Incident Response and Notification Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Information Security Officer (CISO)
Next Review Date: October 2026

1. Purpose

This policy defines Orbitel.ai’s structured approach to identifying, responding to, containing, and recovering from information security incidents and data breaches.
Its objectives are to:

- Minimize impact to systems, customers, and operations.
- Ensure timely notification to affected individuals and regulators.
- Strengthen systems through lessons learned and root cause analysis.

2. Scope

Applies to:

- All employees, contractors, and third parties handling Orbitel data or systems.
- All incidents that could affect the confidentiality, integrity, or availability of Orbitel’s infrastructure, data, or AI models.

3. Governance and Responsibilities

- **Incident Response Team (IRT):** Composed of members from Security, Legal, Compliance, and Engineering.
- **CISO:** Approves response procedures and oversees major investigations.

- **SOC Analysts:** Detect and triage potential threats.
- **Legal and Privacy Teams:** Coordinate notifications to customers, partners, and regulators.

4. Policy Statements and Process

a. Detection and Reporting

- All employees must report suspected incidents to the Security Operations Center (SOC) immediately.
- Automated monitoring tools detect anomalies, malware, and unauthorized access attempts 24/7.

b. Classification and Severity Assessment

Incidents are categorized as:

- *Low:* Minor internal security events (e.g., failed login attempts).
- *Medium:* Limited data exposure or localized service interruption.
- *High:* Confirmed data breach, major outage, or compromise of customer data.

c. Containment and Eradication

- Affected systems are isolated, credentials rotated, and malicious artifacts removed.
- Forensic evidence is preserved according to legal and regulatory requirements.

d. Recovery

- Systems are restored using verified clean backups.
- Post-restoration monitoring continues for at least 72 hours to ensure stability.

e. Communication and Notification

- Customers are notified promptly if their data is affected.

- Regulatory notifications follow statutory timelines (e.g., CERT-In within 6 hours; GDPR within 72 hours).

- All communications are clear, factual, and transparent.

f. Post-Incident Review

- A root cause analysis (RCA) is conducted within 10 business days of resolution.

- Recommendations are logged and tracked to closure through Orbitel's Corrective Action Process.

5. Compliance and Continuous Improvement

The IRT conducts quarterly tabletop exercises to test readiness.
This policy supports ISO 27001 A.5.25 and DPDP 2023 Section 8 requirements for breach notification.
Annual review ensures alignment with evolving threat landscapes and legal expectations.