Information Security 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/information-security-policy

Information Security 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 Information Security Policy stanoví základní rámec řízení informační bezpečnosti ve společnosti Kibios s.r.o. Cílem je:

- chránit důvěrnost, integritu a dostupnost informací,
- zajistit bezpečné poskytování služeb klientům,
- splnit požadavky právních předpisů a smluvních závazků.

Policy se vztahuje na:

- všechny zaměstnance, spolupracovníky a externí dodavatele Kibios,
- všechny systémy, aplikace, sítě a datové úložiště používané Kibios,
- informace klientů, Kibios a třetích stran, se kterými Kibios pracuje.

2. Principy informační bezpečnosti

Kibios uplatňuje zejména tyto principy:

- princip „need-to-know“ a „least privilege“ pro přístupy k informacím,
- ochranu informací v souladu s jejich klasifikací (citlivost, důležitost),
- bezpečný návrh, provoz a změny systémů (security by design/by default),
- průběžné řízení rizik a pravidelnou revizi bezpečnostních opatření.

3. Klasifikace informací

Informace jsou interně klasifikovány například jako:

- veřejné,
- interní,
- důvěrné,
- vysoce důvěrné / citlivé.

Pro jednotlivé úrovně platí odlišné požadavky na:

- přístup,

- ukládání,
- přenos,
- uchování a mazání.

4. Organizační rámec

- vedení Kibios nese celkovou odpovědnost za informační bezpečnost,
- je určena role Information Security Owner / Officer (nebo odpovědná osoba), která koordinuje bezpečnostní aktivity,
- jednotlivé týmy (technický, bezpečnostní, obchodní) jsou odpovědné za dodržování bezpečnostních politik ve svých oblastech.

5. Přístupy a řízení identit

- přístupy jsou řízeny podle Access Control Policy (role, oprávnění, schvalování),
- používá se vícefaktorová autentizace (MFA) pro administrátorské a citlivé účty,
- přístupy se pravidelně revidují (zejména při nástupech, změnách rolí a odchodech).

6. Technická bezpečnost

- systémy a aplikace jsou pravidelně aktualizovány (security patch management) podle Change Management Policy,
- používají se bezpečnostní technologie (firewall, WAF, IDS/IPS, antimalware) odpovídající rizikům,
- síťová komunikace je chráněna šifrováním (např. TLS, VPN), zejména pro vzdálené přístupy.

7. Logování, monitoring a incidenty

- klíčové systémy jsou logovány a monitorovány podle Logging & Monitoring Policy,
- bezpečnostní incidenty jsou řešeny v souladu s Incident Response Policy,
- relevantní logy jsou uchovávány v souladu s Data Retention Policy.

8. Vývoj, změny a testování

- vývoj a změny systémů se řídí Secure Development Policy a Change Management Policy,
- provádí se bezpečnostní testy (např. penetrační testy, vulnerability scanning) v souladu s Rules of Engagement a AUP,
- zjištěné zranitelnosti se řeší podle Vulnerability/Responsible Disclosure Policy.

9. Ochrana dat a soulad s právem

- osobní údaje jsou zpracovávány podle Data Processing Agreement (DPA) a GDPR,
- retenční doby, anonymizace a mazání dat se řídí Data Retention Policy,
- při práci s osobními údaji se uplatňují zásady privacy by design/by default.

10. Školení a povědomí

- zaměstnanci a spolupracovníci jsou pravidelně školeni v oblasti informační bezpečnosti (phishing, práce s daty, přístupy, incidenty),
- noví pracovníci absolvují vstupní školení,
- bezpečnostní zásady jsou připomínány prostřednictvím interní komunikace.

11. Audit, kontrola a zlepšování

- dodržování Information Security Policy může být předmětem interních i externích auditů,
- zjištění z auditů, incidentů a testů jsou využívána ke zlepšování bezpečnostních opatření,
- policy je pravidelně revidována (např. 1× ročně) a aktualizována podle změn rizik, technologií a právního rámce.

12. Vztah k dalším politikám a smlouvám

Information Security Policy je „umbrella“ dokument a navazuje na:

- Incident Response Policy, Backup Policy, DRP/BCP,
- Access Control Policy, Password Policy, Remote Access Policy, Logging & Monitoring Policy, Secure Development Policy, Data Retention Policy, Privacy Policy, Cookie Policy,
- smluvní dokumentaci (MSA, VOP, SLA, DPA, AUP, RoE, SOW).

V případě rozporu mají přednost konkrétní ujednání v MSA/VOP/SLA/DPA;

Information Security Policy je interním rámcem, který tyto ujednání podporuje.

13. Závěrečná ustanovení

- Information Security Policy je interním dokumentem Kibios, jeho shrnutí může být poskytnuto klientům pro účely bezpečnostních dotazníků nebo auditů.
- Aktuální verze policy je dostupná interně; klientům může být poskytnuta vhodně zestručněná verze.
- Dokument je vyhotoven v českém jazyce; v případě překladu je rozhodující české znění.