# Incident Response Plan

Navwis Management ApS · Version 1.0 · April 2026

## SCOPE & OBJECTIVES

This plan governs the detection, containment, eradication, and recovery from security incidents affecting the EUSecureAI platform and its customers' data. It applies to all systems operated by Navwis Management ApS under the eusecureai.com domain.

Objectives: minimize damage and recovery time, protect customer data, meet GDPR Article 33 notification obligations where applicable, and improve defenses after each incident.

## SEVERITY CLASSIFICATION

- P1 — Critical: Active breach, data exfiltration, or complete service outage
- P2 — High: Suspected breach, partial outage, or confirmed significant vulnerability
- P3 — Medium: Degraded performance, isolated error spike, or minor vulnerability
- P4 — Low: Security observation with no immediate risk

## PHASE 1 — DETECTION & IDENTIFICATION

Monitoring sources:

- Sentry — real-time application error tracking
- PM2 logs — process-level error and crash detection
- OVH control panel — infrastructure and database alerts
- Customer reports — via security@eusecureai.com

Upon detection: record time of discovery, describe symptoms clearly, assign an initial severity level, and notify the response lead within 30 minutes for P1/P2 incidents.

## PHASE 2 — CONTAINMENT

Containment actions by severity:

- P1: Take affected service offline, revoke compromised credentials, block known attacker IPs
- P2: Isolate affected component, increase logging verbosity, restrict access scope
- P3/P4: Monitor closely, schedule remediation, no immediate downtime required

Document all actions taken with precise timestamps. Preserve logs and evidence — do not overwrite data that may be needed for investigation.

## PHASE 3 — ERADICATION

Remove the root cause before restoring service:

- Apply security patches or configuration fixes to affected systems
- Rotate all exposed credentials, API keys, and session secrets
- Verify the fix in a safe environment before re-enabling production
- Confirm no persistence mechanisms (backdoors, unauthorized accounts) remain

## PHASE 4 — RECOVERY

Restore service in a controlled, validated manner:

- Restore from OVH point-in-time backup if data integrity is in doubt
- Validate system integrity and data consistency before re-opening to users
- Monitor closely for 24 hours after full recovery

- Confirm with the full response team before declaring the incident closed

## PHASE 5 — POST-INCIDENT REVIEW

Complete within 5 business days of incident closure:

- Reconstruct a full timeline of events from logs and notes
- Identify root cause and all contributing factors
- Document what went well and what should be improved
- Update this plan if the incident revealed a gap in coverage
- Produce a written post-mortem report for all P1/P2 incidents

## COMMUNICATION PROTOCOL

Internal: The response lead notifies all relevant team members immediately. Status updates every 2 hours for active P1/P2 incidents until resolution.

Customers: Affected customers are notified by email within 72 hours of a confirmed breach, including the nature of the incident, data affected, actions taken, and any recommended actions for the customer.

Authorities: Where personal data is involved, Navwis Management ApS will notify the relevant supervisory authority within 72 hours per GDPR Article 33, unless the breach is demonstrably unlikely to result in a risk to individuals.

## CONTACTS

- Security incidents: security@eusecureai.com
- Privacy & GDPR: privacy@eusecureai.com
- General escalation: contact@eusecureai.com