Insert the organization logo by clicking on the image icon

Incident Response Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Incident Response Policy Template |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Objective 4](#_Toc97458031)

[2. Scope 4](#_Toc97458032)

[3. Policy 4](#_Toc97458033)

[3.1 General Requirements 4](#_Toc97458034)

[3.2 Roles and Responsibilities 5](#_Toc97458035)

[3.3 Incident Response Plan 6](#_Toc97458036)

[3.4 Data Classification 6](#_Toc97458037)

[3.5 Incident Reporting 6](#_Toc97458038)

[3.6 Incident Classification 7](#_Toc97458039)

[3.7 Incident Response 7](#_Toc97458040)

[4. Policy Enforcement 8](#_Toc97458043)

# Objective

This policy aims to ensure the consistent and professional management of information security incidents in order to mitigate or minimize any harm to users, information systems and its related devices at the <entity name>.

# Scope

All information created or received by the <entity name> in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely. All users, trainees and third-party contractors working for or on behalf of <entity name> and any other person permitted to have access to <entity name> premises. Information systems and related devices and components managed or held or processed by <entity name>. All locations from which <entity name>’s information is accessed including home use.

# Policy

## General Requirements

1. <entity name> must understand and be aware of the types of data security incident which include but not limited to:
	* Successful unauthorized access attempts.
	* Denial of service.
	* Unauthorized use of resources such as system processing or storage.
	* Unauthorized systems changes.
	* Information and equipment loss or theft
	* Unforeseen circumstances.
	* Human errors.
	* Adversary attacks
2. Incident Handling Team (IHT) must be identified along with roles and responsibilities.
3. Management personnel must be identified to support the incident handling process.
4. Incident Response policy and procedures must be identified.
5. Incident Response policy and procedures must be approved from management level.
6. Incident Response policy and procedures must be reviewed and updated.
7. Incident management should be adopted in a standardized and consistent approach to ensure:
	* Incident reporting should be in a timely manner for proper investigation.
	* Authorized and well skilled personnel should handle the incidents.
	* Response management involves appropriate levels of management.
	* All incidents must be recorded and document.
	* Evidence is gathered, recorded and maintained for internal and external scrutiny.
	* All <entity name>’s data users are informed as required.
	* Incidents are handled in a timely manner and normal operations are restored
	* Incidents are reviewed to list the improvements recommended in policies and procedures.
	* Organizational Impacts are understood, and action is taken to prevent further damages.
8. All types of incidents occurred from various resources must be reported and managed similarly.
9. Incident Scenario sessions must be conducted periodically for IHT to ensure clear understanding of current threats and risk.

## Roles and Responsibilities

1. All information users are responsible for reporting actual, suspected, threatened or potential cyber security incidents and for assisting with investigations as required.
2. IHT are responsible for handling incidents effectively.
3. Management personnel are responsible for ensuring that employees act in compliance with this policy and assist with investigations as required.
4. The directors will be responsible for overseeing management of the breach in accordance with the Incident Response Plan. Suitable delegation may be appropriate in some circumstances.

## Incident Response Plan

1. Incident Response Plan must be developed to address:
	* Organization roadmap for implementing its incident response capability.
	* The structure and organization of the incident response capability.
	* High-level approach concerning how the incident response capability fits the organization.
	* Entity’s mission, size, structure, and functions.
	* Reportable incidents.
2. Incident Response Plan must be updated and communicated in response to system and organizational changes.
3. The unauthorized disclosure and modification of the plan must be prevented.

##  Data Classification

1. <entity name>’s management should respond quickly and identify the data classification of the incident allowing quick incident response in a timely manner.
2. Classification is requested for all reported incidents to assess the risk and mitigation strategies.
3. Data classification shall refer to data categorises such as:
	1. Public Data: Information that can be made publicly or intended for public use without having any negative impact on the <entity name>.

Confidential/Internal Data: Information of more sensitive nature to the <entity name>. Limited access should be granted to employees who need to know as part of their roles within the <entity name>.

Highly confidential Data: Information that causes significant damage if breached to <entity name> operations, reputation, and/or business continuity. Access should be highly restricted.

## Incident Reporting

1. Actual, suspected, threatened or potential Incidents must be reported immediately to IHT for investigation
2. A formal report must be filled with details of security incidents including who is reporting the incident and what data classification is involved. Related personnel only must be reported to prevent sensitive data disclosure.
3. Related information such as system weaknesses must be reported in accordance with the reported Incidents.
4. IHT shall conduct an assessment to the incident to determine whether it is an incident or breach.
5. All incidents should be appropriately documented and logged to ensure consistency in terms of response, management and reporting.
6. Automated reporting of incidents by using email, automated incident response tools and programs

## Incident Classification

1. An incident must be classified when it involved actual or potential failure to meet the legislation to protect information or could lead to a data breach.
2. The data breaches and incident classification should be applied as follows:
	1. **Critical/Major Breach or Incident:** Breaches or Incidents deal with confidential information on a large scale where risk to the <entity name> is high.
	2. **Moderately Critical/Serious Incident:** Breaches or Incidents deal with confidential information on a medium scale where risk to the <entity name> is moderate.
	3. **Low Criticality/Minor Incident:** Incidents deal with personal or internal data on an individualized or small scale where risk to the <entity name> is low.

## Incident Response

1. Responding to incidents must be in accordance with the documented procedures.
2. Incident response management should involve the following activities:
	1. **Data Assessment, Containment and Recovery**

All security incidents should be analyzed, and a complete incident report must be generated by the <Insert Appropriate Role> and shared with relevant stakeholders. The analysis shall include a full assessment to the incident to decide whether it is a breach or not.

* 1. **Risk Assessment and Incident Scope**

All security incidents shall have a complete risk and scope analysis by the <Insert Appropriate Role> and must be documented and shared with relevant stakeholders.

* 1. **Incident Notification and Communications**

All moderately critical or critical security incidents must have communication plans documented by the <Insert Appropriate Role> senior leadership. The plans assist for appropriate incident management and progress communication to all relevant stakeholders.

* 1. **Evaluation and Response**

All moderately critical or critical security incidents must have post incident analysis done by the <Insert Appropriate Role> for appropriate documentation, analysis and recommendation on ways to limit risk and future exposure.

1.
2.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-