

Security Incident Management Policy

**Document Statistics**

|  |  |
| --- | --- |
| **Type Of Information** | **Document Data** |
| Document Title | Security Incident Management Policy |
| Document Code | PO/SIMPO/V01 |
| Date of Release | 11-Apr-2024 |
| Document Revision No | 1st release of document |
| Document Owner | IT Executive |
| Documents Author(s) | IT Head |
| Document Change Reviewer | IT Head |
| Security Classification | Confidential |
| Document Status | Approved |

**Document approvers.**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Approver** | **Approver Contact(Email)** |
| 1 | Vice President Strategy & BIS | Rashmin Vyawahare <r.vyawahare@cloudextel.com> |

**Document Change Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Revision Date** | **Nature of Change** | **Date Approved** |
| 1 | 11th Apr 2024 | Revised Release | 11th Apr 2024 |

**Document Contact Point**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Document/Process** | **Document Author** | **Document Primary Focal Point** |
| 1 | Security Incident Management Policy | IT Head | IT Policy Folder |

**Document Reference List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No** | **Reference No.** | **Document Name** | **Effective date** |
|  |  |  |  |

**Index**

Contents

[1. Purpose and Scope 6](#_Toc165473995)

[2. Abbreviations and Definitions 6](#_Toc165473996)

[3. Guidelines 6](#_Toc165473997)

[4. Policy Statement: 7](#_Toc165473998)

[4.1. Incident Identification and Reporting: 7](#_Toc165473999)

[4.2. Incident Response Team: 8](#_Toc165474000)

[4.3. Incident Response Plan: 9](#_Toc165474001)

[4.4. Containment and Eradication: 9](#_Toc165474002)

[4.5. Communication and Notification: 9](#_Toc165474003)

[4.6. Documentation and Analysis: 11](#_Toc165474004)

[4.7. Training and Awareness: 12](#_Toc165474005)

[4.8. Cybersecurity Insurance: 12](#_Toc165474006)

[4.9. Policy Compliance: 13](#_Toc165474007)

[4.10. Approval: 13](#_Toc165474008)

[5. Supporting Policies and Standards 13](#_Toc165474009)

[6. Roles and Responsibilities 14](#_Toc165474010)

[7. Summary 14](#_Toc165474011)

## Purpose and Scope

The Security Incident Management Policy outlines the procedures and guidelines for effectively detecting, responding to, and mitigating security incidents within the organization. It aims to minimize the impact of security breaches, protect sensitive information, and maintain the integrity of the organization's systems and data.

This policy is applicable to all Temporary Staff, Employees and Process Owners working with Excel Telesonic India Pvt Ltd. All are expected to be familiar with and comply with this policy.

## Abbreviations and Definitions

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Abbreviation/Definition** | **Explanation** |
| 1 | IS | Information systems |
| 2 | ISM | Information Security Manager |
| 3 | ISSC | Information Security Steering Committee |
| 4 | SIM | Security Incident Management Policy |
| 4 | DR | Disaster Recovery Policy |

## Guidelines

The key principles of a security incident management policy Security Incident where our ERP – ERPNext is hosted on AWS and we have Microsoft 365 as our communications platform

* **Simplicity**: Keep incident response processes simple and easy to understand.
* **Automation**: Leverage automation to streamline incident response processes.
* **Learning**: Use incident learning to improve processes, build resilience, and prevent future incidents.
* **Shared Responsibility**: Understand the shared responsibility model in cloud environments.
* **Preparation and Prevention**: Implement security best practices, establish incident response plans, and train teams.
* **Detection and Analysis**: Rapidly identify and analyze security incidents.
* **Containment, Eradication, and Recovery**: Contain, eradicate, and recover from incidents quickly.
* **Post-Incident Activity**: Learn from incidents to improve incident response processes, policies, and procedures.
* **Communication**: Establish clear guidelines for communicating about security incidents.

## Policy Statement:

## Incident Identification and Reporting:

All employees and third-party providers are required to report any suspected or confirmed security incidents, events, or weaknesses in systems or services to the designated IT security team immediately.

The incident response team will be notified of any reported incidents and will take appropriate action to contain, eradicate, and recover from the incident.

The incident classification table below provides several incident factors to assist in proper incident classification. Depending on the nature of the incident, some of the incident criteria represented in the table may not be present in a particular incident. Moreover, if an incident contains characteristics in several different severity columns, the severity of an incident must reflect the highest category.

Incident classification is a dynamic process. Incident severity may change one or more times as incident details emerge over time during the investigation process.

**Incident Classification Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Factors** | **Incident Severity Characteristics** | | |
| **Low** | **Medium** | **High** |
| Criticality – Application | Internal systems and  applications | Internal or external  systems and applications | Internal or external  systems and applications |
| Criticality – Infrastructure  (As defined in the Critical System Inventory) | User system | Non-critical enterprise system | Critical enterprise system |
| Criticality – Infrastructure | No | Limited Scope | Organization-wide impact |
| Impact – User/System | Affects few people or few  systems | Department-wide  impact | Organization-wide impact |
| Impact – Public | None | Potential impact | Definite impact |
| Countermeasures | Solutions are readily  available | Weak countermeasures | No countermeasures |
| Encryption | Robust encryption algorithm, and key  control | Weak algorithm and/or key controls | No encryption, or  easily defeated encryption |
| Resolution Procedures | Available and well- defined | Resolution procedure not well-defined, bypass  available | No resolution procedures or bypass available |
| Information Sensitivity | Affects an individual employee or  unit | Affects an individual | Orgnization-wide |
| Protected Information (Personally- Identifiable Information or Protected  health Information) | None | Possible | Definite |

## Incident Response Team:

An incident response team will be designated and trained to handle security incidents promptly and effectively.

**Formation of Incident Response Team:**

In the event of a security incident, the Incident Response Manager (IRM) is responsible for forming the incident response team based on the severity and nature of the incident. The IRM, in consultation with the Chief Information Security Officer (CISO) and relevant stakeholders, will identify and designate team members from across the organization.

**Training and Responsibilities:**

1. **Initial Formation Training:**

Upon designation, incident response team members will undergo comprehensive training sessions conducted by the IRM or designated personnel.

Training will cover the team's roles, responsibilities, and obligations outlined in this policy, as well as incident handling procedures, communication protocols, and relevant technical skills.

1. **Ongoing Training and Skill Enhancement:**

The incident response team will participate in regular training exercises and simulations to enhance their readiness and proficiency in responding to security incidents.

Training sessions will be conducted periodically to ensure team members are up-to-date with emerging threats, technologies, and best practices in incident response.

1. **Roles and Responsibilities:**

The incident response team will consist of individuals with diverse skills and expertise, including but not limited to:

* Technical experts for incident analysis, containment, and eradication.
* Legal counsel for guidance on regulatory compliance and legal implications.
* Communications professionals for managing external communications and public relations.

Each team member will be assigned specific roles and responsibilities based on their expertise and the requirements of the incident.

**Severity-Based Team Activation:**

The activation and composition of the incident response team will vary depending on the severity classification of the incident:

**Low Severity:** A smaller subset of the incident response team may be activated to handle low-impact incidents with minimal disruption.

**Medium to High Severity:** The full incident response team, including senior management and executive leadership, may be activated to address medium to high-impact incidents that pose significant risks to the organization.

## Incident Response Plan:

A comprehensive incident response plan will be developed, documented, and regularly tested to ensure readiness in the event of a security incident.

The plan will include procedures for containment, eradication, recovery, and post-incident analysis.

## Containment and Eradication:

Upon detection of a security incident, the incident response team will work to contain the incident to prevent further damage.

Efforts will be made to eradicate the root cause of the incident and restore affected systems to a secure state.

## Communication and Notification:

**Notification Protocol:**

**Immediate Reporting:**

* Upon discovery of a security incident, all employees are required to promptly report the incident to the Incident Response Manager (IRM) or designated incident response contact.
* The initial notification should include relevant details such as the nature of the incident, affected systems or data, and any observed indicators of compromise.

**Incident Classification and Escalation:**

* Incidents will be classified based on severity, impact, and potential risks to the organization, as outlined in the Incident Classification Table (refer above).
* The Incident Response Manager (IRM) is responsible for classifying incidents and initiating appropriate response actions in accordance with the severity level.

**Responsibilities for Communicating and Escalating Incidents:**

**Incident Response Team:**

**The incident response team members are responsible for:**

* Communicating incident details and updates to relevant stakeholders within the organization.
* Collaborating with technical experts to assess the impact and scope of the incident.
* Escalating incidents to senior management and executive leadership as necessary, based on the severity classification.

**Senior Management and Executive Leadership:**

**Senior management and executive leadership are responsible for:**

* Reviewing and approving incident response plans and escalation procedures.
* Being informed of high-severity incidents in a timely manner, as outlined in the Incident Classification Table.
* Providing strategic guidance and support for incident response efforts.
* Ensuring that incidents with significant business impact are escalated to the board of directors or regulatory authorities in accordance with regulatory requirements and the Breach Incident Escalation Policy.

This Incident Notification and Escalation Protocol **aligns with the Breach Incident Escalation Policy**, which provides detailed procedures for escalating serious incidents to the board of directors, regulatory authorities, and other relevant stakeholders.

**Required Timeframes for Escalation:**

Incidents classified as high severity must be escalated to senior management and executive leadership within 24 hours, as outlined in the Incident Classification Table.

## Documentation and Analysis:

**Incident Documentation:**

**Required Information:**

Following the resolution of a security incident, the incident response team is responsible for documenting relevant information to facilitate post-incident analysis and reporting.

**Key information to be documented includes:**

* Incident classification and severity level.
* Description of the incident, including its nature, impact, and root cause.
* Actions taken during the incident response process, including containment, eradication, and recovery measures.
* Technical details, such as affected systems, compromised credentials, malware analysis, and forensic findings.
* Communication logs, including internal notifications, updates, and external communications with stakeholders, regulatory authorities, or law enforcement agencies.
* Lessons learned and recommendations for improving incident response procedures and mitigating similar incidents in the future.

**Timeline for Documentation:**

Incident documentation should be initiated as soon as possible following the resolution of the incident.

The Incident Response Manager (IRM) or designated incident response personnel are responsible for ensuring that incident documentation is completed promptly and accurately.

**Post-Incident Reports:**

**Completion Timeline:**

Post-incident reports must be completed within 15 Business days of the incident resolution.

**Review and Approval Process:**

Upon completion, post-incident reports will undergo a review process involving relevant stakeholders, including senior management, executive leadership, legal counsel, and IT governance committees.

The Incident Response Manager (IRM) or designated personnel will coordinate the review process and address any feedback or recommendations provided by stakeholders.

**Continuous Improvement:**

Incident documentation and reflection are integral to the organization's continuous improvement efforts in enhancing incident response capabilities, refining security controls, and mitigating future risks.

## Training and Awareness:

Regular training sessions and awareness programs will be conducted to educate employees on security best practices, incident reporting procedures, and their role in incident response.

## Cybersecurity Insurance:

Cybersecurity insurance is an essential component of the organization's risk management strategy. It provides financial protection against losses resulting from cyber incidents, such as data breaches, network outages, or cyber extortion. This clause outlines the organization's approach to cybersecurity insurance coverage and its integration into the incident management framework.

**Key Points:**

**Coverage Assessment:**

* The organization regularly assesses its cybersecurity insurance coverage to ensure alignment with evolving cyber threats and business requirements.
* Coverage considerations may include liability protection, breach response costs, business interruption losses, and regulatory fines and penalties.

**Incident Reporting Requirements:**

* In the event of a security incident, the Incident Response Manager (IRM) or designated personnel are responsible for promptly notifying the cybersecurity insurance provider and initiating the claims process.
* Timely and accurate reporting is essential to maximize coverage and expedite claim resolution.

**Policy Review and Updates:**

* The organization periodically reviews its cybersecurity insurance policies to verify coverage adequacy and address any gaps or changes in risk exposure.
* Updates to insurance policies are coordinated with the incident management team to ensure alignment with incident response procedures and requirements.
* Integration with Incident Management:

Cybersecurity insurance serves as a critical component of the organization's incident management framework, providing financial support and resources to mitigate the impact of security incidents and facilitate recovery efforts.

## Policy Compliance:

Failure to comply with this Security Incident Management Policy may result in disciplinary action, up to and including termination.

All employees are expected to familiarize themselves with this policy and adhere to its guidelines.

## Approval:

This policy is approved as mentioned in document matrix above.

## Supporting Policies and Standards

This Security Incident Management policy should be read and understood in conjunction with the following policies and standards:

**Breach Incident Escalation Policy:** This policy outlines the procedures for escalating and managing security breaches, including criteria for identifying breaches and the responsibilities of different stakeholders in the escalation process.

**Access Management Policy:** Defines protocols for managing user access to systems, applications, and data within CloudExtel's infrastructure. Access management policies ensure that only authorized individuals have appropriate access privileges, thereby reducing the risk of unauthorized access or breaches that could disrupt business operations.

**Change Management Policy:** Establishes procedures for planning, implementing, and reviewing changes to IT systems and infrastructure. Change management policies ensure that changes are assessed for potential impacts on business continuity and are implemented in a controlled manner to minimize disruptions and maintain system integrity.

**Employee Security Awareness Training**: These standard mandates regular training sessions to educate employees about security best practices, common threats, and their roles and responsibilities in maintaining a secure environment.

## Roles and Responsibilities

CloudExtel assigns specific roles and responsibilities to key personnel to ensure effective implementation and maintenance of the Business Continuity Plan. The following roles and their responsibilities are outlined:

1. **Incident Response Team:**

* CISO: Oversees incident response and approves plans.
* Incident Response Manager: Leads response efforts.
* Technical Experts: Analyze and mitigate incidents.
* Legal Counsel: Advises on legal aspects.
* PR/Communications Team: Handles external communications.

1. **Executive Management:**

* CEO, COO, CIO: Provide leadership and resources.

1. **Business Unit Representatives:**

* Business Line Owners, Department Heads: Provide expertise and support.

1. **Employees:**

* Report incidents promptly and follow security policies.

## Summary

This Security Incident Management Policy is designed to ensure a proactive and effective approach to handling security incidents within the organization, safeguarding its assets, reputation, and stakeholders. The policy addresses all the specified points, including incident reporting, incident response team, incident response plan, containment and eradication, communication and notification, documentation and analysis, training and awareness, data centers/networks/services sharing, incident disclosure, and cybersecurity insurance.