Information Security

MEIL Third Party Management Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Third Party Management Policy
DOCUMENT NO.	MEIL- POL/TPM//08/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

The purpose of the Third-Party Management Policy at MEIL is to safeguard the company's information assets by ensuring that all suppliers meet stringent information security standards. This policy outlines the responsibilities and expectations for securing sensitive data throughout the supply chain, from the initial supplier selection to the ongoing management and review of supplier services. It serves to protect against information security risks, maintain operational resilience, and ensure that supplier agreements and practices align with MEIL Company's commitment to data protection and security.

2. Scope

The scope of this policy extends to all the locations of Mahindra EPC Irrigation Limited.

3. Applicability

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

4. Terms and definitions

Terms	Definitions
Change Management	A structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state
ICT Supply Chain	Information and Communication Technology Supply Chain is a network of suppliers involved in delivering information and communication technology products and services
Non-Disclosure Agreement (NDA)	A legal contract establishing confidentiality between parties
Punitive Clauses	Provisions in a contract that impose penalties for non-compliance or breaches
Risk Assessments	The process of identifying and evaluating potential risks
Service Level Agreement (SLA)	A formal document that defines the level of service expected from a provider
Subcontracting	Outsourcing tasks or projects to third-party companies or individuals
Supplier	Entities that provide goods or services to a company
Vendors	Businesses or individuals that sell products or services

5. Roles and Responsibility

Commented [SM1]: TBU by Document Owner

Roles	Responsibilities
Service Provider / Third-Party Vendor	• Delivers contracted services in adherence to agreed-upon SLAs and security requirements outlined by MEIL • Inform MEIL's contracting department of any intent to subcontract portions of work, providing complete details of the arrangements • Undergoes regular security evaluations and compliance checks as stipulated by M&M Central Team • Ensures their personnel receive necessary security awareness training and that all information security policies of MEIL are followed diligently

6. Third Party Management Policy

6.1 Information Security Policy for Third Party Management

- MEIL shall identify and maintain a list of all service providers and a risk analysis of all the listed third parties shall be carried out before finalizing the contract.
- The third party shall inform the contracting department of MEIL in case the vendor subcontracts a part of the work where information is being shared and the party should also provide all details of the sub-contracting arrangement.
- The ultimate responsibility of subcontracted work shall lie with the third party.
- The third party shall be responsible to disclose involvement of sub-contractor with the contracting department before signing the agreement.
- MEIL shall ensure that physical / logical access to third parties is given based on business need are taking appropriate approvals.
- MEIL shall periodically review and monitor supplier's adherence to information security requirements mentioned in contract agreement.
- MEIL shall periodically monitor the access granted to the supplier.
- When termination of services of any third party takes place, MEIL shall
    - revoke physical / logical access of the supplier as per the defined access management procedure. (refer access management procedure)
    - collect all the assets provided to the supplier before termination of services. (refer asset management procedure)

6.2 Addressing Security within Supplier Agreements

- MEIL shall ensure that services from an outsourced vendor are governed by a Service Level Agreement (SLA) which should include relevant information security requirements such as Intellectual Property Rights, Code of Conduct, Confidentiality, etc.
- All relevant information security requirements shall be established and agreed with the suppliers that may access, process, store, communicate MEIL's information or provide IT infrastructure components to MEIL.
- MEIL shall ensure that access to information and information processing facility to third parties shall be provided only after signing of a formal contract / NDA containing the terms for granting of access.

6.3 Management of Information Security in Information and Technology Communication (ICT) Supply Chain

- Supplier contracts must include requirement to manage the risks to information security that are associated with the supply chain of ICT services and products.

- MEIL shall monitor if the delivered information and communication technology product or services meet the stated security requirements.

6.4 Monitoring and Reviewing of Supplier Services

- MEIL shall monitor and review supplier services to ensure compliance with the information security terms and conditions outlined in agreements.
- MEIL shall ensure that period review is conducted to review information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered.
- Any identified irregularities shall be escalated to the concerned stakeholders.

6.5 Management of Supplier Service Changes

- Suppliers must manage any changes to their services, including updates to their information security measures, with care for the importance of the business information, systems, and processes involved, and shall re-evaluate the risks accordingly.

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.