NimbusTech Solutions, Inc.

Incident Response Plan (IRP)

ISO 27001:2022

Table Of Contents

1. Document Control

- **Document ID :** NT-ISMS-IRP-001
- **Version :** 1.0
- **Date :** August 15, 2025
- **Owner :** Laura Chen, ISMS Manager
- **Approved By :** Rajesh Patel, CISO

2. Purpose

The purpose of this Incident Response Plan is to establish a structural and consistent approach for managing information security incidents at NimbusTech Solutions, Inc. in alignment with ISO/IEC 27001:2022 Annex A.5.24-A.5.28.

3. Scope

The plan applies to all employees, contractors, IT systems, SaaS platforms, cloud services, and third-party vendors within NimbusTech's ISMS scope.

4. Definitions

- Event : Any observable occurrence in a system or network.
- Incident : A confirmed event that compromises confidentiality, integrity, or availability of information.
- Breach : An incident resulting in unauthorized disclosure of sensitive data.

5. Roles & Responsibilities

- CISO (Rajesh Patel) : Executive oversight, approves major incident decisions.
- ISMS Manager (Laura Chen) : Coordinates incident response process.
- IRT (Incident Response Team) : Includes IT, HR, Legal, Communications - responsible for executing this plan.
- All Employees : Must report suspected incidents immediately via the Helpdesk or Security Hotline.

6. Incident Response Lifecycle

6.1 Preparation

- Maintain IRT contact list.
- Conduct annual incident response training.
- Ensure monitoring/ logging systems (A.8.15, A.8.16) are active.

6.2 Identification

- Incidents detected via SIEM, monitoring tools, employee reports.
- Classify incidents as Low, Medium, High, Critical.

6.3 Containment

- Short-term: Isolate affected endpoints, disable compromised accounts.
- Long-term: Apply patches, block malicious IPs, strengthen configs.

6.4 Eradication

- Remove malware, malicious accounts, disable compromised accounts.
- Validate remediation before moving to recovery.

6.5 Recovery

- Restore systems from clean backups (A.8.10).
- Verify capacity and system availability (A.8.6).
- Monitor for re-occurence.

6.6 Lessons Learned

- Conduct post-incident review within 2 weeks.
- Update Risk Register, SoA, and controls as needed.
- Share findings with management review.

7. Incident Reporting & Classification

Severity	Description	Response Time	Escalation
Low	Minor security event, no impact	24 hours	ISMS Manager
Medium	Incident affecting limited systems	12 hours	ISMS Manager + IRT
High	Major impact on operations or sensitive data	4 hours	CISO + IRT
Critical	Widespread outage or major data breach	Immediate	CEO + Regulators

8. Communication Plan

- Internal: Staff notified via intranet/ email. Execs briefed by CISO.
- External: Clients informed within SLA timelines. Regulators notified within 72 hrs. If PII breach (per GDPR).
- Media: Only Communications Manager authorized to speak publicly.

9. Evidence Collection & Forensics

- Logs, memory dumps, and forensic artifacts preserved.
- Chain of custody maintained by IT Security Analyst.
- Evidence retained for at least 1 year, or longer if required by legal, contractual, or regulatory obligations.

10. Linkages to ISMS

- ISMS Policy (A.5.1): Commitment to protecting info.
- SoA (A.5.7, A.8.15, A.8.16): Controls for monitoring and logging.
- Risk Register: Incidents feed into risk reassessment.
- Risk Methodology: Defines process for updating residual risks.

11. Review & Approval

This plan will be reviewed annually or after a major incident.

Approved By:
Rajesh Patel - CISO
Date: August 15, 2025