INCIDENT MANAGEMENT POLICY

INLINE WITH ISO 27001:2022 & SOC 2

Prepared By :

MINISTRY OF MOS SECURITY

Document Name	Incident Management Policy
Classification	Internal Use Only

Document Management Information

Document Title:	Incident Management Policy
Document Number:	ORGANISATION-INC-MNM-POL
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

Document Name	Incident Management Policy
Classification	Internal Use Only

Contents

Document Name	Incident Management Policy
Classification	Internal Use Only

1. Purpose

The purpose of this Incident Management Policy is to establish a structured and repeatable approach to detecting, reporting, managing, and resolving information security incidents that may affect the confidentiality, integrity, or availability of [ORG NAME]'s information assets, systems, and services.

This policy ensures that:

- All actual or suspected security events and incidents are **identified, classified, and escalated** in a timely manner.
- Roles and responsibilities for incident response are clearly defined, enabling **effective coordination** across teams.
- Appropriate actions are taken to **contain, investigate, resolve, and recover** from incidents while minimizing impact.
- **Evidence is collected and preserved** in a manner that supports forensic investigations and legal proceedings.
- Lessons learned are analysed to enable **continuous improvement** of security controls and reduce recurrence.
- The organization meets its **compliance obligations** under standards such as ISO/IEC 27001, SOC 2, and applicable regulatory frameworks (e.g., GDPR, DPDP Act, HIPAA, etc.).

By enforcing this policy, [ORG NAME] aims to build a resilient and responsive incident management capability that supports operational continuity, customer trust, and regulatory compliance.

2. Scope

This policy applies to all **information security events and incidents** that could impact [ORG NAME]'s:

- Digital and physical information assets
- IT infrastructure and cloud environments
- Business applications and services
- Data (including PII, PHI, financial, and customer data)
- Employees, contractors, vendors, and third-party service providers

Specifically, this policy covers:

- All **employees, interns, consultants**, and **third parties** with access to [ORG NAME] systems or data
- All **owned, leased, or managed IT systems**, whether hosted on-premises, in the cloud, or at vendor sites
- All incidents occurring in **production, development, test, and DR environments**
- All business functions, including IT, DevOps, Security, HR, Legal, Customer Support, and Compliance

The policy is applicable to a wide range of incidents, including but not limited to:

- Unauthorized access attempts or data breaches
- Malware infections, ransomware, or phishing attacks
- Denial of service (DoS/DDoS) incidents
- Loss or theft of devices or data
- System outages or integrity failures
- Misuse of privileged accounts or insider threats
- Violations of data protection or compliance obligations
- Third-party or vendor-related security incidents

Exclusions: Minor helpdesk issues, application bugs not posing a security risk, or isolated outages that don't involve data or security breach are out of scope for this policy and are handled via the standard IT ticketing system.

3. Objectives

The primary objectives of this policy are to establish a **systematic and proactive framework** for managing information security incidents in a way that protects [ORG NAME]'s assets, supports business continuity, and enables regulatory compliance.

Specifically, the objectives are to:

- **Enable Early Detection and Reporting**

Establish mechanisms for timely detection, identification, and reporting of actual or suspected security incidents by employees, contractors, and third parties.

- **Define Clear Roles and Responsibilities**

Assign accountability and authority for managing each phase of the incident lifecycle — from triage to resolution — across business, IT, security, and compliance functions.

- **Standardize the Incident Response Lifecycle**

Provide structured procedures for logging, classifying, investigating, escalating, containing, mitigating, and recovering from incidents.

- **Ensure Accurate Tracking and Documentation**

Maintain detailed records of incident status, timelines, communications, evidence, impact, and remediation efforts to support audits and legal obligations.

- **Minimize Business and Customer Impact**

Limit the operational, reputational, financial, legal, and regulatory consequences of incidents through swift containment and effective response.

- **Preserve Digital Evidence**

Ensure that forensic evidence is collected, handled, and retained in a secure, tamper-proof manner to support legal and compliance requirements.

- **Enable Continuous Learning and Improvement**

Derive lessons learned from incident analysis to strengthen controls, update risk assessments, refine processes, and train stakeholders.

- **Support Legal, Regulatory, and Contractual Compliance**

Meet obligations under ISO 27001, SOC 2, GDPR, DPDP Act, customer contracts, and other relevant frameworks or industry mandates.

4. DEFINITIONS & TERMINOLOGY

Term	Definition
Information Security Event	An identified occurrence that indicates a possible breach of security policy, failure of controls, or a previously unknown situation (e.g., alert, anomaly).
Information Security Incident	A single event or a series of events that has been confirmed to compromise the confidentiality, integrity, or availability of information assets or services.
Major Incident	A high-severity incident causing significant impact to business operations, regulatory exposure, or customer-facing services.
Incident Response (IR)	The coordinated activities to detect, assess, contain, eradicate, recover from, and learn from a security incident.
Incident Handler	An individual or team responsible for managing specific aspects of incident response activities.
Root Cause Analysis (RCA)	A systematic process to determine the fundamental reasons why an incident occurred.
Impact	The extent of damage or disruption caused by an incident, measured in operational, financial, reputational, or regulatory terms.
Likelihood	The probability of an incident occurring, based on threat exposure and vulnerability levels.
Chain of Custody	A process that ensures the integrity and traceability of evidence collected during incident investigations, maintaining admissibility in legal cases.

Forensic Evidence	Digital artifacts (e.g., logs, memory dumps, traffic captures) that may support investigation, legal action, or disciplinary procedures.
Playbook	A predefined, scenario-specific response guide outlining steps to be taken during particular types of incidents (e.g., phishing, ransomware).
Security Operations Center (SOC)	The internal or outsourced team responsible for continuous security monitoring, alerting, and first-level incident triage.
SIEM (Security Information and Event Management)	A platform that aggregates and analyzes logs, events, and alerts to support incident detection and investigation.
False Positive	An alert or event flagged as suspicious or malicious but later determined to be harmless or benign.

5. GOVERNANCE & RESPONSIBILITIES

Effective incident response requires **cross-functional collaboration** between technical, business, legal, and compliance teams. The following roles are responsible for the governance, execution, oversight, and continuous improvement of the incident management process:

5.1 Information Security Governance Committee (ISGC)

Role: Strategic oversight and governance of the incident management framework.

- Approves this policy and all associated procedures, templates, and tools
- Reviews critical or high-impact incidents and their resolution effectiveness
- Approves updates to escalation matrix, response plans, and thresholds
- Ensures alignment with business continuity, risk, and compliance strategies

5.2 Chief Information Security Officer (CISO)

Role: Executive leadership of incident response governance.

- Owns the incident management policy, lifecycle, and metrics
- Ensures organizational readiness for emerging threats and attack vectors
- Reports major incident summaries to senior leadership and board (if required)
- Supports compliance and audit reporting related to incidents

5.3 Information Security Team / CSIRT

Role: Lead responders, coordinators, and investigators for security incidents.

- Monitors alerts and threat intelligence to detect incidents early
- Leads triage, classification, containment, and response activities
- Coordinates forensic investigations and evidence handling
- Maintains incident logs, timelines, playbooks, and RCA documentation
- Communicates with Legal, HR, DevOps, and affected teams

5.4 IT Operations / DevOps

Role: Technical support for investigation, recovery, and containment.

- Supports incident triage, patching, and infrastructure isolation
- Provides logs, system snapshots, and access to affected environments
- Assists in restoration of services after incident containment
- Validates fixes and conducts post-incident technical reviews

5.5 Legal / Compliance Team

Role: Regulatory and contractual risk management.

- Determines whether incidents trigger legal or contractual notification obligations

- Coordinates communication with regulators and customers (as needed)
- Reviews liability, breach notification, and indemnity clauses
- Supports e-discovery and litigation readiness during investigations

5.6 Data Protection Officer (DPO)

Role: Privacy incident oversight.

- Assesses personal data breach severity under DPDP Act, GDPR, etc.
- Coordinates notification to Data Principals and Authorities
- Ensures privacy-by-design principles are revalidated post-incident
- Reviews third-party DPAs for breach timelines and escalation duties

5.7 Business Unit Heads / Application Owners

Role: Functional and application-specific impact management.

- Identify operational impact of incidents within their domain
- Validate business recovery timelines and user communications
- Support root cause analysis and control improvements
- Coordinate temporary workaround approvals (if needed)

5.8 SOC / MSSP (if applicable)

Role: First-level monitoring and alert escalation.

- Monitors SIEM, IDS, firewalls, and endpoint alerts
- Performs initial triage and forwards qualified incidents to InfoSec/CSIRT
- Escalates per runbooks or contractual SLAs
- Supports evidence preservation and enrichment

5.9 All Employees, Contractors & Third Parties

Role: Frontline event reporters.

- Promptly report any suspicious activity, data loss, or system anomalies
- Cooperate with incident responders and investigators
- Attend periodic awareness and phishing simulation programs
- Follow policy and acceptable use guidelines to prevent incidents

6. INCIDENT RESPONSE LIFECYCLE

The incident response lifecycle at [ORG NAME] follows a structured, repeatable process that ensures timely, consistent, and coordinated action in response to information security incidents. Each phase of the lifecycle is governed by defined responsibilities, communication protocols, and documentation requirements to support regulatory, contractual, and audit expectations.

Lifecycle Phases Overview

Phase	Description
1. Detection & Reporting	Identifying and capturing the incident via alerts, user reports, or threat intel
2. Triage & Classification	Assessing incident type, scope, severity, and business impact
3. Containment	Limiting the spread or damage of the incident (temporary and long-term containment)
4. Eradication	Removing root cause, malicious actors, or infected components
5. Recovery	Restoring systems, services, and verifying integrity
6. Root Cause Analysis (RCA)	Understanding how the incident occurred and what control(s) failed
7. Lessons Learned	Capturing insights, updating controls, and sharing recommendations
8. Closure	Final review, documentation, and approval of resolution and evidence

6.1 Detection & Reporting

- Security events are detected via SIEM, EDR, IDS/IPS, firewalls, user reports, or vendors.
- Events are logged and validated as incidents using the classification matrix.
- The incident is formally entered into the **Incident Management System (IMS)**.

6.2 Triage & Classification

- CSIRT or Security Team reviews logs, alerts, or user input.
- Assesses **scope, impact, and urgency** based on predefined criteria.
- Assigns a **Severity Level (P1–P4)** and triggers initial containment actions.
- If the incident involves **PII, financial loss, third-party systems, or regulatory implications**, Legal, DPO, and Risk teams are notified.

6.3 Containment

Short-Term Containment:

- Block IPs/domains
- Disable compromised accounts
- Isolate infected systems or containers

Long-Term Containment:

- Apply patches
- Disable vulnerable services
- Segregate affected networks

Actions are carefully logged, with forensic integrity maintained.

6.4 Eradication

- Remove malware, artifacts, or unauthorized configurations
- Validate backups, restore clean states
- Ensure external access or persistence mechanisms are removed
- Re-image systems if required

Root cause indicators are documented, and validation testing is initiated.

6.5 Recovery

- Systems are brought back online gradually, following **BCP/DR plans** if applicable.
- Monitor post-incident behaviours for anomalies.
- Coordinate **UAT** or **business validation** with application owners.
- Ensure controls (MFA, logging, segmentation) are re-enabled before go-live.

6.6 Root Cause Analysis (RCA)

- RCA is mandatory for **High/Critical (P1/P2)** incidents.
- Techniques: 5 Whys, Fishbone Diagram, Fault Tree Analysis.
- Focus on:
    - Technical root cause (e.g., unpatched server)
    - Process failure (e.g., missing alerts, bad firewall rule)
    - Human error (e.g., phishing click, policy bypass)

RCA Reports must be completed within **5–10 business days** post-incident.

6.7 Lessons Learned

- A **Post-Incident Review (PIR)** is conducted within **7–14 days** for high-severity incidents.
- Attendees: Security, IT, impacted business units, compliance, and vendors (if involved)
- Outcomes include:
    - Policy/procedure updates
    - Tooling improvements
    - Additional training needs
    - Control enhancements

6.8 Incident Closure

- Incident can only be closed when:
    - Resolution has been verified by InfoSec + Business Owner
    - RCA and evidence are documented
    - CAPA items are logged or assigned
    - Approvals are recorded in IMS

Closure status is updated in dashboards and included in **MRM Reports**.

7. INCIDENT IDENTIFICATION AND REPORTING

Timely identification and reporting of information security events is critical to minimizing the impact of potential incidents and enabling effective response. All employees, vendors, contractors, and system users must be aware of how to detect and report suspicious activities, security violations, or incidents.

7.1 Sources of Incident Detection

Security incidents can be detected through a variety of sources including:

Source	Examples
Employees / Users	Reporting phishing emails, suspicious activity, lost devices, or unauthorized access
SOC / SIEM Tools	Automated alerts from security tools (e.g., intrusion detection, anti-virus, firewall logs)
DevOps / IT Monitoring	System performance anomalies, unauthorized configuration changes
Vulnerability Scans	Discovery of exploitable systems or insecure applications
Penetration Testing	External testers simulating real-world attacks
Threat Intelligence Feeds	Indicators of compromise (IOCs) or advisories from CERT-IN, ISACs, etc.
Third Parties / Vendors	Notification of breaches or issues in connected systems or services
Customers or Regulators	External complaints, legal notices, or breach notifications

7.2 Employee and Third-Party Responsibilities

All employees, contractors, and vendors must:

- Immediately report any suspected or confirmed incidents via designated channels
- Not attempt to investigate or suppress the issue on their own

- Preserve the current state of affected systems (do not reboot, delete logs, or tamper)
- Maintain confidentiality and avoid sharing incident details externally or on social platforms

7.3 Reporting Channels

Channel	Availability
Email	incident@yourdomain.com
Hotline / Phone	[Insert Emergency Hotline]
Internal Portal / Ticket System	[Insert Service Desk URL or App]
Walk-in / In-person	Information Security / SOC Room

7.4 Anonymous Reporting (Optional)

[ORG NAME] may also provide an **anonymous reporting channel** for whistleblower-style disclosures, including:

- Reporting of insider threats
- Policy violations without fear of retaliation
- Third-party security malpractice or negligence

7.5 Initial Incident Report Template

When reporting an incident, the following **minimum details** should be captured:

- Date and time of observation
- Reporter's name and contact details (unless anonymous)
- Description of what was observed
- Affected systems, applications, or users
- Any screenshots, error messages, or logs (if available)
- Immediate actions taken (if any)

7.6 Awareness and Enablement

- Periodic **training sessions, phishing simulations**, and **awareness campaigns** will be conducted to help employees recognize common incident patterns (e.g., suspicious URLs, social engineering tactics).

- Onboarding for new hires and vendors shall include orientation on how to report incidents securely and promptly.

8. INCIDENT LOGGING AND TRACKING

To ensure visibility, accountability, and continuous improvement, all information security incidents must be **formally recorded and tracked** in a centralized system. The logging and tracking process ensures consistent documentation, prioritization, response coordination, compliance reporting, and post-incident analysis.

8.1 Centralized Incident Logging Mechanism

[ORG NAME] shall maintain a **centralized and access-controlled Incident Management System (IMS)** that integrates with:

- **Security tools** (e.g., SIEM, IDS/IPS, EDR, firewalls, threat intel feeds)

- **ITSM platforms** (e.g., ServiceNow, Jira, Freshservice)

- **DevOps/Cloud pipelines** (e.g., GitHub, Jenkins, Kubernetes events)

- **Third-party SOC/MSSP alert dashboards**

- **Risk register and GRC platforms** (for risk-mapped incidents)

All incident tickets shall be **timestamped**, assigned a **unique identifier**, and accessible only to authorized responders and governance stakeholders.

8.2 Incident Log Attributes

Every incident entry shall contain detailed and standardized fields. The minimum attributes include:

Field Name	Description
Incident ID	Unique, system-generated tracking number
Incident Title	Short and descriptive title summarizing the incident

Document Name	Incident Management Policy
Classification	Internal Use Only

Field Name	Description
Date/Time Reported	Timestamp of when the incident was first observed or reported
Date/Time Detected	Timestamp when alert or system first flagged the anomaly
Reporting Source	Method or team that raised the alert (e.g., user, SOC, SIEM, 3rd party)
Reported By	Name, email, and department (if internal); can be anonymous if policy permits
Type of Incident	Classification (e.g., data breach, ransomware, insider threat, system misconfiguration)
Severity Level	Assigned based on impact and urgency criteria (e.g., P1, P2, P3, P4)
Affected Assets / Applications	Systems, networks, applications, vendors, or data involved
Scope of Impact	Number of users affected, data records involved, geographies impacted
Business Units Impacted	Departments or teams experiencing disruption or risk
Regulatory Impact	Whether legal/compliance obligations (e.g., breach reporting) were triggered
Initial Description	What was observed, how it was identified, and early impact assessments
Response Team Assigned	CSIRT members, escalation owners, and external participants
Triage Actions Taken	Containment steps taken before escalation (e.g., blocking IP, disabling accounts)
Root Cause	Identified origin or reason behind the incident (to be filled post-investigation)

Field Name	Description
Evidence Captured	Whether logs, screenshots, memory dumps, or traffic captures were preserved
Status	Open, Under Investigation, Contained, Resolved, Closed, Reopened
Linked Tickets or Incidents	Other relevant cases from DevOps, HR, BCP, or vendor incidents
Resolution Summary	Final remediation steps and system or control updates applied
Reviewer / Approver	Name and role of final reviewer closing the ticket
Lessons Learned	Actionable improvements derived from post-mortem or RCA
Follow-up Actions / CAPA	Control improvements, training needs, or long-term changes recommended

8.3 Tracking Status & Escalation Workflow

Each incident must move through a **defined status lifecycle**, with SLAs tied to each stage:

Status	Description
Open	Event logged and acknowledged
Under Investigation	Assigned to handler; root cause and scope under analysis
Contained	Incident impact isolated, damage controlled
Resolved	Remediation completed; services restored
Closed	RCA reviewed, documentation completed, and lessons learned logged
Reopened	New evidence or recurrence requires reanalysis

SLA timers must be attached to each stage (e.g., P1 incidents must be contained within 4 hours, resolved within 24 hours).

8.4 Integration with Risk and Compliance

- **High-severity or repeated incidents** must be mapped to the organization's **risk register**
- **Control failures** observed during incident response must trigger:
    - **Risk re-evaluation**
    - **Policy updates**
    - **Training plans**
- **Audit trails** must show:
    - Incident log completeness
    - Timeliness of response
    - Closure and approvals
    - Evidence retention and tagging

8.5 Evidence Management Linkage

Incident logs must reference **evidence repositories**, including:

- Log exports
- Screenshots or system memory
- Email headers and malware samples
- Chain of custody records (see Section 13)

All sensitive data should be securely stored in **encrypted and access-controlled locations**, with **restricted retention periods**.

8.6 Reporting and Dashboarding

The IMS should support:

- **Dashboards**: Open incidents, MTTR (mean time to respond), incident by category, etc.
- **Filters and Reports**: By severity, impacted asset, business unit, regulatory exposure
- **Exportable Reports**: For audits, MRM meetings, and external regulators

8.7 Retention & Archival

- All incident records must be retained for a **minimum of 5 years**
- Archived records must be stored in compliance with:
    - ISO 27001 retention policies
    - Legal and contractual data retention requirements
    - Secure backup practices for auditability

9. NCIDENT CLASSIFICATION & SEVERITY LEVELS

To ensure an appropriate and timely response, all reported security events must be **evaluated, classified, and assigned a severity level** based on business impact, data sensitivity, and potential risk. Classification enables the prioritization of incidents, allocation of resources, and triggering of appropriate escalation procedures.

9.1 Classification Categories

All incidents must be categorized into one of the following **incident types**:

Incident Type	Examples
Unauthorized Access	Compromised user credentials, privilege escalation, insider misuse
Malware / Ransomware	Virus, Trojan, spyware, ransomware, or worm detected on endpoint or server
Phishing / Social Engineering	Targeted phishing email, phone scam, impersonation, smishing
Data Breach / Leakage	Unauthorized disclosure or exposure of personal or confidential data
Denial of Service (DoS/DDoS)	Network flooding, application-layer attacks disrupting service availability
Loss or Theft of Assets	Stolen/lost laptops, USBs, paper files containing sensitive information

Incident Type	Examples
Policy or Compliance Violation	Misuse of systems, unauthorized software, failure to follow security policies
Third-Party Incident	Security breach or SLA violation by vendor affecting [ORG NAME] data/systems

9.2 Severity Levels

Each incident is assessed and assigned a **severity level** using the following matrix:

Severity Level	Description	Response Time	Examples
Critical (P1)	Major breach affecting confidential data, customer trust, or operations. Requires executive attention.	< 1 hour	Ransomware attack, major data breach, regulatory notification required
High (P2)	Incident with serious business impact, but no immediate legal or customer exposure.	< 4 hours	Privilege misuse, targeted phishing, malware with lateral movement
Medium (P3)	Limited or localized impact, contained or recoverable.	< 24 hours	Lost laptop with encrypted data, DDoS attack mitigated by firewall
Low (P4)	Minor violation or false positive; little to no impact on operations or data	< 3 business days	Policy violations, employee reports suspicious email, scan alerts

9.3 Classification Criteria

Incidents are scored using the following **impact criteria**:

Criteria	Key Considerations
Data Sensitivity	Was PII, PHI, financial, IP, or regulated data involved?

Criteria	Key Considerations
Business Impact	Was there downtime, revenue loss, or disruption to critical services?
Scope of Exposure	Number of users, systems, or geographies affected
Regulatory Exposure	Are regulatory notifications or legal obligations triggered?
Reputational Risk	Could this negatively affect customer trust or public image?
Recurrence Likelihood	Is this part of a trend or known campaign (e.g., phishing or zero-day)?

A structured **risk scoring model** or **playbook mapping table** can be used to consistently classify severity using quantitative thresholds (e.g., scoring 1–5 across criteria and calculating a total score).

10. ROOT CAUSE ANALYSIS AND REMEDIATION

Every security incident must be investigated beyond symptoms to identify its **underlying root cause(s)**. This enables the organization to correct not only the immediate issue but also address control weaknesses, improve resilience, and prevent recurrence.

10.1 Objectives of Root Cause Analysis (RCA)

- Understand how the incident occurred and why it was not prevented
- Identify **failures in controls, processes, or human behavior**
- Implement **corrective actions** to address the specific issue
- Recommend **preventive actions** to strengthen the broader environment
- Feed findings into **risk management, training, and compliance** processes

10.2 RCA Triggers

An RCA is **mandatory** for the following incident types:

- **Severity P1 or P2** incidents
- Any incident involving **data breach or customer data exposure**
- Repeated occurrence of the same type of incident

- Incidents involving **regulatory or legal reporting**
- When directed by Internal Audit, Legal, or Management

10.3 RCA Process Steps

1. **Assemble RCA Team**
    - CSIRT Lead
    - Application/System Owner
    - DevOps or Infra team
    - Legal / Compliance (if applicable)
2. **Define Timeline of Events**
    - Construct a **minute-by-minute log** of key events
    - Include alert timestamps, actions taken, and response delays
3. **Identify Root Causes**
   Use techniques such as:
    - **5 Whys**
    - **Fishbone Diagram (Ishikawa)**
    - **Fault Tree Analysis**
    - **Control Failure Mapping**
4. **Document Contributing Factors**
    - Human error
    - Process gap
    - Tool or alert failure
    - Lack of visibility or training
5. **Map to Control Domains**
    - ISO 27001 Annex A controls

- SOC 2 CC series
- Internal control framework

6. **Validate with Stakeholders**
   - Review RCA findings with impacted business teams and leadership

10.4 Corrective and Preventive Actions (CAPA)

Type	Definition
Corrective Action	Fixes the specific issue that caused the incident (e.g., patch system, revoke keys)
Preventive Action	Strengthens the environment to prevent similar future incidents (e.g., policy change, training, new tool deployment)

All CAPAs must be:

- Logged in the **Incident Management System** or **CAPA tracker**
- Assigned to a responsible owner with **due dates**
- Tracked until **closure** and **verified for effectiveness**
- Reported in **Management Review Meetings** and security dashboards

10.5 RCA Documentation Template

An RCA Report must include:

- Incident summary and impact
- Timeline of events
- Detailed root cause(s)
- Control failure mapping
- CAPA plan with timelines and owners
- Evidence references (logs, screenshots, etc.)
- Reviewer and approver sign-offs

RCA reports must be completed and uploaded within **5–10 business days** of incident closure and retained for **at least 5 years**.

11. POST-INCIDENT REVIEW AND LESSONS LEARNED

Following the resolution of any significant incident, [ORG NAME] shall conduct a **Post-Incident Review (PIR)** to formally assess the incident lifecycle, identify control gaps, and document organizational learnings. This process enables continuous improvement of security controls, incident response maturity, and business resilience.

11.1 Objectives of Post-Incident Review

- Validate whether the incident was managed as per policy and playbooks
- Review the **timeline, decisions, communications**, and **response effectiveness**
- Identify **what went well** and **what could have been improved**
- Translate insights into **policy, control, and awareness improvements**
- Enable cross-functional transparency and build response maturity

11.2 Applicability and Triggers

A PIR is **mandatory** for:

- Any incident classified as **Severity P1 or P2**
- Incidents involving **data breaches**, legal obligations, or customer impact
- **Recurring or avoidable incidents**
- Any incident requiring **Board, client, or regulator notification**
- At the discretion of the **CISO, DPO, or Risk Officer**

11.3 PIR Facilitation

- Led by the **CSIRT Lead / Incident Manager**
- Must be scheduled within **7–14 business days** after incident resolution
- Participants should include:
    - Information Security Team
    - IT/DevOps or Application Owners

- Business Units affected
- Legal, Compliance, Risk, and Audit (if relevant)
- Vendors or Third Parties (if involved)

11.4 PIR Meeting Agenda

Agenda Item	Description
Incident Overview	Summary of what happened, when, and how it was detected
Timeline Walkthrough	Step-by-step analysis of key response actions and time taken
Containment & Recovery Review	Discussion on the effectiveness of isolation and restoration steps
Root Cause & Control Failures	Review of technical, process, or human failures that enabled the incident
Communications Review	Analysis of internal and external communications, escalations, and transparency
RCA Findings & CAPAs	Validation of root cause report and corrective/preventive actions taken
Policy or Procedure Gaps Identified	Any required updates to existing processes, controls, or training
Lessons Learned	What worked, what didn't, and key takeaways for the organization
Action Items & Ownership	Formal assignment of any additional remediation, tracking, or documentation
Closing & Approvals	Final sign-off, action log confirmation, and PIR closure

---

11.5 Documentation and Reporting

- A **Post-Incident Review Report** must be documented and attached to the incident record

- Key lessons and recommendations must be:
    - Tracked in the **Security Action Tracker**
    - Shared during **Management Review Meetings (MRMs)**
    - Considered in **Risk Assessments**, **Training Programs**, and **Control Testing** cycles
- Where applicable, anonymized or generalized learnings should be shared across teams to build awareness and improve incident prevention organization-wide

11.6 Continuous Improvement Linkages

PIR outcomes must feed into:

- Updates to **incident response playbooks**
- Enhancements in **monitoring / alerting coverage**
- Review of **security awareness training** effectiveness
- Revisions to **vendor security requirements** if third-party was involved
- **Control design reviews** in relevant domains (e.g., access control, backup, DLP)

12. EVIDENCE COLLECTION & CHAIN OF CUSTODY

During the investigation and resolution of an information security incident, it is critical to collect, preserve, and manage digital evidence in a manner that ensures **integrity, admissibility, and traceability**. This protects [ORG NAME]'s ability to perform forensics, support legal proceedings, and comply with contractual and regulatory obligations.

12.1 Objectives of Evidence Handling

- Preserve data and artifacts relevant to the security incident
- Ensure the evidence is collected in a **secure, tamper-proof, and legally defensible** manner
- Maintain a verifiable **chain of custody** from identification to disposal
- Support internal root cause analysis, external investigations, or regulatory audits

12.2 Types of Evidence

Evidence Type	Examples
Log Files	Application logs, server logs, audit trails, SIEM exports
Network Traffic Captures	PCAP files, firewall traces, NetFlow data
Screenshots / Session Records	Screenshots of malicious activity, error messages, or alerts
System Snapshots	Memory dumps, disk images, configuration exports
Email Headers / Metadata	Full headers of phishing/malicious emails
Malware Samples	Infected binaries or scripts isolated during incident
Access Logs	Login activity, privileged account usage, identity provider logs
Endpoint Artifacts	Antivirus logs, EDR records, file hashes, registry changes

12.3 Evidence Collection Process

1. **Identify and Isolate Evidence Sources**
    - Use forensic tools or built-in logging systems
    - Isolate systems (e.g., VMs, laptops) if active compromise is suspected
2. **Use Forensically Sound Tools**
    - Use approved tools that do not alter timestamps or metadata
    - Examples: FTK Imager, Autopsy, Volatility, Wireshark
3. **Record Metadata for Each Artifact**
    - Include timestamp, location, collector name, hash value (SHA-256), system name, and storage location
4. **Hash Verification**
    - Compute and record **hash value** (e.g., SHA-256) to ensure evidence is not altered

5. **Store in Secured Repository**

    - Upload only to encrypted, access-controlled evidence drives (with retention policy)

    - Avoid transferring over unsecured channels or public cloud storage

12.4 Chain of Custody Log

All evidence must be accompanied by a **Chain of Custody Record**, tracking every transfer, access, and use of the artifact.

Field	Details Captured
Evidence ID	Unique reference number
Date / Time Collected	When the artifact was acquired
Collected By	Name and designation of evidence handler
Description	What the artifact is, and where it was sourced from
Hash (SHA-256)	To ensure integrity across handling steps
Stored At	Path or repository location (e.g., /forensics/INC2025-001/)
Transferred To	Next custodian (if any) with timestamp and reason
Access Logs	Every instance of access (person, purpose, time)
Disposal / Archive	Final status of evidence (retained, archived, or destroyed with reason)

The chain of custody form must be retained with the incident record for **at least 5 years**.

12.5 Evidence Handling Roles

Role	Responsibility
CSIRT / Security Analyst	Primary evidence collectors and loggers
IT Operations / DevOps	Provide access to servers, logs, and backups if needed

Role	Responsibility
Legal / Compliance	Review admissibility, legal holds, and disclosure boundaries
Incident Manager	Owns the evidence folder and chain of custody tracking

12.6 Retention and Disposal

- Evidence must be retained for a **minimum of 5 years**, or longer if required by:
    - Legal hold
    - Regulatory requirements (e.g., DPDP, GDPR, SOX)
    - Customer contracts
- Disposal must be:
    - **Documented** in the chain of custody record
    - **Approved** by Legal and Information Security
    - Performed using secure deletion techniques (e.g., DoD wipe, physical destruction)

13. ESCALATION PROCEDURES AND TIMELINES

Effective incident response requires **timely escalation** of information security incidents to appropriate personnel based on their severity, impact, and regulatory obligations. Escalation ensures that qualified stakeholders are involved early, enabling fast containment, communication, and decision-making.

13.1 General Escalation Principles

- **Severity-based escalation** must be followed according to the assigned classification (P1 to P4).
- All escalations must be **tracked, timestamped, and documented** in the Incident Management System (IMS).
- In case of uncertainty, escalation must be performed to the **next higher authority** without delay.

- Escalations must include relevant details such as: incident ID, scope, current impact, affected users/systems, and action taken so far.

13.2 Severity Levels & Escalation Matrix

Severity Level	Initial Response Time	Internal Escalation To	Notification to External Parties	Containment Target	Resolution Target
P1 - Critical	< 15 minutes	CISO, CTO, DPO, CEO, Legal, Business Head	Regulators, Customers, Auditors	< 1 hour	< 24 hours
P2 - High	< 1 hour	CSIRT Lead, CISO, Legal, Business Unit Head	On-demand based on impact	< 4 hours	< 48 hours
P3 - Medium	< 4 hours	Security Analyst, IT Manager, Application Owner	Optional (internal only)	< 1 business day	< 5 business days
P4 - Low	< 8 hours	Security Analyst / Service Desk Lead	Not required	< 3 business days	< 10 business days

13.3 Executive-Level Escalation

If an incident meets any of the following conditions, it must be escalated to **Executive Leadership** (CISO/CEO/Board):

- Impact to critical systems or national infrastructure
- Exposure of **sensitive customer or personal data**
- Likely to cause **regulatory reporting obligations** (e.g., DPDP Act, GDPR, HIPAA)
- **Reputational or media exposure**
- Cross-border breach involving third parties or vendors

13.4 Regulatory Escalation (Breach Notification)

If personal data, payment information, or regulated business data is exposed:

- The **DPO and Legal** team must assess reporting requirements
- Breach notifications must be sent **within defined timelines**:

Jurisdiction	Reporting Deadline
India (DPDP Act)	"As soon as possible" (TBD – subject to final rules)
EU (GDPR)	Within 72 hours
USA (varies by state)	Within 1–15 business days (depending on state law)
PCI-DSS	Immediately upon detection if cardholder data is involved

All such escalations must be coordinated and approved by the **DPO + Legal** teams.

13.5 Stakeholder Notification Matrix

Stakeholder Group	When Notified	By Whom
IT/Infra Team	Immediately for system-related incidents	Security / SOC
Legal & DPO	For data breaches, privacy, or third-party risk	CSIRT or CISO
Executive Management	For P1/P2 or incidents with business disruption	CISO or Risk Lead
Affected Customers / Clients	If client data is breached or services are impacted	Legal + Client Success
Vendors / Subprocessors	If the incident involves their system/data	Vendor Manager + Legal
Regulatory Authorities	As per breach notification rules	DPO + Legal
Internal Audit / Risk	For high-risk or control failure cases	CISO / Risk Officer

13.6 Escalation Triggers

Escalation is mandatory under the following circumstances:

- Incident remains **unresolved beyond target SLA**
- Additional systems or geographies become impacted
- **Media attention or legal action** is anticipated
- Affected users or third parties begin reporting issues
- Incident requires **cross-functional or third-party coordination**

14. COMMUNICATION & NOTIFICATION PROTOCOLS

Timely, accurate, and secure communication during an incident is critical to ensure coordinated response, stakeholder confidence, and compliance with legal or contractual obligations. This section defines the channels, roles, formats, and timing for incident-related communication.

14.1 Communication Objectives

- Prevent misinformation and panic through consistent, fact-based updates
- Keep internal and external stakeholders informed at appropriate levels
- Ensure communications are approved, traceable, and audit-ready
- Meet contractual, legal, and regulatory breach notification obligations
- Support post-incident debriefing, trust rebuilding, and lessons learned

14.2 Internal Communication Protocol

Audience	What is Communicated	Channel	Frequency
Security/CSIRT	Technical status, logs, containment actions	Ticketing system, Slack/SOC tools	Live / as events unfold
IT & DevOps	System impact, rollback status, technical support needs	Email, Jira, Teams, SMS	As required
Business Unit Heads	Functional impact, user impact, ETA for recovery	Email, Dashboard, Escalation calls	At major milestones / daily

Audience	What is Communicated	Channel	Frequency
Senior Management / Execs	Incident summary, customer exposure, legal implications	Email + Incident Briefing	P1: Hourly / P2: Daily
Risk / Audit / Compliance	Control failures, documentation completeness, audit trail needs	Email, SharePoint	Within 24–48 hours

14.3 External Notification Protocol

- **Sensitive Communications Must Be Pre-Approved by:**
  - **CISO**
  - **Legal Team**
  - **Data Protection Officer (DPO)**
  - **Executive Management**
- **Who May Be Notified**

Entity	Trigger for Notification	Timeline
Regulators / Authorities	Data breach involving PII, PHI, or financial data	GDPR: 72 hrs, DPDP: ASAP
Impacted Customers / Clients	Their data was accessed, deleted, or modified without authorization	Immediately after regulator notification
Third-Party Vendors / Partners	Their services were involved or impacted	Within 24–48 hours
Media / Press	Only in critical situations with reputational risk	By Executive Team only
Law Enforcement / CERT-IN	Nationally notifiable incident or attack origin traced to India	As required

14.4 Communication Templates

[ORG NAME] shall maintain ready-to-use templates for:

- Internal status updates (email/slack/IMS notifications)
- Client breach disclosure notices (short and long forms)
- Regulator reports (GDPR, DPDP, HIPAA, etc.)
- Public holding statements (press, investor, or media use)
- Post-incident executive summaries

Templates must include:

- Incident reference number
- Date/time of detection
- Affected assets/systems
- Summary of impact and root cause (if known)
- Containment and recovery actions taken
- Contact person or response team POC

14.5 Secure Communication Channels

To prevent data leakage and preserve evidence:

- All incident-related communications must use **encrypted, company-approved channels**
- Use of personal messaging apps (e.g., WhatsApp, Telegram) for incident discussions is prohibited
- Do not attach sensitive logs or evidence to unsecured emails
- Access to incident documentation (IMS, playbooks, RCA reports) must be **role-based**

14.6 Record Keeping and Audit Trail

- All formal notifications must be logged in the **incident record or tracker**, including:
    - Date and time sent
    - Recipient(s) and method

    - Copy of communication or summary

- Communications are retained as part of the incident audit package for **at least 5 years**

15. THIRD-PARTY AND CUSTOMER INVOLEMENT

Information security incidents may originate from, or impact, third-party vendors, cloud service providers, partners, or customers. To ensure a coordinated and timely response, [ORG NAME] will follow a structured approach to engage external stakeholders based on the nature and scope of the incident.

15.1 Vendor and Subprocessor Involvement

Incidents involving **vendors**, **subcontractors**, or **subprocessors** must be:

- Logged in the **incident tracking system** as a **third-party incident**
- Mapped to the associated **vendor risk profile** or SLA
- Escalated per the **vendor tiering and criticality matrix**

Vendor Responsibilities (as per contract / DPA):

- Promptly notify [ORG NAME] of any incidents impacting systems, data, or services within agreed SLA (e.g., 24–48 hours)
- Cooperate in root cause analysis, containment, and evidence sharing
- Provide audit logs, forensic details, and compliance documentation
- Implement corrective actions and communicate closure

[ORG NAME] Actions:

- Assess contractual clauses and indemnification obligations
- Determine data exposure or SLA violation impact
- Notify affected internal teams or clients (if relevant)
- Trigger a **vendor performance review** if breach was due to negligence

15.2 Third-Party Tools and SaaS Platforms

If an incident is traced back to a third-party software or cloud platform:

- [ORG NAME] will initiate emergency contact via the vendor's **security contact**
- A **risk assessment** will be initiated to determine dependency, data scope, and business impact
- Depending on severity, actions may include:
    - Temporary suspension of integration
    - Compensating controls (e.g., firewall block, geo-blocking)
    - Executive-level vendor communication or escalation

15.3 Customer Involvement

If a security incident directly or indirectly affects customer data, availability, or trust:

- **Customer Success** and **Legal** teams must be engaged immediately
- Communication must follow the approved **Breach Notification Plan** (see Section 11)
- Notification to customers may include:
    - Nature and scope of the incident
    - Data or service impacted
    - Steps taken to contain and mitigate
    - Timeline and POC for follow-up

Customer Notification Must Be:

- Reviewed by Legal and Executive Management
- Logged in the incident record (including copies or summaries)
- Shared within **contractual breach notification timelines** (usually 24–72 hours)
- Respectful of confidentiality obligations

15.4 Shared Responsibility Incidents

For **joint accountability** cases (e.g., SaaS or API-based integrations):

- Incident will be co-managed with the third party

- Shared root cause reports (RCA) may be developed
- Follow-up risk treatments may include:
    - Security review of integration
    - Reassessment of access scopes, tokens, or keys
    - Review or renegotiation of DPAs or SLAs

15.5 Confidentiality and Legal Safeguards

- All third-party and customer communications must be **vetted by Legal**
- Non-disclosure agreements (NDAs) and **data processing addendums (DPAs)** must be honored
- Any external investigation participation must have executive/legal approval
- For incidents involving regulated data, **regulator-specific obligations** will override vendor SLAs

16. Policy Enforcement

This section defines how compliance with the Incident Management Policy is ensured, and the consequences of non-compliance.

16.1 Policy Compliance

All employees, contractors, third parties, and vendors with access to [ORG NAME]'s systems, applications, or data are expected to:

- **Understand and adhere** to the requirements of this Incident Management Policy
- **Report incidents or suspicious activities promptly** using approved channels
- **Cooperate fully** with incident investigations and follow guidance from the CSIRT or Security Team
- Participate in **security awareness programs** related to incident reporting and handling

16.2 Enforcement Actions

Violations of this policy — whether due to negligence, misconduct, or willful disregard — may result in disciplinary actions, including but not limited to:

- Verbal or written warning

- Revocation of system or network access
- Mandatory retraining or reassignment
- Suspension or termination of employment/contract
- Legal action, financial penalties, or criminal referral where applicable

Disciplinary actions will be proportionate to the severity of the violation and consistent with HR and legal policies.

16.3 Monitoring and Audit

- Compliance with this policy may be **monitored** through internal audits, control testing, or live response simulations.
- Gaps, violations, or process delays identified during **post-incident reviews** will be logged as part of continuous improvement.
- Reports of policy violations or systemic failure may be escalated to **internal audit, legal, risk committee**, or **executive leadership**.

17. POLICY EXCEPTIONS

There may be exceptional situations where full adherence to the Incident Management Policy is not feasible due to business, technical, legal, or regulatory constraints. In such cases, formal exception handling ensures that risks are understood, approved, and mitigated to acceptable levels.

17.1 Exception Conditions

Policy exceptions may be requested under the following conditions:

- Temporary business requirement prevents full compliance (e.g., tool not yet implemented)
- Technical limitations in legacy or third-party systems
- Ongoing integration with a newly acquired entity or platform
- Jurisdictional or regulatory differences requiring alternate treatment
- Incident that deviates from standard classification or lifecycle due to extraordinary scope

17.2 Exception Request Process

Step	Action
1. **Submit Request**	Submit a formal request via [Exception Request Form or Portal]
2. **Provide Justification**	Include reason for exception, affected systems, risk impact, and duration
3. **Initial Review**	CSIRT / Information Security reviews risks and recommends compensating controls
4. **Risk Assessment**	May involve Legal, Risk, and Business Unit input
5. **Approval**	Final approval by CISO, Risk Owner, or relevant Steering Committee
6. **Documentation**	Exception is logged with ID, reviewer comments, approval, and expiry
7. **Monitoring**	Exceptions are monitored and reviewed at the defined expiry or renewal point

17.3 Exception Duration and Renewal

- Exceptions are granted for a **specific period** (default: 30 to 90 days)
- Renewal requests must follow the same approval workflow
- Long-standing exceptions must be revisited during:
    - Management Review Meetings
    - External audits or surveillance
    - Major incidents or control failures

17.4 Compensating Controls

Where exceptions are granted, **compensating controls** must be proposed and documented to reduce residual risk. These may include:

- Temporary system restrictions or isolation
- Manual monitoring of high-risk activities

- Additional approvals or logging
- Accelerated roadmap for permanent remediation

18. REVIEW, MAINTENANCE & VERSION CONTROL

To ensure ongoing relevance, effectiveness, and alignment with [ORG NAME]'s risk posture, regulatory obligations, and technological landscape, this Incident Management Policy will be reviewed and maintained on a regular basis.

18.1 Policy Review Frequency

- This policy shall be reviewed **at least once annually** by the Information Security Team, or more frequently if:
    - Major incidents occur
    - Regulatory requirements change
    - New tools or procedures are introduced
    - Internal audits or external assessments recommend updates

18.2 Review Ownership

Function	Responsibilities
Information Security / CSIRT	Coordinate the review, gather feedback from stakeholders, propose revisions
Legal & Compliance	Validate regulatory alignment (e.g., ISO 27001, SOC 2, GDPR, DPDP)
Executive Management / ISGC	Approve final revisions and ensure business alignment
Internal Audit / Risk	Provide feedback based on audits, control testing, or incident learning

18.3 Maintenance Activities

- Ensure all **incident forms, templates, playbooks**, and **contact directories** referenced in this policy are updated alongside the policy

- Validate that **incident management systems (IMS)** reflect latest classification and workflow updates
- Ensure changes are **communicated to all employees and stakeholders**, where applicable

18.4 Version Control Table

Version	Date	Author / Reviewer	Description of Changes
1.0	[DD-MM-YYYY]	Information Security Team	Initial release
1.1	[DD-MM-YYYY]	CISO / Compliance	Updated severity matrix and roles
1.2	[DD-MM-YYYY]	Legal / Risk	Included DPDP Act obligations

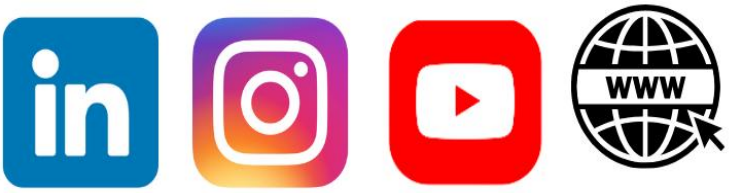
(Expand as required)

18.5 Policy Location & Access

- This policy is stored in the official **Information Security Policy Repository** (e.g., SharePoint, Confluence, or internal portal)
- Only the **latest approved version** shall be considered valid
- Archived versions are retained for **at least 5 years** for audit traceability

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS



WWW.MINISTRYOFSECURITY.CO