

Incident Response Policy

Methodology for Security Triage, Threat Containment, Breach Notification, and Operational Recovery

ORGANIZATION

Northwind Labs, Inc. (14 Personnel)

DOCUMENT OWNER

Head of Security & Infrastructure

VERSION / STATUS

Version 1.0 • Active & Approved

EFFECTIVE DATE

October 1, 2026

CORE INFRASTRUCTURE

AWS • Okta • GitHub • PagerDuty • Slack

TARGET AUDIT SCOPE

SOC 2 Type II (Security / Availability)

1. Purpose

SOC 2: CC7.2, CC7.3, CC7.4

The purpose of this Incident Response Policy is to establish a structured, repeatable methodology for detecting, triaging, containing, remediating, and recovering from information security events and incidents affecting Northwind Labs, Inc. ("Northwind Labs"). This policy aims to minimize operational disruption, safeguard customer data, fulfill statutory and contractual breach notification requirements, and continuously improve defensive postures.

2. Scope

This policy applies to:

- All information systems, cloud infrastructure on Amazon Web Services (AWS), production databases, container clusters (AWS ECS/Fargate), corporate networks, endpoints, and software applications owned, leased, or operated by Northwind Labs.

- All customer and business data processed, transmitted, or stored on behalf of customers and integration partners.
- All personnel—including full-time employees, part-time staff, contractors, advisors, and temporary staff—who discover, report, or respond to suspected security anomalies.

3. Roles and Responsibilities

SOC 2: CC1.3, CC7.3

The Incident Response Team (IRT) executes security triage, technical containment, and stakeholder communications according to defined functional roles:

ROLE	PRIMARY ASSIGNED TITLE	RESPONSIBILITIES DURING INCIDENT	DESIGNATED ALTERNATE
Incident Commander (IC)	Head of Security & Infrastructure	Directs the overall response effort, declares incident severity, coordinates cross-functional resources, authorizes high-impact containment actions, and manages executive communications.	VP of Engineering
Technical Response Lead	Lead Cloud Infrastructure Engineer	Leads forensic investigation, log analysis across AWS CloudTrail and Datadog, containment execution, vulnerability eradication, and system restoration.	Senior Backend Engineer
Communications Lead	Chief Executive Officer (CEO)	Manages external communications with impacted customers, regulatory authorities, external legal counsel, cyber insurers, and the public.	Head of Security & Infrastructure
Documentation Lead / Scribe	On-Duty Site Reliability Engineer	Maintains the real-time chronological timeline log, captures command history, preserves evidence artifact IDs, and logs decision rationales.	Technical Response Lead
All Personnel	All Staff	Immediately report any suspected security anomaly, credential exposure, lost company device, phishing attempt, or unauthorized access event to the Incident Response Team via Slack or PagerDuty.	N/A

4. Policy Statements

4.1 Incident Definition and Event Distinction

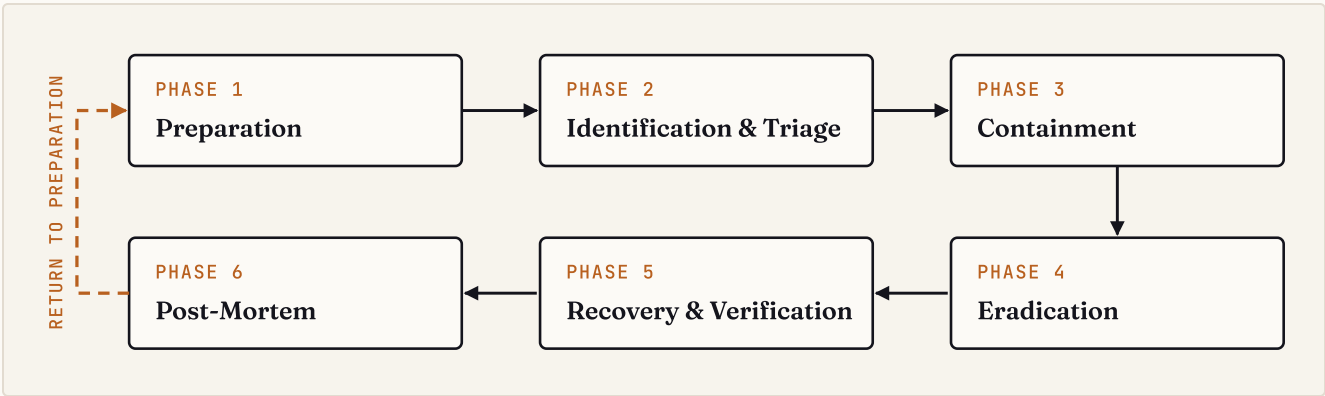
SOC 2: CC7.2, CC7.3

- **Security Event:** Any observable occurrence in an information system, network, or cloud service (e.g., routine firewall blocks, transient authentication failures, or vulnerability scanner telemetry). Security events represent standard operational data points and do not inherently constitute a security incident.
- **Security Incident:** An adverse event or series of events that actually or potentially jeopardizes the confidentiality, integrity, or availability of Northwind Labs information systems, customer environments, or data, or constitutes a documented violation of security policies, acceptable use standards, or applicable legal obligations. Any security event meeting these criteria shall immediately be declared and handled as a security incident.

4.2 Incident Response Methodology and Operational Governance

SOC 2: CC7.3, CC7.4

Northwind Labs shall maintain and execute an incident response program governed across six disciplined phases:



To ensure strict operational discipline and consistent policy governance, the following requirements shall apply across all lifecycle phases. Detailed operational step-by-step procedures, technical execution commands, and playbooks are maintained separately in the *Incident Response Runbook*.

- **Phase 1: Preparation Requirements:**

- Centralized audit logging shall be enabled and maintained across all AWS infrastructure (AWS CloudTrail, Amazon CloudWatch) and Datadog, with immutable log archives retained in encrypted Amazon S3 buckets protected by S3 Object Lock.
- Continuous 24/7/365 on-call rotation schedules shall be maintained within PagerDuty to guarantee immediate availability of primary and secondary incident responders.
- Pre-configured, restricted communications infrastructure (including dedicated private Slack channels and out-of-band communication bridges) shall be maintained in a constant state of readiness.
- Offline, encrypted emergency contact rosters containing verified contact information for all IRT members, executive leadership, external legal counsel, cyber insurance carriers, and AWS enterprise support shall be reviewed and verified quarterly.

- **Phase 2: Identification and Mandatory Reporting Requirements:**

- All personnel who detect, observe, or suspect a security anomaly, unauthorized access attempt, credential compromise, or device loss shall report the event immediately via the designated Slack command (`/incident`) or by paging the on-call engineer in PagerDuty.
- The Incident Commander shall evaluate incoming reports, validate the anomaly, assign a formal severity level in accordance with Section 5, and declare an active incident where warranted.
- A centralized, timestamped chronological incident log shall be initiated for every declared incident to record all observations, technical decisions, responder actions, and evidence artifact references.

- **Phase 3: Containment and Evidence Preservation Requirements:**

- Upon declaring a Sev 1 or Sev 2 incident, containment actions shall be prioritized to isolate affected systems and arrest lateral movement before attempting eradication or permanent remediation.
- Containment strategies shall balance active threat arrest with the preservation of volatile digital evidence. Before modifying or terminating affected resources, responders shall secure point-in-time forensic snapshots (e.g., Amazon EBS snapshots, memory dumps where feasible, and network flow records) and store them in an access-restricted forensic evidence repository.

- Emergency isolation controls—including revoking active Okta SSO sessions, invalidating temporary AWS IAM credentials, enforcing perimeter Cloudflare WAF/Zero Trust blocks, and applying restrictive quarantine security groups—shall be authorized for immediate execution by the Incident Commander.

- **Phase 4: Eradication and Remediation Requirements:**

- The underlying vulnerability, configuration defect, or threat vector enabling the incident shall be identified and eliminated prior to restoring standard operations.
- All potentially exposed or compromised credentials, API keys, database secrets, and cryptographic certificates shall be rotated across AWS Secrets Manager and 1Password Business.
- Affected software or containerized environments shall be rebuilt from verified, uncompromised source code and deployed exclusively through automated GitHub Actions CI/CD deployment pipelines.
- Automated vulnerability and credential scanning shall be conducted to verify that the attack vector is closed and no secondary backdoors or persistence mechanisms remain.

- **Phase 5: Recovery and Verification Requirements:**

- Production services and datastores shall be restored from clean, verified infrastructure-as-code (Terraform) manifests and validated backup snapshots preceding the compromise timestamp.
- Restored systems shall undergo functional verification, integrity testing, and security health checks prior to reintroducing customer production traffic.
- Heightened monitoring, elevated alerting sensitivity, and continuous log inspection shall remain active on all recovered environments for a mandatory minimum observation period of thirty (30) consecutive calendar days following recovery.

5. Severity Classification and Service Level Commitments

SOC 2: CC7.3

All confirmed security incidents shall be classified according to the severity matrix below. Personnel and responders shall adhere to the mandatory response SLAs, containment milestones, and notification pathways defined for each classification tier:

SEVERITY LEVEL	CLASSIFICATION CRITERIA & IMPACT	EXAMPLE QUALIFYING SCENARIOS	RESPONSE SLA	TARGET CONTAINMENT SLA	REQUIRED ESCALATION PATH
Sev 1–Critical	Catastrophic impact. Confirmed compromise of production customer data, active ransomware, or complete service outage affecting all tenants.	Production database exfiltration; compromised AWS root credentials; active supply chain breach; uncontained privilege escalation in production clusters.	Within 15 minutes (24/7 on-call page via PagerDuty)	Within 2 hours	Immediate automated page to Incident Commander, VP of Engineering, and CEO. Convene executive bridge. External customer notification within 24–48 hours.
Sev 2–High	Severe operational impact or potential data compromise without confirmed exfiltration. Critical infrastructure compromised or isolated tenant impacted.	Production host root compromise; unencrypted company laptop stolen with active session tokens; active volumetric denial-of-service attack; public S3 bucket exposure containing configuration backups.	Within 30 minutes	Within 6 hours	Page Incident Commander and Technical Response Lead via PagerDuty. Notify executive management via <code>#incident-war-room</code> . If customer data is confirmed affected, notify affected customers in writing within 24–48 hours per Section 6.
Sev 3–Medium	Moderate impact. Isolated system compromise, policy violation, or elevated security vulnerability without exposure of sensitive customer data.	Developer workstation infected with non-propagating malware; single employee phishing credential entry immediately revoked; misconfigured internal IAM permission set; high-severity dependency vulnerability with public exploit.	Within 2 business hours	Within 24 business hours	Notify Technical Response Lead and on-call engineer via Slack (<code>#security-alerts</code>). Log Jira incident tracking ticket.

SEVERITY LEVEL	CLASSIFICATION CRITERIA & IMPACT	EXAMPLE QUALIFYING SCENARIOS	RESPONSE SLA	TARGET CONTAINMENT SLA	REQUIRED ESCALATION PATH
Sev 4—Low	Minimal or theoretical risk. Security anomaly contained by automated defense layers, or routine compliance scan finding.	Minor third-party dependency vulnerability alert without active exploit; unsuccessful brute-force attack blocked by Cloudflare rate limiting; internal accidental misdirection of non-sensitive file.	Within 8 business hours	Within 72 business hours	Queue in Jira Security backlog for standard triage. Reviewed during weekly security engineering sync.

Tailoring Note for Startups: Clear severity definitions and published containment SLAs (such as Sev 1 response within 15 minutes and containment within 2 hours) relate to SOC 2 CC7.3 and CC7.4. Northwind Labs' policy defines binding escalation thresholds and a mandatory 5-day postmortem SLA to give documented, verifiable operational evidence.

6. Notification and Reporting Requirements

SOC 2: CC7.3, CC2.3

- **Confidentiality and Communication Discipline:** All personnel are strictly prohibited from discussing ongoing security incidents, breach investigations, or forensic findings outside authorized IRT communication channels. Under no circumstances shall personnel comment on active incidents via social media, public forums, or unencrypted personal channels.
- **Internal Executive and Governance Escalation:** The Incident Commander shall formally brief the CEO, VP of Engineering, and Board of Directors within two (2) hours of confirming a Sev 1 incident, and within four (4) hours of confirming a Sev 2 incident.
- **Out-of-Band Communications:** If internal corporate email or Slack workspaces are suspected of compromise, unavailable, or untrusted, the Incident Response Team shall immediately transition all coordination and communications to an approved, encrypted out-of-band platform (Signal).
- **Contractual Customer Breach Notification:** In the event of confirmed unauthorized access to, exposure of, or exfiltration of customer confidential data or personal information:
 - Northwind Labs shall formally notify affected customer organizations in writing without unreasonable delay, and in all cases within **twenty-four (24) to forty-eight (48) hours** of confirmed compromise, in strict compliance with executed Master Services Agreements (MSAs) and Data Processing Agreements (DPAs).

- Customer notifications shall include, at minimum: an executive summary of the event, categories and volume of records compromised, immediate containment and remediation measures enacted, recommendations for customer-side mitigation, and designated IRT contact channels.
- **Statutory and Regulatory Notification (GDPR / UK GDPR):** Where an incident involves confirmed or probable compromise of personal data pertaining to European Economic Area (EEA) or United Kingdom (UK) data subjects:
 - The Communications Lead and external legal counsel shall notify the relevant supervisory authority (e.g., the Irish Data Protection Commission or UK Information Commissioner's Office) within **seventy-two (72) hours** of becoming aware of the breach, pursuant to Article 33 of GDPR, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
 - Affected enterprise customers acting as data controllers shall be notified without undue delay and within **forty-eight (48) hours** to ensure fulfillment of their independent controller notification obligations.
- **Payment Processor Notification:** Northwind Labs utilizes Stripe (PCI DSS Level 1 Service Provider) for payment processing and does not store, process, or transmit raw cardholder data. In the event of a security incident affecting billing integrations, webhook endpoints, or payment secrets, Northwind Labs shall notify Stripe within twenty-four (24) hours and comply with required payment card brand operating rules.

7. Post-Incident Review Requirements

SOC 2: CC7.3, CC7.4

- **Mandatory Blameless Postmortem:** For all Sev 1 and Sev 2 incidents, the Incident Commander shall convene a formal, blameless post-incident review meeting within **five (5) business days** of official incident closure.
- **Post-Incident Review Report Deliverables:** The IRT shall author a comprehensive postmortem report containing:
 - A rigorous root-cause analysis conducted utilizing the Five Whys methodology.
 - A verified chronological timeline detailing detection, initial response, escalation milestones, containment, and ultimate recovery.

- An assessment of total operational impact, including system downtime, affected customer accounts, volume of exposed data records, and estimated business impact.
- A structured corrective action plan detailing technical and organizational preventions, with each item assigned a named engineer, priority, and binding completion deadline in Jira Software.
- **Governance and Action Item Closure:** Postmortem remediation action items shall be incorporated directly into the engineering backlog and reviewed during weekly engineering sprint planning until verified and closed.

8. Testing and Incident Simulation Requirements

SOC 2: CC7.4

- **Annual Simulation Requirement:** The Head of Security & Infrastructure shall plan and conduct a structured incident response tabletop exercise at least once every twelve (12) months.
- **Scenario Realism:** Simulation scenarios shall model realistic threat vectors relevant to Northwind Labs' operating profile, including cloud credential theft, ransomware on endpoints, public S3 bucket exposure, and supply-chain dependency compromise.
- **Continuous Improvement:** Following every tabletop exercise, the IRT shall document lessons learned and update this policy, the *Incident Response Runbook*, and technical monitoring configurations accordingly within thirty (30) calendar days.

9. Enforcement

Compliance with this Incident Response Policy is mandatory for all Northwind Labs personnel and contractors. Deliberately withholding knowledge of a security anomaly, intentionally tampering with forensic audit trails, or failing to participate in incident triage constitutes a severe violation resulting in disciplinary action up to and including immediate termination of employment or contract, and potential civil or criminal legal liability.

10. Exceptions

Emergency deviations from standard operational workflows during an active incident (e.g., bypassing standard CI/CD deployment gates to deploy an emergency hotfix) may be authorized exclusively by the Incident Commander or VP of Engineering, provided such actions are necessary to preserve service availability or protect customer data. Any emergency deviation must be recorded in the active incident log and formally documented in the postmortem report.

11. Review Cadence

This Incident Response Policy shall be reviewed, evaluated, and updated at least annually by the Head of Security & Infrastructure, and immediately following any major (Sev 1) security incident to incorporate operational learnings, architecture changes, and statutory updates.

12. Revision History

VERSION	DATE	AUTHOR / ROLE	SUMMARY OF CHANGES
1.0	October 1, 2026	Head of Security & Infrastructure	Initial policy adoption