[Company Logo]

Security Incident Management Policy

The purpose of this policy is to ensure that the company reacts appropriately to any actual or suspected security incidents relating to information systems and data. Ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Document Owner
Head of IT/Security

[Company Logo]	**CONTROLLED DOCUMENT** **Security Incident Management Policy**	Document: Security Incident Management Policy Developed by: Reviewed by: Approved by:

Security Incident Management Policy
For
[Company Name]
Version: 1.0
Date: 08 March 2022
Next Review Date :

Note: Verify with the Policy Owner if this is the correct and latest version before use.

Revision History

Rev. #	Date	Modification Details	Page#	Suggested By	Reviewed By	Approved By
1.0		First Draft	NA			

[Company Logo]	**CONTROLLED DOCUMENT** **Security Incident Management Policy**	Document: Security Incident Management Policy Developed by: Reviewed by: Approved by:

Table of Contents

Purpose

The purpose of this policy is to ensure that the company reacts appropriately to any actual or suspected security incidents relating to information systems and data. Ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Scope

- All personnel, including employees, contractors, interns, vendors, and third parties with access to [Company Name]'s IT systems, networks, or data.
- All IT resources, including on-premises systems, cloud services, mobile devices, and applications owned or managed by [Company Name].
- All types of security incidents, including but not limited to:
    - Unauthorized access or data breaches
    - Malware infections or ransomware attacks
    - Phishing or social engineering attempts
    - Denial-of-Service (DoS/DDoS) attacks
    - Insider threats or misuse of privileges
    - Loss or theft of devices containing company data

Objective

Ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody and infrastructure.

Responsibility & Accountability

- Employees & Users: Must promptly report any suspected or actual security incidents to the designated IT Security team.
- IT Security Team: Responsible for investigating, containing, and mitigating security incidents, as well as documenting and reporting findings.
- Management/CISO: Accountable for overseeing incident response efforts, ensuring compliance with this policy, and communicating critical incidents to senior leadership and regulatory bodies if required.
- Legal & Compliance Teams: Ensure incident handling aligns with legal and regulatory obligations, including breach notifications.

Non-Compliance

Any Non-Compliance with this Security Incident Management Policy will be dealt with Disciplinary Action as decided by the organization and respective authorities.

Exceptions

Not Applicable.

Policy Statement

- **Security Incident Identification**

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorized access to data or information storage, or a computer system
- Unauthorized access or modification of Data or network or systems or services, or programs
- Advanced Persistent Threats
- Ransomware Infection
- Malware/Virus/Trojan/Worm: Outbreak
- Intentional or unintentional damage to access control and surveillance systems
- Unwanted disruption or denial of service to a system.
- Hacking
- Disclosure of sensitive data in the public domain

- **Responsibilities**

- Incidents are reported promptly and can be properly investigated
- Incidents are handled by appropriately authorized and skilled personnel
- Incidents are recorded and documented
- The impact of the incidents is understood, and action is taken to prevent further damage
- Evidence is gathered, recorded, and maintained in a form that will withstand internal and external scrutiny
- Effective, appropriate communication at all levels of an organization shall be implemented to limit the impact of security events.
- Who can access data relating to an incident under what circumstances, and what auditing is required to document the access, shall be specified.
- Any weaknesses in procedures or policies are identified and addressed.
- Similar incidents will not recur.
- Learning from the incidents is recorded.

Conclusion

This document provides an overview of the Security Incident Management Policy & its deliverables, the project team participants, and their roles and responsibilities. It is intended to assist Security Admin and developers of [Company Name] applications and to ensure a consistent approach to Security Incident management

<<< End of Document >>>