Logging & Monitoring 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/logging-monitoring-policy

Logging & Monitoring 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 Logging & Monitoring Policy stanoví pravidla pro logování, sledování a vyhodnocování událostí v systémech provozovaných nebo spravovaných společností Kibios s.r.o. Cílem je:

- zajistit včasné odhalení bezpečnostních incidentů a provozních problémů,
- podpořit analýzu incidentů a auditní stopu,
- splnit požadavky klientů a právních předpisů.

Policy se vztahuje na:

- interní systémy Kibios,
- systémy a služby klientů, u nichž Kibios poskytuje monitoring/logování v rámci smlouvy (MSA/SOW/SLA).

2. Typy logovaných událostí

Logovány jsou zejména:

- autentizační události (přihlášení, odhlášení, neúspěšné pokusy),
- změny oprávnění a konfigurací (administrátorské akce),
- systémové události (restarty, chyby, výpadky služeb),
- bezpečnostní události (detekce malwaru, firewall blokace, podezřelé přístupy),
- provozní metriky (dostupnost, výkon, kapacita) pro monitoring.

Rozsah logování může být přizpůsoben konkrétním systémům a požadavkům klienta.

3. Nástroje pro logging a monitoring

- Pro sběr a uchovávání logů se používají centrální nebo distribuované logovací systémy (např. SIEM, log management nástroje).
- Pro monitoring se využívají specializované nástroje (např. monitoring serverů, aplikací, sítí) s alertingem.
- Výběr nástrojů zohledňuje bezpečnost, škálovatelnost a potřeby klientů.

4. Alerting a reakce

- Pro klíčové systémy jsou definovány prahové hodnoty a pravidla pro generování alertů (např. neúspěšná přihlášení, vysoké zatížení, nedostupnost služby).
- Alerty jsou směrovány na odpovědné osoby/týmy (support, on-call technici, bezpečnostní tým).
- Reakce na alerty se řídí Incident Response Policy a SLA (priority P1–P4, reakční časy).

5. Uchovávání logů

- Logy jsou uchovávány po dobu stanovenou v Data Retention Policy, s ohledem na:
  - bezpečnostní potřeby (analýza incidentů, forenzika),
  - smluvní požadavky klientů,
  - právní předpisy (např. účetnictví, kybernetická bezpečnost).
- Po uplynutí retenční doby jsou logy bezpečně mazány nebo anonymizovány.

6. Ochrana logů

- Logy mohou obsahovat citlivé informace; proto jsou:
  - ukládány na zabezpečených úložištích,
  - přístupné pouze oprávněným osobám (RBAC, MFA),
  - chráněny proti neoprávněné změně a smazání (integrita).

7. Přístup k logům a jejich využití

- Přístup k logům mají pouze osoby, které je potřebují pro:
  - provozní monitoring,
  - bezpečnostní analýzu,
  - audit nebo reporting.
- Logy mohou být využity jako důkazní materiál při incidentu nebo sporu; s takovými logy se nakládá podle Incident Response Policy a právních předpisů.

8. Logging v prostředí klientů

- Rozsah a způsob logování u systémů klientů spravovaných Kibios je stanoven v MSA/SOW/SLA nebo jiných dohodách.
- Kibios může klientům poskytovat:
  - přístup k vybraným logům,
  - reporty (např. měsíční přehled incidentů, dostupnosti),
  - doporučení na zlepšení logování/monitoringu.

9. Soukromí a osobní údaje

- Logování a monitoring probíhá v souladu s GDPR a DPA; logy obsahující osobní údaje jsou zpracovávány s odpovídající ochranou.

- Osobní údaje v logách jsou uchovávány jen po nezbytně nutnou dobu a jejich přístup je omezen na oprávněné osoby.

10. Vztah k ostatním politikám

Logging & Monitoring Policy je provázána zejména s:

- Incident Response Policy (detekce, analýza incidentů),
- Data Retention Policy (retenční doby logů),
- Access Control Policy (přístupy k logovacím systémům),
- Information Security Policy (monitoring bezpečnosti),
- Backup Policy (zálohování logů, pokud je to nutné).

11. Závěrečná ustanovení

- Logging & Monitoring Policy může být aktualizována podle změn technologií, služeb, rizik nebo požadavků klientů.
- 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.