Information Security

MEIL Incident Management Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Incident Management Policy
DOCUMENT NO.	MEIL- POL/IM/05/V1

AUTHORISATION

	Prepared By	**Reviewed By**	**Approved By**
Name	Priyanka Haldankar	Anil Khedulkar	Giriraj Mohta
Designation	GRC Consultant	Manager - IT	Chief Finance Officer
Date	4-July-2025	24-Feb-2026	24-Feb-2026

SECURITY CLASSIFICATION: Internal

VERSION HISTORY

VERSION	DATE	PREPARED BY	CHANGES & REASONS FOR CHANGE
1.0	4-July-2025	Priyanka Haldankar	Initial Release

DISTRIBUTION LIST

Sr. #	Location	Department
1	All MEIL Locations	All Departments

Table of Contents

1. Purpose

This policy aims to ensure a consistent and effective approach to the management of information security events and incidents, including those related to personal data breaches, within the organization.

2. Scope

This policy applies to all IT and non-IT related information security events and incidents that affect the organization's systems, services, networks, physical security, and personnel.

3. Applicability

This policy is applicable to all the locations of Mahindra EPC Irrigation Limited.

4. Terms and Definitions

Terms	Definitions
Incident Assessment	The process of evaluating information security events to determine whether they constitute a security incident and the potential impact on the organization.
Incident Classification	The process of categorizing information security incidents based on their severity, impact, and urgency to determine the appropriate response.
Incident Management Plan	A documented plan that outlines the procedures for managing information security incidents, including preparation, detection, response, recovery, and post-incident activities.
Incident Response Team	A group of individuals, designated by the organization, who are responsible for managing the response to information security incidents
Information Security Event	Any observable occurrence in a system or network that may have implications for the security of information or information systems. Events may or may not lead to an incident but are assessed for potential impact.
Information Security Incident	An event that has the potential to impact the confidentiality, integrity, or availability of information assets and requires a response to manage and mitigate its effects.
Post-Incident Review	An analysis conducted after an incident has been resolved to identify the root cause, evaluate the effectiveness of the response, and identify improvements to prevent future occurrences.

5. Roles and Responsibility

Roles	Responsibilities
Information Technology	• Monitor systems and networks for security events and potential incidents. • Perform an initial assessment of detected events to determine if escalation to the MSolve Team is required. • Provide technical support and expertise to the MSolve Team during incident response and recovery operations. • Ensure that all information security systems are properly maintained and updated to prevent security incidents.
MSolve Team	• Serve as the primary point of coordination for all activities related to significant information security incidents. • Execute the incident response plan, including containment, eradication, and recovery from incidents. • Communicate with internal and external stakeholders, including management, employees, and possibly external authorities, about the status and resolution of incidents. • Document all incident response activities, decisions, and outcomes for post-incident review and evidence collection.
Users	• Report any observed or suspected information security events or incidents promptly through the established reporting mechanism. • Adhere to the Information Security Incident Management Policy and cooperate with the IRT during incident response activities. • Remain vigilant for signs of security events and maintain good information security practices to help prevent incidents.

6. Incident Management Policy

6.1 Information Security Incident Management Planning and Preparation

- A comprehensive incident management plan shall be developed and maintained, outlining the processes for incident detection, reporting, response, and recovery.
- The plan shall define roles and responsibilities for all stages of incident management, ensuring clear accountability and authority.
- Regular training and awareness programs shall be conducted to ensure that all personnel are familiar with the incident management procedures.
- The incident management plan shall be tested and reviewed annually to ensure its effectiveness and to make necessary adjustments.

6.2 Assessment and decision on information security events

- All information security events shall be assessed to determine whether they constitute a security incident.
- Criteria for making this determination shall be clearly defined and communicated to all relevant personnel.
- A designated team (Msolve) or individual shall be responsible for the assessment and categorization of security events.
- The decision-making process shall be documented and include steps for escalation where necessary.

6.3 Response to information security incidents

- Upon confirmation of a security incident, a structured response shall be initiated in accordance with the incident management plan.
- The response shall aim to contain, eradicate, and recover from the incident, minimizing impact on operations.
- Incident response activities shall be coordinated by the Incident Response Team
- The Incident Response Team shall communicate with relevant stakeholders, including management and external parties, as required by the nature of the incident.

6.4 Learning from information security incidents

- Following the resolution of an incident, a review shall be conducted to identify the root cause and to evaluate the effectiveness of the response.
- Actions shall be taken to prevent recurrence and to improve the incident management process.
- Lessons learned shall be documented and shared with relevant personnel to enhance the organization's security posture.
- The incident management plan shall be updated to reflect the knowledge gained from the review process.

6.5 Collection of evidence

- Procedures for the collection, handling, and safeguarding of evidence related to security incidents shall be established.
- Evidence shall be handled in accordance with legal requirements and organizational procedures to maintain its integrity and admissibility.
- The chain of custody for evidence shall be documented and maintained.
- Personnel involved in evidence collection shall be trained in proper procedures to ensure the validity and reliability of the evidence.

6.6 Information security event reporting

- All personnel should report observed or suspected information security events to the designated teams.

- All personnel shall be made aware of the reporting procedures and their importance to the organization's security.

6.7 Management of Non - IT Security Incidents

- Protocols for responding to unauthorized access, theft, vandalism, health and safety incidents and other physical security breaches shall be established.
- This process shall cover emergency response, medical intervention, investigation, and implementation of preventive measures to safeguard personnel health and safety.
- Incident management protocols related to human resources issues, such as harassment, discrimination, or insider threats, shall be clearly defined.

7. Exception

- Exceptions to this policy must be formally documented, reviewed, and approved by the IT Head, ensuring compliance with security policies while addressing specific operational or business requirements.

8. Disclaimer

- This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of is document is strictly prohibited and may be unlawful.