
# Langslide

## Incident Management Policy

Version 1.0

## PURPOSE

This policy applies to all information security incidents within Rudramsa Systems Pvt. Ltd., (hereby referred to as organization), covering every information system and IT asset owned or managed by the organization. It includes all employees—full-time, part-time, temporary staff, contractors, consultants, and third parties—and encompasses all data, whether stored, transmitted, on writable media, or within databases. Additionally, the policy spans all departments and functions, ensuring that any area of the organization that may encounter information security incidents is protected. By addressing these elements, the policy provides a comprehensive framework for managing and mitigating information security risks across the organization.

## SCOPE

This Incident Management Policy aims to establish a structured and systematic approach for identifying, responding to, managing, and mitigating information security incidents within an organization. It seeks to ensure timely and effective responses to incidents, minimize their impact on operations, assets, and individuals, protect the confidentiality, integrity, and availability of information assets, and facilitate continuous improvement in incident management processes by incorporating lessons learned.

## DEFINITIONS

Following is an explanation of various terms used within this document:

- **ISG (Information Security Group)**
  The team is responsible for overseeing the implementation and management of information security policies and procedures, including incident management.
- **Information Security**
  The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability.
- **Event**
  An observable occurrence within a network or system (e.g., unusual login attempts or system errors) may signify potential security incidents).
- **Security Event**
  A specific type of event indicating that a security policy may have been violated or a security safeguard may have failed (e.g., multiple failed login attempts, malware detection).
- **Security Incident**
  An event or series of events indicating unauthorized access, use, disclosure, modification, or destruction of information or interference with information systems operations, posing a threat to the organization's security posture.
- **Information Security Incident**
  A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with IT operations; or significant violation of any information security-related policy.
- **Security Breach**
  Any incident that results in unauthorized access to data, applications, services, networks, or devices by bypassing underlying security mechanisms can be intentional or unintentional.
- **Data Breach**
  A security incident involving the unauthorized copying, transmission, viewing, theft, or use of sensitive, protected, or confidential data.

- **Personal Data Breach**
  A data breach involving personal data or personally identifiable information (PII) of any living individual, including unauthorized sharing or disclosure without consent.
- **RCCA (Root Cause Corrective Action)**
  A process for identifying the fundamental cause of an incident and implementing corrective and preventive measures to prevent recurrence.
- **Incident Handling Team**
  A designated team responsible for managing and resolving incidents, potentially including members from HR, Admin, IT, Product, and other relevant departments.
- **Incident Response Team (IRT)**
  The team is tasked with responding to and managing information security incidents, including maintaining the Incident Response Plan, coordinating training and exercises, and overseeing the incident response process.
- **IRT Lead**
  The leader of the Incident Response Team is responsible for coordinating technical response activities, managing team members, and liaising with the Executive Sponsor for decisions impacting business operations.
- **Client Services Contact**
  The designated individual responsible for communicating incident alerts and updates to affected clients, maintaining a client contact list for incident escalation.

## RESPONSIBILITIES

The primary ownership of implementing this policy is with the information security group (ISG).

All employees are responsible for reporting an event, and the Incident handling team is responsible for responding.

The organization is responsible for the detection of and immediate response to information security incidents.

The following roles have been assigned to provide a coordinated and organized response process.

- **Information Security Group (ISG)**
  - **Policy Implementation:** Owns and implements the Incident Management Policy.
  - **Monitoring:** Continuously monitors information systems for potential security events and incidents.
  - **Coordination:** Coordinates with department heads and other stakeholders to ensure effective incident management.
  - **Documentation:** Maintains records of all incidents, responses, and lessons learned.
- **Executive Sponsor**
  - **Support:** Provide executive-level support and resources for the Incident Response Plan.
  - **Decision-Making:** Approves major decisions during incidents, including the availability of critical services and communication with external organizations.
  - **Oversight:** Ensures alignment of incident management with organizational goals and compliance requirements.
- **Incident Response Team (IRT)**
  - **Plan Maintenance:** Maintains and updates the Incident Response Plan.
  - **Training:** Coordinates and conducts training and testing of the Incident Response Plan.

- **Response Coordination:** Manages the overall incident response process, ensuring timely and effective actions are taken.
- **Threat Identification:** Identifies and communicates new information security threats that may impact the organization.

- **IRT Lead**
  - **Technical Coordination:** Coordinates all technical aspects of incident response.
  - **Support Initiation:** Initiates support from third parties as needed.
  - **Decision Approval:** Works with the Executive Sponsor to approve response decisions affecting business operations.
  - **Communication:** Ensures effective communication within the IRT and with other stakeholders during incidents.
- **IRT Members**
  - **Hands-On Response:** Execute specific tasks related to detection, analysis, containment, eradication, and recovery.
  - **Evidence Collection:** Collect and preserve evidence for forensic analysis and future prevention.
  - **Documentation:** Maintain detailed records of all actions taken during the incident response.
- **Client Services Contact**
  - **Client Communication:** Notifies affected clients about incidents and provides regular updates.
  - **Contact List Maintenance:** Maintains an up-to-date list of client contacts for incident escalation.
  - **Reporting:** Reports incident resolution to clients once the incident is resolved.

- **All Employees, Contractors, and Third Parties**
    - **Reporting:** Responsible for promptly reporting any suspected or actual security events or incidents.
    - **Compliance:** Must adhere to security policies and procedures to prevent incidents.
    - **Cooperation:** Cooperate with the IRT during incident investigations and response activities.

# POLICY

## SECURITY INCIDENT SEVERITY

Security incidents within the organization are categorized based on their potential impact on its operations, assets, individuals, mission, and reputation. Proper categorization facilitates the appropriate allocation of resources and ensures that incidents are managed with the necessary urgency and effectiveness.

**Security Categories**

Security categories assess the severity of incidents by evaluating their impact on the three core security objectives: Confidentiality, Integrity, and Availability (collectively known as the CIA triad). Each security objective is examined to determine the overall severity level of the incident.

- **Low-Security Category**
    - **Impact Assessment:**
        - **Confidentiality:** Minor unauthorized access to non-sensitive data.
        - **Integrity:** Limited alteration or corruption of non-critical data.
        - **Availability:** Brief downtime affecting non-essential systems or services.
    - **Potential Effects:**
        - Minimal disruption to day-to-day operations.
        - Minor financial implications or reputational impact.
        - Loss of secondary mission capabilities.
    - **Required Actions:**
        - Implement minor corrective actions or routine system repairs.
        - Conduct a fundamental review to prevent recurrence.
- **Moderate Security Category**
    - **Impact Assessment:**
        - **Confidentiality:** Unauthorized access to sensitive or proprietary information.
        - **Integrity:** Significant alteration or corruption of critical data.
        - **Availability:** Prolonged downtime affecting key systems or services.
    - **Potential Effects:**
        - Severe disruption to operations and business processes.

        - Significant financial losses or potential legal implications.
        - Non-life-threatening bodily harm or loss of privacy.
        - Significant damage to IT infrastructure or critical systems.
    - **Required Actions:**
        - Deploy extensive corrective measures and remediation efforts.
        - Conduct thorough system audits and vulnerability assessments.
        - Notify affected stakeholders in compliance with regulatory requirements.
- **High-Security Category**
    - **Impact Assessment:**
        - **Confidentiality:** Massive unauthorized disclosure of highly sensitive or classified information.
        - **Integrity:** Severe corruption or destruction of mission-critical data.
        - **Availability:** Total or near-total system outages affecting essential services.
    - **Potential Effects:**
        - Catastrophic disruption to operations and core mission objectives.
        - Severe financial and legal repercussions.
        - Threat to human life or safety.
        - Irreparable damage to organizational reputation and stakeholder trust.
    - **Required Actions:**
        - Immediate and comprehensive incident response involving all relevant teams.
        - Engage external authorities, forensic experts, and legal counsel as necessary.
        - Implement emergency protocols to safeguard affected areas and expedite recovery.
        - Communicate transparently with stakeholders to maintain trust and manage reputational impact.

Understanding the various types of security incidents enables organizations to identify, categorize, and respond effectively. The following table outlines the defined security incident types and their respective definitions:

| **Incident Type** | **Incident Definition** |
| --- | --- |
| System Compromise/ Intrusion | All instances of system compromise or intrusion by unauthorized individuals, whether intentional or unintentional, must be reported. This includes user-level compromises, root (administrator) compromises, and instances where users exceed their privilege levels. Examples include unauthorized server access, exploitation of vulnerabilities, and privilege escalation. |

| | |
|---|---|
| Malicious Code | All instances of successful infection or persistent attempts to infect systems with malicious code, such as viruses, Trojan horses, worms, ransomware, or spyware, must be reported. This includes introducing malicious code through phishing emails, infected downloads, or compromised websites. |
| Loss, Theft, or Missing | All loss, theft, or missing organizational assets must be reported, including laptop computers, mobile devices, removable storage media, and any IT resources containing sensitive information or Personally Identifiable Information (PII). This ensures timely actions to mitigate potential data breaches and secure compromised assets. |
| Denial of Service | Any intentional or unintentional attempts to disrupt the availability of critical services or deny access to network resources must be reported. This includes single-source DoS attacks and Distributed Denial of Service (DDoS) attacks, which simultaneously involve multiple sources targeting a network or service. Critical services are determined through Business Impact Analyses (BIA). |
| Information Compromise | Any unauthorized disclosure, access, or transmission of information to entities that do not require such information. This includes inadequate clearing, purging, or destruction of media and related equipment and transmitting information to unauthorized entities through unsecured channels. |
| Web Site Defacement | Any unauthorized website content, design, or functionality alteration that could harm the organization's reputation or disrupt services must be reported. This includes defacing public-facing websites, injecting malicious scripts, or modifying web content to display misleading or damaging information. |

## INCIDENT PREVENTION

Minimizing the occurrence of security incidents is critical to maintaining business operations. Preventative controls such as technology solutions, policies, procedures, and training are the most effective ways to minimize information security and privacy incidents.

The organization maintains security controls to prevent and detect information security incidents.

| **Corporate Environment** | |
|---|---|
| | Trained Users |

| | |
|---|---|
| **People** | 24x7 network availability monitoring by managed service |
| **Process** | Security Policies and Procedures User Security Education Operations Security Education Risk Management<br>Vulnerability Management<br>Patch Management<br>User Access Management Incident Reporting<br>Monitoring and Audit Procedure |
| **Technology** | Antivirus Software Firewalls<br>Antivirus Software<br>Network Vulnerability Scanning System Audit and Event Logging Application Vulnerability Scanning |

## INCIDENT RESPONSE TRAINING

All users are provided with annual Security Awareness Training.

**Security Awareness Training**

- **Annual Training:** All employees, contractors, and third parties must participate in yearly security awareness training programs. These sessions cover:
    - Information security best practices.
    - Recognizing and reporting potential security threats.
    - Understanding the organization's incident response protocols.
- **Role-Specific Training:** Provide specialized training for Incident Response Team (IRT) members and other key roles involved in incident management, focusing on advanced response techniques and tools.
- **Phishing Simulations:** Conduct regular phishing simulations to test employee awareness and reinforce training objectives. Analyze results to identify areas needing additional training.

**Incident Response Plan Review**

- **Group Review Sessions:** Conduct group review sessions of the Incident Response Plan with the IRT to ensure all members are familiar with the procedures and can execute their roles effectively during an incident.
- **Workflow Updates:** Regularly update response workflows based on feedback from training sessions, exercises, and incidents to enhance efficiency and effectiveness.
- **Scenario-Based Training:** Use realistic incident scenarios to train the IRT to handle various types of security incidents, ensuring preparedness for diverse threat landscapes.

**Continuous Education**

- **Ongoing Learning Opportunities:** Provide continuous education opportunities, such as workshops, webinars, and certifications, to keep the IRT and other security personnel updated on the latest threats and response strategies.
- **Knowledge Sharing:** Encourage knowledge sharing within the team through regular meetings, documentation of best practices, and collaboration with industry peers.

## INCIDENT RESPONSE TESTING AND EXERCISES

Regular testing and exercises are essential to validate the Incident Response Plan's effectiveness and ensure the Incident Response Team's (IRT) readiness.

**Annual Testing**

- **Full-Scale Exercises:** Conduct comprehensive incident response exercises annually to test the Incident Response Plan's effectiveness. These exercises should simulate realistic attack scenarios to evaluate the team's response capabilities.
- **Tabletop Exercises:** Engage in tabletop exercises to facilitate scenario-based discussions. This allows the team to walk through response procedures and identify potential gaps without requiring physical simulations.

**Incorporating Actual Incidents as Tests**

- **Real Incidents as Tests:** If an actual incident occurs and the Incident Response Plan is followed, the incident will be treated as a test to evaluate the plan's effectiveness. Ensure that the incident is appropriately documented and reported to derive actionable insights.
- **Documentation:** Thoroughly document lessons learned from actual incidents and integrate improvements into the Incident Response Plan to enhance future responses.

**Test Scenario Development**

- **IRT Lead Responsibility:** The IRT Lead is responsible for developing realistic and relevant test scenarios based on potential threats and emerging security trends.
- **Diverse Scenarios:** Ensure that test scenarios cover a wide range of incident types, including malware infections, data breaches, insider threats, and infrastructure compromises, to ensure comprehensive preparedness.

**Post-Test Review**

- **Debriefing Sessions:** Hold debriefing sessions after each exercise to discuss what worked well and identify areas for improvement.
- **Action Items:** Assign and track action items identified during testing to address gaps and enhance the Incident Response Plan's effectiveness.
- **Continuous Improvement:** Use feedback from testing and exercises to continuously improve incident response capabilities and policies.

## IDENTIFICATION AND MANAGEMENT OF NEW THREATS

To prevent security incidents, the Incident Response Team (IRT) or approved delegates will monitor the following public information sources for new information security threats. Newly identified threats will be escalated for preventative action:

**For India:**

**CERT-In:** https://www.cert-in.org.in/s2cMainServlet?pageid=VLNLIST

**For the US:**

**SANS Internet Storm Center:** http://isc.sans.org/

**US CERT, National Cyber Alert System:** http://www.us-cert.gov/

**NIST National Vulnerability Database:** http://nvd.nist.gov/

**Secunia:** http://secunia.com/advisories/

## INCIDENT ANALYSIS

### EVENT ANALYSIS

Practical incident analysis is critical for understanding the nature of security incidents, determining their impact, and formulating appropriate responses.

#### Event Analysis

Security event analysis is the process of examining security events to determine whether they qualify as security incidents. Familiar sources of security event notifications include:

- **User Reports:** Users, clients, or vendors report potential incidents to members of the organization.
- **Automated Alerts:** Antivirus tools detect, alert to, and often prevent incidents through computerized mechanisms.
- **Log Analysis:** Operating system, application, and network device logs provide evidence of security and privacy incidents that are in progress or have occurred.
- **Regular Meetings:** Periodic meetings review support and incident details, facilitating collaborative analysis.
- **Suspicious Behaviour:** Detection of unusual system behavior indicative of a potential compromise.

#### Immediate Investigation

- **Responsibility:** IRT members are responsible for immediately investigating security events that indicate a Security Incident may have occurred or is underway.
- **Documentation:** Maintain a detailed written timeline of events to support post-incident analysis and future prevention measures.
- **Advanced Evidence Collection:** If legal action is possible, engage qualified Incident Management Consultants to perform advanced evidence collection. The IRT Lead will coordinate with the Executive Sponsor to determine the necessity of this action.

#### Root Cause Analysis (RCCA)

- **Objective:** Identify the fundamental cause of the incident so that corrective and preventive measures can be implemented to prevent its recurrence.
- **Process:**
    - **Data Collection:** Gather all relevant data, including logs, system configurations, and evidence collected during the incident.
    - **Analysis:** Conduct a thorough analysis to determine how the incident occurred, the vulnerabilities exploited, and the effectiveness of existing controls.
    - **Action Plans:** Develop and implement action plans to address identified root causes and strengthen security controls.
- **Documentation:** Record all findings and actions taken during the RCCA to inform future incident prevention and response strategies.

## DECLARATION OF A SECURITY INCIDENT

Prompt declaration and escalation of security incidents are essential for effective incident management and minimizing potential impacts.

**Escalation Process**

- **Suspicion of Incident:** If an IRT member suspects a security incident has occurred or is in progress, they must immediately escalate the issue to the IRT Lead.
- **Assessment:** Upon notification, the IRT Lead will assess the severity and potential impact of the incident to determine whether the Incident Response Plan needs to be activated.

**Activation of Incident Response Plan**

- **Criteria for Activation:** The IRT Lead will activate the Incident Response Plan based on predefined criteria, including the incident's severity, impact, and potential legal or regulatory implications.
- **Notification:** Notify all relevant stakeholders and assemble the Incident Response Team per the communication plan.

**Incident Response Lifecycle**

The Incident Response Lifecycle outlines the phases through which security incidents are managed, ensuring a structured and effective response.

**Preparation**

- **Incident Response Plan (IRP):** Develop and maintain a comprehensive IRP outlining roles, responsibilities, and procedures for responding to incidents.
- **Training:** Conduct regular training sessions for the IRT and all employees on incident response protocols and security awareness.
- **Tools and Resources:** Ensure the availability of necessary tools (e.g., SIEM systems, forensic tools) for effective incident detection and response.
- **Access Control:** Implement strict access controls to sensitive information and systems to prevent unauthorized access.

**Detection and Analysis**

- **Identify Potential Incidents:**
  - Monitor security systems and logs for indicators of compromise.
  - Encourage employees to report suspicious activities promptly.
- **Initial Assessment:**
  - Determine whether the event qualifies as a security incident based on predefined criteria.
  - Categorize the incident based on severity and potential impact.

- **Detailed Analysis:**
    - Investigate the root cause and extent of the incident.
    - Assess the impact on systems, data, and business operations.
    - Determine if the incident involves data breaches or legal implications.

**Containment, Eradication, and Recovery**

- **Containment:**
    - Short-Term Containment: Immediately isolate affected systems to prevent further damage (e.g., remove compromised machines from the network).
    - Long-Term Containment: Implement measures to maintain isolation while preparing for eradication and recovery.
- **Eradication:**
    - Remove the incident's root cause (e.g., malware removal, patching vulnerabilities).
    - Ensure no remnants of the threat remain in the environment.
- **Recovery:**
    - Restore affected systems and data from clean backups.
    - Validate the integrity and functionality of restored systems.
    - Gradually restore normal operations while monitoring for any signs of recurring issues.

**Post-Incident Activity**

- **Incident Review:**
    - Conduct a thorough review of the incident response process.
    - Identify what worked well and what needs improvement.
- **Root Cause Analysis (RCCA):**
    - Perform RCCA to determine the underlying causes of the incident.
    - Develop and implement corrective and preventive actions to avoid recurrence.
- **Documentation:**
    - Update incident records with detailed findings and actions taken.
    - Archive all documentation by organizational retention policies.
- **Reporting:**
    - Generate comprehensive incident reports for internal and external stakeholders as required.
    - Share lessons learned with relevant teams to enhance overall security posture.

## COMMUNICATION PLAN

Security incident-related communication methods should be efficient and confidential. When dealing with an ongoing technology breach, incident details should not be communicated via email.

**INTERNAL COMMUNICATION**

It is critical to maintain communication during the incident management process. Once a Security Incident has been declared, appropriate team members must be notified immediately.

The following table outlines the organization's internal incident communication plan:

| Event Description | Communication Process |
|---|---|
| Suspected Security Incident | The IRT Lead communicates in person or via phone to assess the situation. |
| Confirmed Security Incident | Upon confirmation by the IRT Lead, relevant management contacts must be informed in person or via secure call.<br>Use secure communication channels (e.g., encrypted messaging protected conference calls) to discuss specific details. |
| Incident Updates | Unless otherwise approved by the Executive Sponsor, the IRT Lead will provide the Incident Response Team with hourly updates until the incident is resolved.<br>Updates will be provided via secure conference calls or in-person meetings. |
| Incident Resolution | Once the Security Incident has been eradicated and normal business operations resume, the IRT Lead will send a summary email detailing the final resolution to all Incident Response Team members and the IRT. |

| | |
|---|---|
| Post Mortem | For all incidents involving the incident response team, a post-incident analysis meeting will be held within one week of closing the Incident. The meeting's purpose is to give participants an opportunity to share and document details about the incident and identify lessons learned. |

Upon initial notification that an information Security Incident has occurred or is in progress, the Client Services Contact is responsible for alerting all clients who are likely to be affected by the incident. The Client Services Contact must also provide regular updates to each client contact as the incident response activities as follows:

| Timeline | Communication |
|---|---|
| Immediately after the IRT has assessed the severity and potential client impact of an incident | The Client Services Contact communicates the incident details to all clients who may have been impacted, including severity level and steps that<br><br>.CLIENT will rectify the situation. |
| Every 4 Hours After the Last Client Communication until the<br><br>The incident has been resolved | Client Services Contact provides status updates to potentially impacted clients. |

The Client Services Contact is responsible for maintaining a list of all clients' preferred contact information for reporting information on security incidents. This contact list is to be stored in the company document repository folder.

## BREACH NOTIFICATION PLAN

If the organization confirms that an unauthorized disclosure of confidential information has occurred, there are potential requirements that the organization is legally or contractually obligated to follow. Ultimately, it is the responsibility of the Executive Sponsor to decide whether to execute the breach notification plan. The Client Services Contact is responsible for maintaining a list of all client contacts' preferred contact information for reporting information on security incidents.

If the confidential information is involved in a data breach, the following steps will be taken:

- If required, the organization will contact an approved third-party forensics organization to support the continued internal investigation.
- The organization will report the breach to local law enforcement agencies.
- Contact relevant clients and third parties. The following table describes unique obligations based on different data categories:

| | | |
|---|---|---|
| **Data Category** | Personally Identifiable Information<br><br>Defined as: Any individually identifiable information a client or other party provides to the organization. | Intellectual Property<br><br>Defined as: Any client information protected by patent, copyright, trademark, or is considered a trade secret or material non-public information. |
| **Breach Definition** | Unauthorized acquisition, access, use, or disclosure of unencrypted personally identifiable information, except where an unauthorized person to whom such information is disclosed | Unauthorized acquisition, access, use, or disclosure of unencrypted intellectual property, except where an unauthorized person to whom such information is disclosed would not |

| | | |
|---|---|---|
| | would not reasonably have been able to retain such<br><br>information. | reasonably have been able to retain such<br><br>information. |
| **Notification Plan** | The organization will promptly contact all affected clients and inform them of the incident. To the best of the organization's ability, the following information will be provided:<br><br>Describe the breach event. D. Describe the data involved. Quantify the number of individual records involved. List the specific individuals affected<br><br>Describe the next steps the organization is taking | The organization will promptly contact all affected clients and inform them of the incident. To the best of the organization's ability, the following information will be provided:<br><br>Describe the breach and even describe the data involved. Quantify the volume of information involved. Describe the next steps the organization is taking. |

## MAINTENANCE OF THE PLAN

To ensure the ongoing effectiveness and relevance of the Incident Management Plan, the organization adheres to a rigorous maintenance schedule and incorporates continuous improvement practices.

- **Annual Review:**
  - The Incident Response Team (IRT) or approved delegates will meet at least annually to review, test, and update the incident response plan.
  - Updates should reflect changes in the organizational environment, emerging threats, technological advancements, and lessons learned from past incidents.
- **Post-Incident Review:**
  - After each incident, conduct a post-incident review to analyze the response's effectiveness, identify areas for improvement, and update the Incident Response Plan accordingly.
  - Document lessons learned and integrate them into training programs and policy updates.
- **Continuous Improvement:**
  - Utilize feedback from training sessions, exercises, and actual incidents to continuously improve incident response capabilities.
  - Implement enhancements based on identified gaps and evolving best practices in information security.
- **Stakeholder Engagement:**
  - To ensure comprehensive coverage and support, key stakeholders from various departments (e.g., IT, HR, Legal, Client Services) should be involved in the review and maintenance process.
  - Communicate updates and changes to all relevant parties to maintain alignment and preparedness.

- **Documentation and Accessibility:**
    - Maintain all incident-related documentation in a secure, centralized repository accessible only to authorized personnel.
    - Ensure that the Incident Response Plan and related documents are readily accessible during an incident to facilitate swift and effective response actions.

# Appendix

A. Contact Sheet

## INCIDENT RESPONSE TEAM CONTACT SHEET

## PRIMARY INCIDENT RESPONSE AND BUSINESS CONTINUITY TEAM

| Name | Incident Response Role | Phone | Email |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

A. External Support

| Vendor | Role | Contact |
|---|---|---|
| | | |
| | | |

### External Incident Response and Forensics Support

| Name | Incident Response Role | Contact |
|---|---|---|
| | | |

### Law Enforcement

| Name | Phone |
|---|---|
| | |
| | |
| | |

A. Response Checklist

## INCIDENT RESPONSE CHECKLIST

| | | |
|---|---|---|
| **Detection and Analysis** | | |
| 1. | Determine whether an incident has occurred. | |
| 1.1 | Analyze precursors and indicators. | |
| 1.2 | Correlate information from various sources. | |
| 1.3 | Research to understand the threat. | |
| 1.4 | Document the investigation and evidence collection process. | |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) | |
| 3. | Report the incident to the appropriate internal personnel and external organizations | |
| **Containment, Eradication and Recovery** | | |
| 4. | Acquire, preserve, secure, and document evidence. | |

| | | |
|---|---|---|
| 5. | Contain the incident | |
| 6. | Eradicate the incident | |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited | |
| 6.2 | Remove malware, inappropriate materials, and other components | |
| 6.3 | If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other<br>affected hosts, then contain ⑤ and eradicate ⑥ the incident for them | |
| 7. | Recover from the incident.t | |
| 7.1 | Return affected systems to an operationally ready state | |
| 7.2 | Confirm that the affected systems are functioning normally | |
| 7.3 | Additional monitoring should be implemented to look for future related activity if necessary. t.y | |
| **Post Incident Activity** | | |
| 8. | Create a follow-up report. | |
| 9. | Hold a lessons-learned meeting (mandatory for significant incidents, optional<br>otherwise) | |

A. Incident Report

## A SECURITY INCIDENT REPORT

<table>
<tr><td colspan="2" rowspan="2">Incident Name:</td><td>Approved by</td><td>Reported by</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Select the applicable incident category:</td><td colspan="3"><ul><li>Loss or theft of PCs or removable storage media</li><li>Confidential data compromise or loss</li><li>Malicious code or other software infection to PCs, data, or removal media except for prevented cases before an infection</li><li>Phishing</li><li>Information system disruption that impacted a customer or stopped the production process for more than half a day (Denial of Service)</li><li>Unauthorized access or system compromise that was not able to be prevented</li><li>Web website defacement and other incident that may result in reputational damage</li><li>The case that the IT security officer or IT manager regards the incident as serious.</li></ul></td></tr>
<tr><td>When did the incident occur?</td><td>Date: Time:</td><td>When will this report be submitted?</td><td>Date:</td></tr>
<tr><td colspan="4">Summary of the incident</td></tr>
<tr><td>Describe exactly what happened.</td><td colspan="3"></td></tr>
<tr><td>What was the cause?</td><td colspan="3"></td></tr>
<tr><td>What measures did you take?</td><td colspan="3"></td></tr>
</table>

| | |
|---|---|
| As a result... | |

| | | |
|---|---|---|
| | | |
| Review to learn from the incident. | | |
| What is a preventive measure against recurrence? | | |
| Should the measures be applied somewhere?<br>Yes/No/Other | | If Yes, Describe the details. |
| Describe the person, the place, or the organization<br>which was influenced. | | |
| How much is the damage, and what is the recovery cost? | | |
| Remarks | | |

# Version Details

| Version | Version Date | Description of changes | Created By | Approved By | Published By |
|---|---|---|---|---|---|
| Version 1.0 | Mar 14 2026 | Initial Release | Pronoy | Kartikeya | Kartikeya |