Remote Access 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/remote-access-policy

Remote Access 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 Remote Access Policy stanoví pravidla pro přístupy na dálku k systémům, službám a datům společnosti Kibios s.r.o. a k systémům klientů spravovaným Kibios.

Cílem je:

- zajistit bezpečné vzdálené přístupy,
- minimalizovat riziko neoprávněného přístupu,
- chránit data klientů i Kibios při práci mimo kancelář.

Policy se vztahuje na:

- všechny zaměstnance, spolupracovníky a externí dodavatele využívající vzdálený přístup (home-office, cestování, outsourcing),
- všechny systémy, ke kterým se přistupuje mimo interní zabezpečenou síť Kibios.

2. Povolené způsoby vzdáleného přístupu

- VPN přístup (IPSec / SSL) do interní sítě Kibios nebo do sítí klientů,
- zabezpečené protokoly (např. SSH, RDP přes VPN, HTTPS management rozhraní),
- přístup přes schválené remote management nástroje (např. RMM), pokud jsou správně zabezpečeny.

Přímý nešifrovaný přístup (např. telnet, nešifrované RDP, HTTP bez TLS) není povolen.

3. Autentizace a bezpečnost

- Vzdálené přístupy musí používat vícefaktorovou autentizaci (MFA) pro administrátorské a citlivé účty.
- Přihlášení probíhá přes individuální účty, sdílené účty se používají pouze ve výjimečných případech a pod zvýšenou kontrolou.
- Hesla a přístupové údaje se řídí Password Policy.

4. Koncová zařízení

- Pro vzdálený přístup je povoleno používat pouze:
  - firemní zařízení spravované Kibios (notebooky, pracovní stanice, mobilní zařízení),

    - výjimečně schválená soukromá zařízení, pokud splňují minimální bezpečnostní požadavky (aktualizovaný OS, antimalware, šifrovaný disk, silné heslo).
- Zařízení musí být:
    - pravidelně aktualizována,
    - chráněna antimalwarem,
    - zabezpečena šifrováním disku (např. BitLocker, LUKS) u citlivých dat.

5. Pravidla pro práci na dálku

- Přístup k citlivým systémům a datům se provádí pouze z důvěryhodných sítí;

používání veřejných nezabezpečených Wi-Fi je zakázáno nebo musí být doplněno VPN.

- Uživatel nesmí nechávat zařízení bez dozoru na veřejných místech.
- Při práci s citlivými daty je nutné zabránit pohledu třetích osob (např. ve veřejné dopravě, kavárnách).

6. Přístupy k systémům klientů

- Vzdálené přístupy Kibios k systémům klientů jsou zřizovány a používány v souladu se smlouvou (MSA, SOW, SLA) a jejich interními pravidly.
- Preferuje se přístup přes VPN nebo jiné zabezpečené kanály s MFA.
- Rozsah oprávnění je omezen na nezbytné minimum pro poskytované služby (správa, monitoring, incident response).

7. Logování a monitoring vzdálených přístupů

- Vzdálené přístupy (VPN, SSH, RDP, management) jsou logovány (přihlášení, odhlášení, IP, účet).
- Logy jsou uchovávány v souladu s Logging & Monitoring Policy a Data Retention Policy.
- Podezřelé aktivity (neobvyklé časy, lokality, počty pokusů) jsou předmětem bezpečnostní analýzy.

8. Bezpečnostní incidenty a reakce

- Při ztrátě nebo krádeži zařízení, podezření na kompromitaci účtu nebo přihlašovacích údajů musí uživatel bezodkladně informovat Kibios (support, bezpečnostní kontakt).
- Přístupové údaje jsou resetovány a zařízení je, pokud možno, vzdáleně zablokováno nebo vymazáno.
- Incident je řešen podle Incident Response Policy.

9. Vztah k ostatním politikám

Remote Access Policy doplňuje zejména:

- Access Control Policy (role, oprávnění, zřizování účtů),
- Password Policy (požadavky na hesla a MFA),
- Information Security Policy (principy ochrany informací),
- Incident Response Policy (postup při incidentech),

- Asset Management Policy (evidence a správa koncových zařízení).

10. Závěrečná ustanovení

- Remote Access Policy může být aktualizována podle změn technologií, služeb, způsobu práce (např. více home-office) a rizik.
- 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.