ALAI Client Incident Response — Runbook

ALAI Client Incident Response — Runbook

Version: 1.0 **Created:** 2026-07-28 **Owner:** John (AI Director) / Alem Basic (CEO) **Source process:** processes/incident-management.md (full spec), processes/quick-ref/incident-response-quickref.md
Related: processes/templates/incident-report.md, processes/communication-protocol.md

---

1. Purpose

Client-facing runbook for handling any incident that affects a client's service: production outages, bugs, security incidents, SLA breaches. This is the condensed operational version — the full governance document (classification rationale, GDPR appendix, KPIs, audit trail) lives in `processes/incident-management.md`.

---

2. Severity Matrix

Severity	Definition	Response Time	Resolution Target	Notify
P1 CRITICAL	Service completely down, active data breach, revenue impact, legal/regulatory violation	15 min	4 hours	Alem + Client + Datatilsynet (if GDPR)
P2 HIGH	Major feature broken, client blocked, no workaround, security vulnerability	1 hour	8 hours	John + Tech Lead + Client

Severity	Definition	Response Time	Resolution Target	Notify
P3 MEDIUM	Minor feature broken, workaround exists	4 hours	24 hours	John + relevant agent
P4 LOW	Cosmetic, no business impact	24 hours	5 days	Assigned agent

When in doubt, escalate up. Better to downgrade a P1 to P2 than to underestimate a critical incident.

---

3. Response Flow

```
Detection -> Triage & Classify -> Investigation -> Resolution -> Verification -> Communication -> Post-Mortem -> Closure
```

Step 1 — Detection

Source	Action
Automated monitoring (Mission Control, health checks)	Auto-alert to John
Client report (email, ticket)	Logged via `support-ticket.js`, escalated by John
Internal discovery (agent/dev)	Report to John immediately (Slack #ai-ops)
Third-party/vendor	Forward to John + Alem

Step 2 — Triage & Classify (John, within SLA response time above)

1. Acknowledge receipt to the reporter
2. Classify severity using the matrix in Section 2
3. Assign owner (agent/role per incident type)
4. Create incident record: `comms/incidents/INC-YYYY-MM-DD-NNN.md` from `processes/templates/incident-report.md`
5. Notify stakeholders per Escalation Matrix (Section 4)
6. Open Slack thread in `#incidents`

Step 3 — Investigation

- Reproduce the issue in the affected environment
- Gather evidence: logs, metrics, screenshots

- Root cause analysis (5 Whys / Fishbone / Timeline) — **mandatory for P1/P2**
- Assess impact: users, data, services affected
- Fix plan: immediate mitigation vs. long-term fix

Step 4 — Resolution

- Implement fix (code, config, infra, or process change)
- Validate: staging for P2-P4, production hotfix + 1h monitoring for P1
- Deploy per deployment protocol
- Monitor metrics/logs/error rates for 1 hour post-deploy

Step 5 — Verification

- ☐ Fix deployed to production
- ☐ Smoke tests passing
- ☐ No related errors in the last hour
- ☐ Monitoring shows normal metrics
- ☐ Client confirms resolution (if client-reported)
- ☐ Incident record updated to "Resolved"

Step 6 — Communication cadence

Severity	Initial Update	Progress Updates	Resolution Notice
P1	Within 15 min	Every 30 min	Immediately + 24h follow-up
P2	Within 1 hour	Every 2 hours	Within 1h of resolution
P3	Within 4 hours	Daily if >24h	Next business day OK
P4	N/A unless client-reported	N/A	Next sprint review

Step 7 — Post-Mortem (mandatory P1/P2, optional P3)

- Scheduled within 2 business days of resolution, conducted within 5
- Blameless, fact-based, action-oriented
- Every post-mortem produces at least one action item, tracked in Mission Control
- Template and full 10-section structure: see `processes/incident-management.md` §7.3

Step 8 — Closure

- ☐ Incident resolved and verified
- ☐ Post-mortem completed (P1/P2)
- ☐ Action items created and assigned
- ☐ Documentation/runbooks updated
- ☐ Client notified (final resolution email)
- ☐ Incident record archived to `comms/incidents/archive/YYYY/`

---

4. Escalation Matrix

```
P4: Developer -> Tech Lead (review) -> Archive
P3: Developer -> Tech Lead (notified) -> Archive
P2: Tech Lead (owns) -> John (notified) -> Client notified -> Archive
                                        -> if SLA breach: Alem involved
P1: John coordinates -> Alem notified IMMEDIATELY -> Client notified IMMEDIATELY
                                                  -> Datatilsynet if GDPR breach (72h)
```

Escalate to Alem when: any P1; P2 affecting a major client or revenue; client relationship risk; legal/regulatory implication (GDPR, lawsuit threat); media/PR risk; financial impact >50,000 NOK; requires external assistance.

Authority	When	Deadline	Contact
Datatilsynet	Personal data breach (GDPR Art. 33)	72h from detection	postkasse@datatilsynet.no
Client	Breach of data processing agreement	24h per DPA	Client contact per contract
Politiet (Kripos)	Criminal activity	Immediately	02800, tips@politiet.no
NSM	Critical infrastructure attack	Immediately	nsm@nsm.no

---

5. Client Communication Templates

Initial notification (email, within SLA)

Use values from the incident record and the client contract/contact record before sending.

```
Subject: Action Required or Informational — Service Incident Notification — {{client_name}}

We are writing to inform you of a service incident affecting {{affected_service_or_feature}}.

Incident Summary:
- What: {{impact_what_users_experience}}
- When Detected: {{detected_date_time_with_timezone}}
- Current Status: {{investigating_mitigating_or_resolved}}
- Impact to Your Users: {{specific_user_impact}}

What We Are Doing: {{response_actions_underway}}
Next Steps: {{client_expectation_workaround_next_update_time}}
Estimated Resolution: {{estimated_resolution_or_investigating}}

We will provide updates every {{update_cadence}} until resolved.
```

Resolution confirmation

Use values from the incident record and production verification evidence before sending.

```
Subject: RESOLVED: Service Incident — {{client_name}}

Incident Summary:
- Issue: {{issue_summary}}
- Root Cause: {{brief_non_technical_root_cause}}
- Resolution: {{what_was_fixed}}
- Resolved At / Total Duration: {{resolved_timestamp_and_duration}}

Preventive Actions: {{prevention_actions}}
Impact to Your Data: {{data_impact_statement}}
```

Full template set (internal declared/update/resolved, GDPR Art. 33/34 regulatory notices): `processes/incident-management.md` §6.

---

6. On-Call

- **Primary:** John (AI Director) — 24/7 via automated monitoring
- **Human backup:** Alem (CEO) — for P1 decisions requiring a human

- **Business hours:** Mon-Fri 08:00-18:00 CET; after-hours P1 = John responds immediately + alerts Alem by phone, P2 = John within 1h + email to Alem (reviewed within 4h)
- **Contact priority:** Slack #ai-ops -> email alem@alai.no -> phone (P1 only)

---

7. Tools

Tool	Purpose	Command
support-ticket.js	Create incident record from client report	`node ~/system/tools/support-ticket.js create --title "<incident title>" --severity <P1-P4>`
Mission Control	Track incident as task	`node ~/system/tools/mc.js add "<INC-ID> <incident title>" --priority high`
Slack	Real-time incident channel	`node ~/system/tools/slack.js send incidents "<incident update>"`
HiveMind	Log lessons learned	`node ~/system/agents/hivemind/hivemind.js post john incident "<lesson learned>"`
health-check.js	System health monitoring	`node ~/system/tools/health-check.js --quick`
auto-fix.js	Automated recovery for known issues	`node ~/system/tools/auto-fix.js <service> <issue>`

Mission Control Dashboard: http://localhost:3030

---

8. Hard Rules

- **Blameless post-mortems** — focus on systems/process, never individuals.
- **Every P1/P2 gets a post-mortem** within 5 business days, no exceptions.
- **GDPR 72h clock starts at detection**, not at confirmation — when in doubt, start the clock.
- **Client communication is never skipped** for P1/P2, even if resolution is fast.
- **No incident closes without an incident record** in `comms/incidents/`.

---

9. Related Documents

- processes/incident-management.md — full 13-section governance document (severity rationale, KPIs, RCA appendix, GDPR breach assessment tree, quarterly review process)
- processes/quick-ref/incident-response-quickref.md — 1-page field version

- processes/templates/incident-report.md
- ALAI-CLIENT-ONBOARDING.md
- ALAI-CLIENT-INVOICE-CYCLE.md

Document Location: `~/ALAI/processes/runbooks/ALAI-CLIENT-INCIDENT-RESPONSE.md` **Access Control:** INTERNAL

Revision #3
Created 2026-07-28 17:56:28 UTC by John
Updated 2026-07-28 18:02:45 UTC by John