Business Continuity Plan

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/business-continuity-plan

Business Continuity Policy / Plan (BCP) 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

Tento Business Continuity Policy / Plan (BCP) stanoví zásady a základní rámec zajištění kontinuity klíčových služeb a činností společnosti Kibios s.r.o. v případě závažných narušení provozu (incidenty, výpadky, havárie, katastrofy).

Cílem je:

- minimalizovat přerušení poskytování služeb klientům,
- zajistit pokračování kritických funkcí,
- podpořit rychlou obnovu do normálního provozu.

BCP se vztahuje na:

- klíčové služby poskytované klientům (monitoring, správa systémů, incident response, pen-testy, zálohování),
- interní procesy nezbytné pro poskytování těchto služeb (support, ticketing, přístupy, komunikace).

2. Kritické činnosti a systémy

Mezi kritické činnosti a systémy Kibios patří zejména:

- monitoring a alerting klientských systémů,
- incident response a podpora (ticket systém, komunikační kanály),
- zálohování a obnova dat,
- přístup k infrastruktuře (VPN, přístupové údaje, správcovské účty),
- interní koordinace (komunikační nástroje, dokumentace).

Pro každý kritický systém/proces je interně určeno:

- jeho význam (kritický/vysoký/střední),
- maximální tolerovatelná doba výpadku (RTO),
- maximální tolerovatelná ztráta dat (RPO),
- alternativní postupy v případě nedostupnosti.

3. Scénáře narušení

BCP počítá zejména s těmito typy narušení:

- výpadek datacentra nebo cloudové lokace,
- rozsáhlé síťové výpadky (ISP, routing, DDoS),
- selhání klíčových interních systémů (ticketing, monitoring),
- fyzická omezení (např. nedostupnost kanceláře, omezení pohybu),
- personální výpadky (nedostupnost klíčových osob, nemoc, jiné krizové situace).

4. Principy zajištění kontinuity

- redundance a geo-redundance pro klíčové systémy (monitoring, ticketing, zálohy),
- dokumentované postupy pro přechod na náhradní řešení (fallback plány),
- pravidelné zálohování a testování obnovy (viz Backup Policy),
- jasně definované role a kontakty pro krizové situace,
- možnost práce na dálku (remote access) pro klíčové role.

5. Role a odpovědnosti

- Business Continuity Owner / Manager – odpovědný za koordinaci BCP, aktualizaci plánů a vedení krizového týmu.
- Krizový tým (Crisis / Continuity Team) – zástupci technického, bezpečnostního, provozního a obchodního úseku, kteří koordinují reakci na závažné narušení.
- Technické týmy – zajišťují technické kroky (přepnutí, obnovu, alternativní řešení).
- Account / Client manažeři – komunikují s klienty o dopadech, očekávané době obnovy a dostupných alternativách.

6. Aktivace BCP

BCP se aktivuje v případě, že:

- dojde k narušení provozu, které přesahuje běžný incident a má dopad na více služeb nebo klientů,
- nelze dodržet standardní SLA bez zvláštních opatření,
- je pravděpodobná delší nedostupnost klíčového systému nebo infrastruktury.

Po aktivaci BCP:

- se svolá krizový/continuity tým (fyzicky nebo online),
- identifikuje se rozsah a dopad narušení,
- rozhodne se o přechodu na náhradní režim/řešení,
- stanoví se komunikační plán vůči klientům.

7. Náhradní režimy (fallback)

Příklady náhradních režimů:

- přechod na sekundární monitoring platformu nebo cloudovou lokaci,
- využití alternativního ticketing systému či nouzové e-mailové adresy pro podporu,

- dočasné omezení některých ne-kritických služeb, aby byly zdroje soustředěny na kritické funkce,
- využití vzdálené práce (home-office) pro klíčové osoby, pokud není dostupná kancelář.

Detailní technické postupy jsou popsány v interních provozních dokumentech (runbooky).

8. Komunikace s klienty při narušení

- Klienti jsou informováni o závažných narušeních, která mohou ovlivnit poskytování služeb, bez zbytečného odkladu.
- Informace obsahují: stručný popis problému, rozsah dopadu, odhadovanou dobu nápravy, případná doporučení pro klienta.
- Při delším narušení jsou poskytovány průběžné updaty.
- Po obnovení běžného provozu může být klientům poskytnuto shrnutí opatření (post-incident/post-disruption report).

9. Vztah k Disaster Recovery (DRP), SLA a dalším dokumentům

BCP je provázán zejména s:

- Disaster Recovery Policy/Plan (DRP) – technické scénáře obnovy po závažných incidentech,
- Backup Policy – zálohování a obnova dat,
- Incident Response Policy – řešení incidentů,
- Access Control Policy / Remote Access Policy – přístupy a práce na dálku,
- SLA – garantované úrovně služeb a reakční časy.

BCP se zaměřuje na kontinuitu provozu jako celku, zatímco DRP se soustředí na technickou obnovu po katastrofě; oba dokumenty se doplňují.

10. Testování a aktualizace BCP

- BCP je pravidelně testován, minimálně 1× ročně, pomocí simulací a cvičení (tabletop, technické testy přepnutí na záložní systémy).
- Výsledky testů jsou dokumentovány a zohledněny při aktualizaci plánů.
- BCP je aktualizován v návaznosti na:
  - změny infrastruktury a služeb,
  - zkušenosti z incidentů a narušení,
  - změny regulatorních požadavků (např. DORA).

11. Závěrečná ustanovení

- Business Continuity Policy / Plan je interním dokumentem Kibios, jehož shrnutí může být poskytnuto klientům pro účely bezpečnostních dotazníků, auditů nebo regulatorních požadavků.
- Aktuální verze BCP je dostupná interně; klientům lze poskytnout přiměřeně detailní verzi nebo shrnutí.
- Dokument je vyhotoven v českém jazyce; v případě překladu je rozhodující české znění.