Incident Response Policy

Verze dokumentu: 2026-07-25
Kategorie: incidenty

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/incident-response-policy

Incident Response 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 působnost

Tato Incident Response Policy (dále jen „IR Policy“) stanoví pravidla a postupy společnosti Kibios s.r.o. pro zjišťování, řízení a řešení bezpečnostních incidentů v oblasti IT a kybernetické bezpečnosti. IR Policy se vztahuje na:

- všechny služby poskytované Kibios klientům (monitoring, správa systémů, bezpečnostní audity, penetrační testy, zálohy, incident response),
- interní systémy Kibios, které souvisí s poskytováním těchto služeb.

2. Definice incidentu

Incident je každá událost, která má nebo může mít dopad na důvěrnost, integritu nebo dostupnost systémů, služeb nebo dat klienta či Kibios. Za incident se považuje zejména:

- kybernetický útok (např. ransomware, phishing, exploit zranitelnosti),
- neautorizovaný přístup nebo pokus o něj,
- únik nebo ztráta dat,
- neautorizovaná změna konfigurace či kódu,
- selhání bezpečnostních opatření (např. nefunkční zálohy, nefunkční MFA).

Závažný incident je takový incident, který:

- má významný dopad na provoz klienta nebo Kibios,
- může mít regulatorní dopad (např. podle GDPR, zákona o kybernetické bezpečnosti, DORA),
- vyžaduje eskalaci na úroveň vedení nebo právního/DPO.

3. Role a odpovědnosti

3.1 Incident Manager

- řídí řešení incidentu,
- koordinuje technické, komunikační a organizační kroky,
- zajišťuje komunikaci s klientem, vedením a případně s regulatorními orgány,
- schvaluje závěrečný post-incident report.

3.2 Technical Response Team

- provádí technickou analýzu incidentu,
- zajišťuje containment, eradikaci a obnovu,
- sbírá a uchovává relevantní logy a důkazní materiály,
- navrhuje technická nápravná opatření.

3.3 Account / Client Manager

- zajišťuje koordinaci s klientem,
- informuje klienta o průběhu incidentu, dopadech a navržených opatřeních,
- zohledňuje obchodní důsledky incidentu.

3.4 DPO / právní

- posuzuje, zda incident představuje porušení zabezpečení osobních údajů podle GDPR,
- doporučuje, zda je nutné oznámení dozorovému orgánu (ÚOOÚ) a subjektům údajů,
- koordinuje případnou komunikaci s NÚKIB, ČNB apod., pokud je relevantní.

4. Fáze Incident Response

4.1 Detekce a hlášení

- incident je detekován monitoringem Kibios (alert) nebo nahlášen klientem (ticket, e-mail, telefon),
- vytvoří se incident ticket s minimálně: popisem, časem, postiženými systémy, kontaktní osobou klienta.

4.2 Triage a klasifikace

- Incident Manager nebo pověřený technik přiřadí prioritu P1–P4 dle SLA (kritický, vysoký, střední, nízký),
- odhadne rozsah dopadu (které systémy, jaký typ dat, počet uživatelů).

4.3 Containment (zadržení)

- cílem je zabránit dalšímu šíření incidentu (např. izolace serveru, blokace účtu, úprava firewall pravidel),
- provádí se tak, aby se minimalizoval dopad na provoz, ale zároveň byla zajištěna bezpečnost.

4.4 Analýza a eradikace

- provede se technická analýza příčin (root cause analysis) a vektoru útoku,
- odstraní se malware nebo jiné škodlivé prvky,
- opraví se zranitelnost (patch, konfigurace, změna kódu),
- aktualizuje se konfigurace nebo přístupová práva.

4.5 Obnova (recovery)

- obnoví se postižené systémy z bezpečných záloh, pokud je to nutné,
- systémy se vrátí do běžného provozu,
- po určitou dobu se provádí intenzivnější monitoring, aby se včas odhalily případné re-incidenty.

4.6 Post-incident review (lessons learned)

- vypracuje se post-mortem report, který shrnuje: průběh, příčiny, dopady, přijatá opatření, doporučení,

- identifikují se změny procesů, konfigurací, školení nebo technologií, které sníží riziko opakování.

5. Komunikace s klientem

- U incidentů s prioritou P1/P2 Kibios informuje klienta bez zbytečného odkladu, typicky do max. 4 hodin od zjištění.
- Klient má určenu kontaktní osobu pro incidenty, která je dostupná pro eskalace.
- Průběh incidentu je komunikován průběžně (např. periodické updaty u P1 incidentů).
- Po ukončení incidentu Kibios předá klientovi shrnutí, případně detailní post- mortem report.

6. Evidence, logování a důkazy

- Každý incident je evidován v incident/ticket systému (ID incidentu, datum, systém, dopad, priorita, stav).
- Relevantní logy, artefakty a důkazní materiály (např. log files, hash soubory, screenshoty) jsou uchovávány po dobu nezbytně nutnou k analýze, reportingu a ochraně právních nároků, v souladu s Data Retention Policy.
- S citlivými daty (osobní údaje, hesla, klíče, tokeny) se nakládá podle DPA a bezpečnostních politik Kibios; po ukončení incidentu jsou v maximální možné míře anonymizovány nebo smazány.

7. GDPR a regulatorní dopady

Pokud incident zahrnuje osobní údaje:

- Incident Manager informuje DPO/právní.
- DPO posoudí, zda jde o porušení zabezpečení osobních údajů ve smyslu čl. 33 a 34 GDPR.
- Pokud je nutné oznámení ÚOOÚ nebo subjektům údajů, Kibios poskytne klientovi technickou a faktickou součinnost (logy, detail incidentu, přijatá opatření).

U klientů spadajících pod:

- zákon č. 264/2025 Sb., o kybernetické bezpečnosti,
- Nařízení (EU) 2022/2554 (DORA), Kibios poskytuje technické podklady a podporu pro jejich vlastní regulatorní reportování; odpovědnost za splnění regulatorních povinností má primárně klient.

8. Testování Incident Response procesu

- Incident Response proces je pravidelně testován, minimálně 1× ročně, formou:
  - tabletop cvičení,
  - simulačních scénářů,
  - technických testů vybraných částí (např. detekce, eskalace, obnovy).
- Výsledky testů budou zaznamenány a zohledněny při aktualizaci IR Policy a souvisejících procesů.

9. Vztah k ostatním dokumentům

Tato IR Policy doplňuje a konkretizuje:

- Master Service Agreement (MSA), Všeobecné obchodní podmínky (VOP) a Service Level Agreement (SLA),

- Backup Policy, Logging & Monitoring Policy, Data Retention Policy, Data Processing Agreement (DPA), Information Security Policy.

V případě rozporu mezi IR Policy a smluvní dokumentací (MSA/VOP/SLA) mají přednost ujednání v MSA/VOP/SLA; IR Policy slouží jako interní a klientsky sdílený procesní předpis.

10. Závěrečná ustanovení

- IR Policy může být aktualizována podle změn technologií, právních předpisů nebo zkušeností z incidentů.
- Aktuální verze IR Policy je dostupná klientům na vyžádání nebo prostřednictvím klientského portálu Kibios.
- IR Policy je vyhotovena v českém jazyce; v případě překladu je rozhodující české znění.