AlertOwl

Incident Response Plan

Version 1.1 | March 2026
Friday Surprise LLC
CONFIDENTIAL

1. Purpose

This plan establishes procedures for detecting, responding to, and recovering from security incidents affecting AlertOwl systems or customer data. It ensures timely response, minimizes impact, and meets notification obligations under EU GDPR, UK GDPR, UAE PDPL, and US state privacy laws.

2. Incident Classification

Severity	Description	Examples	Response Time
Critical (P1)	Active data breach or complete service outage	Unauthorized access to customer data, database compromise, credential leak	Immediate (within 1 hour)
High (P2)	Significant security event or major degradation	Failed breach attempt with indicators, OAuth token exposure, DDoS attack	Within 4 hours
Medium (P3)	Security concern requiring investigation	Suspicious login patterns, unusual API usage, dependency vulnerability	Within 24 hours
Low (P4)	Minor security observation	Failed login attempts, routine vulnerability scan alerts	Within 72 hours

3. Incident Response Team

Role	Primary	Secondary / Backup	Responsibilities
Incident Commander	Ali Munir (Founder) ali@alertowl.ai	Yasir Naveed yasir@alertowl.ai	Overall response coordination, external communications, regulatory notifications
Technical Lead	Ali Munir ali@alertowl.ai	Yasir Naveed yasir@alertowl.ai	Investigation, containment, remediation, evidence preservation
Communications Lead	Ali Munir ali@alertowl.ai	Yasir Naveed yasir@alertowl.ai	Customer notification, status updates, regulatory correspondence

Note: As a bootstrapped startup, all primary roles are held by the founder with the co-founder as backup. If the primary contact is unavailable, the secondary contact assumes all responsibilities. As the team grows, these responsibilities will be distributed to dedicated personnel.

4. Detection

- Sentry alerts for application errors and anomalies
- Supabase dashboard for unusual database activity
- Twilio console for unexpected messaging patterns
- Manual review of n8n execution logs
- Customer reports via security@alertowl.ai
- DigitalOcean monitoring agent for server-level anomalies

5. Response Procedures

5.1 Containment (Immediate Actions)

1. Assess scope: identify affected systems, data, and customers
2. Isolate: disable affected workflows, revoke compromised credentials
3. Preserve evidence: screenshot logs, export execution data before credential rotation
4. Rotate credentials: regenerate API keys, OAuth secrets, database passwords as needed
5. Block attack vector: update firewall rules, disable compromised endpoints

5.2 Eradication

6. Identify root cause through log analysis (n8n execution logs, Sentry, Supabase logs)
7. Remove malicious access or code
8. Patch vulnerability that enabled the incident
9. Verify fix through testing in isolated environment

5.3 Recovery

10. Restore services from known-good state (restore from DO Spaces backup if needed)
11. Monitor for recurrence (enhanced logging for 30 days)
12. Validate data integrity against Supabase backups
13. Re-enable disabled workflows one at a time, verifying each

5.4 Post-Incident

14. Write incident report within 48 hours
15. Conduct root cause analysis
16. Update security controls based on lessons learned
17. Update this plan if gaps were identified
18. Brief all team members on lessons learned

6. Notification Requirements

6.1 Regulatory Notification

Jurisdiction	Authority	Timeline	Trigger
EU (GDPR)	Relevant Member State supervisory authority	Within 72 hours	Personal data breach likely to result in risk to data subjects
Germany	BfDI or relevant state DPA	Within 72 hours	Same as EU GDPR
UK (UK GDPR)	ICO (Information Commissioner's Office)	Within 72 hours	Personal data breach likely to result in risk to data subjects
UAE (PDPL)	UAE Data Office	Immediately (interpreted as 72 hours)	Breach compromising privacy, confidentiality, or security
USA (CCPA)	California Attorney General	Per state law requirements	Breach of unencrypted personal information

6.2 Customer Notification

- All affected customers notified via email within 72 hours
- Notification includes: nature of incident, data affected, remediation steps taken, recommended actions for the customer
- Where breach poses high risk to data subjects (EU/UK GDPR), affected individuals are also notified without undue delay

7. Contact Information

Contact	Details
Incident Commander (Primary)	Ali Munir | ali@alertowl.ai
Incident Commander (Backup)	Yasir Naveed | yasir@alertowl.ai
Security Inbox	security@alertowl.ai
Privacy Inbox	privacy@alertowl.ai
Supabase Support	support@supabase.io
DigitalOcean Support	Via DO dashboard
Twilio Support	Via Twilio console

8. Escalation Matrix

Severity	Notify Primary	Notify Backup	Notify Customers
P1 (Critical)	Immediately	Immediately	Within 72 hours
P2 (High)	Within 1 hour	Within 4 hours	If data affected
P3 (Medium)	Within 4 hours	Next business day	Only if data affected
P4 (Low)	Next business day	Weekly summary	No

9. Plan Testing and Review

This plan is tested annually through a tabletop exercise simulating a data breach scenario. Results are documented and gaps are addressed in plan updates. The plan is also reviewed upon any significant change in infrastructure, team, or regulatory requirements.

Document Control

Version	Date	Author	Changes
1.0	March 2026	Ali Munir	Initial version
1.1	March 2026	Ali Munir	Added Yasir Naveed as backup for all roles. Added escalation matrix. Added multi-jurisdiction notification table.