Secure Development 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/secure-development-policy

Secure Development 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 Secure Development Policy stanoví zásady bezpečného vývoje, úprav a nasazování software a skriptů používaných společností Kibios s.r.o. při poskytování služeb klientům i pro interní potřeby. Cílem je:

- snížit riziko vzniku zranitelností v aplikacích a automatizačních nástrojích,
- zajistit bezpečný životní cyklus software (SDLC),
- podpořit soulad s bezpečnostními požadavky klientů a standardy.

Policy se vztahuje na:

- interně vyvíjený software, skripty a nástroje,
- konfigurace „as-code“ (např. IaC, CI/CD pipeline),
- úpravy a integrace třetích stran, pokud je Kibios provádí.

2. Principy bezpečného vývoje

- security by design a security by default,
- minimalizace útokového povrchu (nepoužívat zbytečné funkce, porty, služby),
- validace vstupů a bezpečné nakládání s výstupy (ochrana proti XSS, SQL injection, command injection),
- bezpečné nakládání s identitami, přístupy a tajnými informacemi (hesla, tokeny, klíče).

3. Vývojový proces (SDLC)

- Požadavky: zahrnutí bezpečnostních požadavků klientů a interních politik (Information Security Policy, DPA, AUP).
- Návrh: posouzení bezpečnostních rizik architektury (autentizace, autorizace, šifrování, logování).
- Implementace: dodržování bezpečnostních kodérských standardů (např.

OWASP, secure coding guidelines).

- Testování: zahrnutí bezpečnostních testů (statická analýza, dynamické testy, pen-testy, regresní testy).
- Nasazení: řízené a dokumentované, v souladu s Change Management Policy.

4. Nakládání s tajnými informacemi (secrets)

- Hesla, API klíče, tokeny a certifikáty se nesmí ukládat přímo v kódu nebo v nešifrovaných konfiguračních souborech.
- Secrets se ukládají v bezpečných úložištích (např. secret manager, vault) se řízeným přístupem.
- Přístup k secrets mají pouze oprávněné role; jejich použití je logováno, kde je to vhodné.

5. Závislosti a knihovny třetích stran

- Používané knihovny a závislosti (frameworky, balíčky) musí být pravidelně aktualizovány.
- Před použitím se ověřuje jejich důvěryhodnost (zdroj, licence, reputace).
- Zranitelnosti v závislostech se sledují a řeší (např. pomocí nástrojů pro dependency scanning).

6. Bezpečnostní testování

- Pro nové verze a významné změny se provádějí bezpečnostní testy, např.:
  - statická analýza kódu (SAST),
  - dynamické testování (DAST),
  - penetrační testy vybraných komponent,
  - testy autorizace a přístupových kontrol.
- Zjištěné zranitelnosti se klasifikují (kritičnost, CVSS) a řeší v souladu s Incident Response / Vulnerability Management procesem.

7. Logování a monitoring aplikací

- Aplikace musí generovat adekvátní logy (přihlášení, chyby, bezpečnostní události) v souladu s Logging & Monitoring Policy.
- Logy nesmí obsahovat citlivé údaje v nezašifrované nebo zbytečně detailní podobě (např. hesla, kompletní čísla platebních karet).

8. Prostředí pro vývoj, test a produkci

- Vývojové, testovací a produkční prostředí jsou oddělena.
- Produkční data se nepoužívají ve vývojovém/testovacím prostředí, pokud nejsou patřičně anonymizována nebo pseudoanonymizována.
- Nasazení do produkce podléhá Change Management Policy (schválení, plán, rollback).

9. Dokumentace a školení

- Bezpečnostní aspekty aplikací jsou dokumentovány (architektura, autentizace, autorizace, šifrování, logování).
- Vývojáři a devops/infrastrukturní týmy jsou pravidelně školeni v oblasti secure coding, OWASP Top 10 a aktuálních hrozeb.

10. Vztah k ostatním politikám

Secure Development Policy doplňuje zejména:

- Information Security Policy (principy ochrany informací),
- Change Management Policy (řízení změn a nasazení),
- Incident Response Policy (řešení zranitelností a incidentů),
- Logging & Monitoring Policy (logování aplikací),
- Data Retention Policy a DPA (nakládání s daty, osobní údaje).

11. Závěrečná ustanovení

- Secure Development Policy může být aktualizována podle vývoje technologií, přijatých standardů a zkušeností z auditů/incidentů.
- 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.