INFORMATION SECURITY INCIDENT MANAGEMENT POLICY/ PROCEDURE

Version Control

Current Version	**4.0**
Released on:	**01-07-2022**
Classification	**INTERNAL USE**

Version Number	Date of Release	Nature / Description of Change	Prepared / Changed By	Approved By
1.0	01-07-2022	Initial Release	Chintan Lad	Gautam Udani
2.0	01-07-2023	Annual Review- No Change	Chintan Lad	Gautam Udani
3.0	01-02-2024	Annual Review- No Change	Chintan Lad	Gautam Udani

4.0	01-02-2025	Annual Review- No Change	Chintan Lad	Gautam Udani
Scope				

This policy applies to all types of information security incidents occurring within Veefin Solutions Limited . This policy is applicable to all employees and related departments and functions that may come across any information security incident.

. PURPOSE

The purpose of this policy is to define the rules for managing information security incidents which include reporting, categorization, resolution, causal analysis, and planning corrective actions for avoiding recurrence. This document provides details of the processes being followed at Veefin Solutions Limited to ensure a prompt and effective response to any information security incident that has the potential to harm the Company.

. TERMS AND DEFINITIONS

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

ISG: Information Security Group

Information Security: Protection of confidentiality, integrity, and availability of information and information assets.

Event: An event is an exception to normal operation.

Incident: An incident is an event that indicates a harm or a has a high potential to cause harm to the company.

Security Event: A security event is a change in the everyday operations of a network or information technology service indicating that a security policy may have been violated or a security safeguard may have failed.

Information Security Incident: An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of any information security related policy.

Security Breach: A security breach is any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms. A security breach may be intentional or unintentional.

Data Breach: A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. A data breach may be intentional or unintentional.

Personal Data Breach: A data breach involving personal data or personally identifiable information of any living person or individual. The personal data breach also includes sharing or disclosure of personal data without the knowledge or consent of the person to whom it belongs.

RCCA: Root Cause Corrective Action – Process of conducting causal analysis of any incident to identify the root cause (why the incident occurred) and planning corrective action / preventive action so as to avoid recurrence of the incident.

Incident Handling Team: Team handling or resolving the Incidents. Incident Handlers maybe –

1. Human Resource for HR-related incidents

2. Admin Team for Physical Security related incidents

3. IT Team for IT related incidents

4. Product Team for Platform related incidents.

. RESPONSIBILITIES

The primary ownership of implementing this policy is with the Information Security Group (ISG).

All employees of Veefin Solutions Limited are responsible for reporting an event and the Incident handling team is responsible for responding to the event.

. POLICY

- Appropriate channels for reporting information security events and weaknesses shall be established.
- All employees and third-party users having access to the Veefin Solutions Limited 's information assets and information processing facilities shall receive adequate information related to reporting information security events and weaknesses.
- Information security events and incidents shall be reported as early as possible through the appropriate channel so that a quick response can be given by the company and further impacts can be prevented or reduced.
- All reported information security events and weaknesses shall be assessed by the Information Security Group to determine if they can be classified as information security incidents.
- Procedures shall be established to –
    - Contain the information security incident so that its further spread can be prevented.
    - Remediate the information security incident by eradicating the cause of the incident to ensure that the effects are eliminated, and further recurrence of such information security incident is prevented.
    - Recover from the incident by re-establishing the normal operations of the affected information assets or information processing facilities.
- Incidents shall be responded by an Incident Handling Team, as applicable. The Incident Handling Teams are identified as below –
    - Human Resource for HR-related incidents
    - Admin Team for Physical Security related incidents
    - IT Team for IT related incidents
    - Product Team for Platform-related incidents.
- All personnel involved in responding to an information security incident shall receive adequate training on procedures for responding to information security incidents.
- Evidence related to the information security incidents shall be collected and preserved for further analysis or reporting, as necessary.
- Knowledge gained from analyzing and resolving information security incidents shall be captured and used for reducing the likelihood or impact of future incidents.

. PROCEDURE

6.1Reporting an information security event or weakness

- Any detected information security event or weakness shall be reported through any of the following channels

- Ticketing tool – OpenProject
- Email – gautam@Veefin Solutions Limited .com
- In-person – Gautam Udani, Chief Operations Officer

- Following details shall be provided to facilitate appropriate analysis and response –
  - Name and contact details of the person reporting the information security event/weakness
  - Date and time of first identification of the event/weakness
  - Information system/information processing facility where the event/weakness is observed
  - Impacts (if known)
- If the event/weakness is reported through email, phone, or in-person, the Information Security Group shall report the event/weakness in the ticketing tool and assign a ticket to self.

6.2 Analyzing reported information security events or weaknesses

- The Information Security Group shall assess the reported event/weakness to determine if it can be classified as an information security incident. If it is identified as an information security incident, the Information Security Group shall mark it as an 'information security incident' or else assign the ticket to someone from the company who has authority over the subject.
- For identified information security incident, the Information Security Group shall conduct an impact analysis and document the impact in either of the following categories –
- **High Impact** – incidents that have a monumental/catastrophic impact on the company's business or services to its customers. E.g., Ransomware attack, DDoS attack, compromise of administrative privileges of core business applications, etc. ***Note****: in cases where such high impacting incidents have the potential to cause a complete shutdown/stoppage of the company's business or services to its customers, the Information Security Group may request the Business Continuity Team to initiate the Business Continuity Plan.*
- **Medium-Impact** – incidents that have a significant impact or have the potential to escalate to a monumental/catastrophic incident. E.g., an in-progress hacking attempt, virus infection detected on a few networked systems, etc.
- **Low** – incidents that are isolated in nature and may not have the potential to affect a significant number of users. E.g., virus infection on an end-user device, suspected or occurred unauthorized entry in the company's facility, etc.
- Based on the impact analysis, the Information Security Group shall assign the ticket to the Incident Handling Team with a priority level for the response based on the impact –
- **Priority Level 1** – needs to be responded to immediately (same day).
- **Priority Level 2** – needs to be responded to within 1 (one) business day.
- **Priority Level 3** – needs to be responded to within 3 (three) business days.

Note: Priority Levels are applicable for 'Remediation' only. In any situation, the containment must be done immediately.

6.3 Responding to the information Security Incident

- **Containment**: The Incident Handling Team shall take either of the following containment actions to prevent further damage from occurring –
  - **Short-term containment** – These are actions to cut off the attack or damage. E.g., isolating a network segment that is under attack or taking down production servers that have been hacked.
  - **Long term containment** – These are actions to temporarily fix the issue while working on a permanent solution. E.g., applying temporary fixes to affected systems to allow them to be used in production, while rebuilding a clean system, preparing to bring them online in the recovery stage of the response procedure.
- **Remediation**: Once the incident has been contained, the Incident Handling Team shall follow the following steps to remediate the incident –

    - **Analysis** – The root cause of the incident shall be determined through appropriate investigation of the incident.
    - **Eradication** – The root cause of the incident shall be addressed through appropriate application of procedural or technical measures. E.g., let's say that the hacker exploited the production server with the help of a known vulnerability existing in the operating system of the server, then an appropriate patch/update from the vendor is applied to ensure that the vulnerability is eliminated.
- **Recovery** – After remediating the incident, the Incident Handling Team shall restore the systems/facilities back to their normal state. For E.g., a hacked server may undergo clean build, patch management, restoration of configuration and data, etc., and then will get connected back to the network.

6.4 Post-incident procedures

- **Review** – The Information Security Group shall conduct a post-incident review to validate if the incident was effectively responded to or not. If it is determined that the incident was not addressed adequately, the Information Security Group shall require the concerned Incident Handling Team to reinitiate the 'Remediation' stage.
- **Archival of evidence** – The Information Security Group shall take a backup of all the evidence related to the incident reporting and response in a secure location so that in case of further escalations (e.g., to the customer, law enforcement or regulatory bodies, etc.), the evidence can be reproduced. All care shall be taken by the Information Security Group not to tamper with the evidence during such backup.
- **Breach notification** – If the incident involved a breach of customer data or personal data of any individual or group of individuals, the Information Security Group shall notify all such affected persons or entities using the Breach Notification Form.
- **Lessons Learnt** – The Information Security Group shall maintain conduct a retrospective session (meeting) with all the personnel involved in responding to the incident and capture the lessons learned during such response. These lessons learned shall be used by the Information Security Group to initiate further changes to the information assets or information process facilities to ensure that such or similar incidents do not occur in the future.