Access Control 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/access-control-policy

Access Control 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 Access Control Policy stanoví pravidla pro řízení přístupů k systémům, aplikacím, datům a službám společnosti Kibios s.r.o. Cílem je:

- zajistit, aby měl každý uživatel pouze taková oprávnění, která nezbytně potřebuje (princip least privilege),
- chránit důvěrnost, integritu a dostupnost informací,
- zabránit neoprávněnému přístupu a zneužití účtů.

Policy se vztahuje na:

- všechny zaměstnance, spolupracovníky a externí dodavatele s přístupem k systémům Kibios,
- všechny systémy a služby provozované nebo spravované Kibios (interní i klientské).

2. Principy řízení přístupů

- přístup k systémům je poskytován na základě role a pracovní potřeby (role-based access control – RBAC),
- přístupy jsou udělovány, měněny a rušeny podle formálního schvalovacího procesu,
- administrátorské a citlivé účty používají vícefaktorovou autentizaci (MFA),
- sdílené účty se pokud možno nevyužívají; pokud je to nutné, jsou pod zvýšeným dohledem.

3. Životní cyklus účtů

3.1 Zřízení účtu

- účet je zřizován na základě schválené žádosti (např. HR, manažer, projektový vedoucí),
- jsou definována role a oprávnění, která uživatel potřebuje,
- uživatel je seznámen s bezpečnostními pravidly (Password Policy, Remote Access Policy).

3.2 Změna oprávnění

- při změně pracovní pozice, projektu nebo odpovědnosti se oprávnění přizpůsobí nové roli,
- změny oprávnění podléhají schválení nadřízeným nebo vlastníkem systému.

3.3 Zrušení účtu

- při ukončení spolupráce, odchodu zaměstnance nebo ukončení projektu se účet deaktivuje nebo smaže,

- administrátorské a přístupové údaje jsou odebrány bez zbytečného odkladu,
- tato změna se eviduje (datum, systém, odpovědná osoba).

4. Role a oprávnění

- pro klíčové systémy jsou definovány standardizované role (např. administrátor, power user, běžný uživatel, pouze čtení),
- každá role má přehledně definovaný rozsah oprávnění,
- při žádosti o přístup se vždy volí nejnižší role, která umožňuje splnit úkol.

5. Autentizace a MFA

- přihlášení k systémům probíhá pomocí individuálních účtů (uživatelské jméno, heslo, případně certifikát/token),
- administrátorské a citlivé účty (např. přístup k produkčním systémům, citlivým datům) musí používat vícefaktorovou autentizaci (MFA),
- použití MFA se řídí Password Policy a Remote Access Policy.

6. Revize přístupů

- přístupy k citlivým systémům jsou pravidelně revidovány (např. 1× za 6–12 měsíců),
- při revizi se ověřuje:
  - zda uživatel stále potřebuje daná oprávnění,
  - zda nedošlo k neoprávněnému rozšíření rolí,
  - zda existují nevyužívané účty, které je vhodné zrušit.
- výsledky revize jsou zaznamenány a vedou k případným úpravám oprávnění.

7. Administrátorské přístupy

- administrátorské účty jsou vyhrazené pouze pro technické role, které provádějí správu systému,
- administrátorské akce (např. změny konfigurace, vytváření účtů, mazání dat) jsou logovány podle Logging & Monitoring Policy,
- je preferováno oddělení administrátorského účtu od běžného uživatelského účtu jedné osoby.

8. Přístupy k klientským systémům

- přístupy Kibios k systémům klientů jsou poskytovány v souladu se smluvní dokumentací (MSA, SOW, SLA) a souhlasem klienta,
- rozsah oprávnění je omezen na úkony nutné pro poskytované služby (např.

správa, monitoring, pen-testy),

- přístupy jsou evidovány a chráněny (MFA, VPN, audit).

9. Vztah k Password Policy a Remote Access Policy

Access Control Policy je úzce provázána s:

- Password Policy (požadavky na hesla, jejich změny a správa),
- Remote Access Policy (pravidla pro přístupy na dálku, VPN, zabezpečení koncových zařízení),
- Information Security Policy (principy least privilege, need-to-know).

Konkrétní technické požadavky na hesla, MFA a vzdálené přístupy jsou uvedeny v samostatných politikách.

10. Logování a audit přístupů

- přístupy k citlivým a kritickým systémům jsou logovány (přihlášení, neúspěšné pokusy, změny oprávnění),
- logy jsou uchovávány v souladu s Logging & Monitoring Policy a Data Retention Policy,
- přístupy mohou být předmětem interního nebo externího auditu (např. v rámci bezpečnostních auditů klientů).

11. Závěrečná ustanovení

- Access Control Policy může být aktualizována podle změn technologií, služeb, rizik nebo právních požadavků.
- 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.