Information Security

MEIL Network Security and Communication Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Network Security and Communication Policy
DOCUMENT NO.	MEIL- POL/NSC/11/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 this policy is to safeguard the confidentiality, integrity, and availability of MEIL information and network infrastructure. It aims to establish secure practices for information transfer, network access, and data protection, ensuring compliance with legal and regulatory requirements.

2. Scope

The scope of this policy extends to all MEIL employees, contractors, and third-party service providers with access to the company's network and information systems.

3. Applicability

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

4. Terms and Definitions

Terms	Definitions
Cabling Security	Measures taken to protect physical cables that transmit data from interception, damage, or unauthorized access.
Information Transfer	The process of moving data from one location to another, whether within the organization or to external parties.
Intrusion Detection System (IDS)	A device or software application that monitors a network or systems for malicious activity or policy violations.
NOC (Network Operations Center)	A centralized location where IT professionals directly support the efforts of remote monitoring and management of client networks.
Remote Diagnostic Port	A network port used to access, diagnose, and manage devices remotely.
Secure Configuration	The administrative and technical controls that are applied to network devices and services to reduce vulnerabilities and protect against unauthorized access.
Two-Factor Authentication	A security process in which the user provides two different authentication factors to verify themselves.
V-LAN (Virtual Local Area Network)	A logical subdivision of a network that groups together a collection of devices from different physical LANs.
WAN (Wide Area Network)	A telecommunications network that extends over a large geographic area for the purpose of computer networking.

Web Filtering	The technique of blocking access to web content based on a set of user-defined rules, often used to restrict access to sites that are considered harmful or not related to business needs.

5. Roles and Responsibility

Roles	Responsibilities
NOC (Network Operations Center)	• Continuously monitor network performance, security alerts, and system health to ensure high availability and quick response to issues • Manage and respond to network incidents, document actions taken, and follow up with post-incident analysis and reporting • Define secure configuration standards, document procedures, and ensure new installations align with these standards. • Implement and maintain network segregation strategies, including V-LAN configurations, to ensure proper isolation of network segments • Maintain detailed connectivity diagrams and operational procedures for the network infrastructure under NOC management • Assess and project network capacity demands to ensure scalability and performance
Information Technology	• Ensure adherence to the Network Security and Communication Policy across the organization, including all local and wide area networks • Oversee the security of the physical cabling infrastructure, ensuring protection and adherence to cabling guidelines. • Authorize hosting/collocation of IT equipment at remote locations and maintain asset management records.

6. Network Security and Communication Policy

6.1 Information Transfer

- Information transfers must be secure, controlled, logged, and authorized by MEIL IT.
- Transfers across different security domains must be controlled and logged.
- System documentation copies shall be kept off-site for disaster recovery, with restricted access.
- Routing configurations must prevent the relay of routing information to third-party/shared networks.
- Network address translation may be used to isolate networks and prevent propagation of routes wherever applicable.

6.2 Confidentiality or Non-Disclosure Agreements

- Confidentiality agreements are mandatory for all personnel with access to sensitive information.
- NDAs must be reviewed periodically and updated as necessary to remain compliant with legal and regulatory requirements.

6.3 Cabling Security

- Physical cabling carrying sensitive information must be protected from interception or damage.

6.4 Network Security

- MEIL IT shall be responsible for the management and monitoring of the respective network segments.
- The WAN shall be centrally managed by MEIL IT.
- Network devices must be secured with strong authentication and access control mechanisms.
- Regular network security assessments must be conducted to identify and remediate vulnerabilities.
- MEIL IT shall authorize for hosting/collocating IT equipment at remote locations with third party. MEIL IT shall be responsible for asset management of the same.
- A formal security analysis shall be carried out before awarding any facility management contract. All relevant security clauses shall be included in the service level agreements and annual maintenance contracts.

6.5 Security of Network Services

- Network services must be configured securely, with standards defined by M&M Central Team.
- Unused network services and ports must be disabled to reduce the attack surface.
- Critical network elements such as routers, switches, firewalls, IDS, and servers shall be configured as per configuration guidelines.
- Standard for secure configuration of MEIL's network/Information infrastructure/systems shall be defined and documented by SECTORIT/ MEIL IT.
- SECTORIT/ MEIL IT shall be responsible to align the configuration of all newly installed MEIL's network/information infrastructure/systems to the configurations outlined in the secure configuration standard.

6.6 Segregation of Networks

- Networks must be segregated physically or using V-LAN architecture, as established by the NOC at Kandivali Data Center or the local network administrator.
- Controls such as firewalls and access lists must be used to enforce segregation.
- Segregation of network shall be done either physically between various business entities of MEIL or V-LAN architecture shall be established by the NOC at Kandivali Data Center or the local network administrator.

6.7 Web Filtering

- Web filtering mechanisms shall be implemented and managed by M&M Central Team to restrict access to unauthorized websites.
- Policies for web filtering must be established and communicated to all users, and compliance must be monitored.
- Access to the Internet and Third-party networks shall be restricted and managed through proper perimeter security controls, such as routers, firewalls, and intrusion detection systems (IDS).

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.