno; pokud je nutné sdílené technické heslo, musí být pod zvýšeným dohledem a co nejdříve nahrazeno individuálními přístupy.

6. MFA (vícefaktorová autentizace)

- Pro administrátorské účty a citlivé systémy je povinné použití vícefaktorové autentizace (MFA), např.:
  - heslo + OTP (aplikace, SMS),
  - heslo + hardware token,
  - heslo + FIDO2 klíč.
- MFA se používá zejména pro vzdálené přístupy (VPN, SSH, management rozhraní) v souladu s Remote Access Policy.

7. Reakce na bezpečnostní incidenty související s hesly

- Pokud je zjištěn únik nebo kompromitace hesel (např. napadení systému, únik databáze):
  - dotčená hesla jsou bezodkladně resetována,
  - uživatelé jsou informováni a vyzváni ke změně,
  - provádí se analýza příčin a nápravná opatření (Incident Response Policy).

8. Uživatelská odpovědnost

- Uživatelé odpovídají za ochranu svých hesel a nesmí je sdílet s jinými osobami.
- Uživatelé nesmí používat hesla, o kterých vědí, že se vyskytla v únikových databázích nebo jsou veřejně dostupná.
- Při podezření na zneužití účtu musí uživatel bezodkladně informovat podporu Kibios nebo svého nadřízeného.

9. Vztah k ostatním politikám

Password Policy doplňuje zejména:

- Access Control Policy (řízení oprávnění a účtů),
- Remote Access Policy (bezpečné přístupy na dálku),
- Information Security Policy (principy ochrany informací),
- Incident Response Policy (postup při kompromitaci účtů).

10. Závěrečná ustanovení

- Password Policy může být aktualizována podle změn technologií, rizik nebo doporučení v oblasti kybernetické bezpečnosti.
- Aktuální verze policy je dostupná interně; shrnutí může být poskytnuto klientům v rámci bezpečnostních dotazníků nebo auditů.
- Dokument je vyhotoven v českém jazyce; v případě překladu je rozhodující české znění.