Incident Management and Response Policy

Organization: Caliber Technologies Inc. (Calimatic Mail) **Document Version:** 1.0 **Effective Date:** February 14, 2026 **Last Reviewed:** February 14, 2026 **Classification:** Confidential

---

1. Purpose

This policy defines procedures for detecting, responding to, containing, and recovering from security incidents affecting the Calimatic Mail platform and its users.

2. Scope

This policy covers all security incidents affecting:

- Calimatic Mail production infrastructure
- User data (PII, email content, OAuth tokens)
- Third-party integration data (Zoom, Google)
- Service availability and integrity

3. Incident Classification

3.1 Severity Levels

Severity	Description	Examples
SEV-1 (Critical)	Active data breach, complete service outage, or active exploitation	Unauthorized access to user data, database compromise, OAuth token leak
SEV-2 (High)	Partial service degradation, confirmed vulnerability under exploitation	DDoS attack affecting availability, brute-force attack bypassing rate limits
SEV-3 (Medium)	Suspicious activity requiring investigation, no confirmed impact	Unusual authentication patterns, failed intrusion attempts, dependency vulnerability with production exposure
SEV-4 (Low)	Informational security events, no immediate risk	Automated scanning activity, low-severity dependency advisories

3.2 Incident Categories

- **Data Breach:** Unauthorized access to or disclosure of user data
- **Service Disruption:** Denial of service, system outage, or degraded performance
- **Account Compromise:** Unauthorized access to user or administrative accounts
- **Integration Compromise:** Unauthorized use of OAuth tokens or third-party API abuse
- **Infrastructure Compromise:** Unauthorized server access, container escape, or configuration tampering

4. Detection

4.1 Automated Detection

- **Application Logs:** Structured JSON logging of all API requests, authentication events, and errors, aggregated via Loki.
- **Rate Limiting Alerts:** Logging at 80% rate limit threshold and on limit exceed.
- **Health Checks:** Automated container health checks with restart on failure.
- **Metrics:** Prometheus metrics for request rates, error rates, and latency, visualized in Grafana dashboards.

4.2 Manual Detection

- Code review during development
- Periodic `npm audit` scans

- User reports via support@calimatic.app
- Third-party security researcher reports via security@calimatic.app

5. Response Procedures

5.1 Initial Response

Step	Action	Timeframe
1	**Detect and Acknowledge** - Confirm the incident and assign an incident lead	Within 1 hour (SEV-1/2), 4 hours (SEV-3/4)
2	**Classify** - Determine severity and category	Within 30 minutes of acknowledgment
3	**Notify** - Alert relevant team members	Immediately after classification
4	**Contain** - Take immediate steps to limit impact	Within 2 hours (SEV-1), 8 hours (SEV-2)

5.2 Containment

Depending on the incident type:

Data Breach:

- Revoke compromised OAuth tokens
- Rotate affected API keys and JWT secrets
- Block compromised accounts
- Isolate affected database records

Service Disruption:

- Activate rate limiting escalation
- Block offending IP addresses
- Scale infrastructure if needed
- Failover to backup services

Account Compromise:

- Force password reset on affected accounts
- Invalidate all active sessions
- Review audit logs for unauthorized actions
- Notify affected users

Integration Compromise:

- Revoke OAuth tokens for affected integrations
- Notify the integration provider (Zoom, Google)
- Disable the affected integration endpoint temporarily
- Rotate client secrets

5.3 Investigation

- Collect and preserve logs from all affected services.
- Identify the attack vector and timeline of events.
- Determine the scope of data affected.
- Document all findings in an incident report.

5.4 Recovery

- Restore services from known-good state.
- Deploy fixes for identified vulnerabilities.
- Re-enable disabled features after verification.

- Monitor for recurrence.

5.5 Communication

Internal:

- Engineering team is notified immediately for SEV-1/2.
- Regular status updates during active incidents.

External (User Notification):

- Users are notified if their data was compromised.
- Notification includes: what happened, what data was affected, what actions were taken, and recommended user actions.
- Notification timeframe: within 72 hours for data breaches (GDPR requirement).

Third-Party (Integration Providers):

- Zoom and Google are notified if their integration tokens or APIs were compromised.
- Coordination with provider security teams as needed.

6. Post-Incident Review

6.1 Post-Mortem

Within 5 business days of incident resolution:

1. **Timeline:** Detailed chronological account of the incident
2. **Root Cause:** Identification of the underlying cause
3. **Impact:** Assessment of data, users, and services affected
4. **Response Effectiveness:** Evaluation of detection and response times
5. **Lessons Learned:** What worked well and what can be improved
6. **Action Items:** Specific improvements with owners and deadlines

6.2 Improvements

Post-incident action items may include:

- Code fixes and security patches
- Infrastructure configuration changes
- Monitoring and alerting improvements
- Policy and procedure updates
- Additional security controls

7. Roles and Responsibilities

Role	Responsibility
Incident Lead	Coordinates response, makes containment decisions, communicates status
Engineering Team	Investigates, implements fixes, deploys patches
Operations	Monitors infrastructure, manages access controls, executes containment
Management	Authorizes communication, makes business decisions, resource allocation

8. Contact Information

Purpose	Contact
Security incidents	security@calimatic.app

User support	support@calimatic.app
Legal/compliance	legal@calimatic.app
Privacy inquiries	privacy@calimatic.app

9. Testing

- Incident response procedures are reviewed during post-mortems.
- Response playbooks are updated based on lessons learned.
- Team members are briefed on this policy upon onboarding.

10. Review Cycle

This policy is reviewed:

- Annually at minimum
- After every SEV-1 or SEV-2 incident
- When significant infrastructure changes occur
- When team structure changes

Approved by: Engineering Team, Caliber Technologies Inc. **Contact:** security@calimatic.app