

Information Security

MEIL Physical & Environmental Security Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Physical & Environmental Security Policy
DOCUMENT NO.	MEIL- POL/PES/12/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	4
2. Scope	4
3. Applicability	4
4. Terms and Definitions	4
5. Roles and Responsibility	5
6. Physical and Environmental Security Policy	5
6.1 <i>Physical Security Perimeters</i>	5
6.2 <i>Physical Entry</i>	5
6.3 <i>Securing Offices, Rooms, and Facilities</i>	6
6.4 <i>Physical Security Monitoring</i>	6
6.5 <i>Protecting Against Physical and Environmental Threats</i>	6
6.6 <i>Working in Secure Areas</i>	6
6.7 <i>Clear Desk and Clear Screen Policy</i>	7
6.8 <i>Equipment Siting and Protection</i>	7
6.10 <i>Supporting Utilities</i>	7
6.11 <i>Equipment Maintenance</i>	7
6.12 <i>Secure Disposal or Re-use of Equipment</i>	7
7. Exception	7
8. Disclaimer	Error! Bookmark not defined.

1. Purpose

The Purpose of this document is to address all the aspects involved in prevention of unauthorized physical access, loss, theft, damage and interference to information and IT systems/assets, which lead to interruption of business activities or financial loss of information value.

2. Scope

The scope of this document 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
Access Control	A security measure that restricts access to specific areas, assets, or information, ensuring that only authorized individuals can enter designated spaces.
Common Area	A designated area within an organization's premises that is accessible to both employees and visitors. Examples include canteens, discussion rooms, and public hallways.
Data Centre/ Server Room	A secured area that houses the critical computing infrastructure, including servers, storage devices, and network systems, requiring strict access control.
Environmental Threats	Risks that arise from natural or man-made disasters, such as fire, flood, earthquake, or civil unrest, which can impact the physical security of an organization.
Physical Security	Measures taken to protect an organization's physical premises, assets, and information from unauthorized access, damage, theft, or other security threats.
Restricted/ Secure Area	An area designated for sensitive information or critical infrastructure that requires heightened access controls to ensure only authorized individuals can enter.
Surveillance System	A set of tools, such as cameras and monitoring software, used to monitor and record activities within an organization to prevent and respond to security breaches.
Work Area	Areas where employees perform their duties, and which may be accessible to authorized visitors or third-party service providers.

5. Roles and Responsibility

Roles	Responsibilities
Security Officer/ Personnel	- Monitor surveillance systems (CCTV) and respond to alarms or intrusions promptly. - Enforce access control measures and manage visitor passes. - Conduct regular security patrols to identify vulnerabilities. - Investigate suspicious activities and escalate the incidents when it is needed. - Maintain access logs to ensure compliance with security protocols.
Local Admin / Facility Manager	- Ensure physical protection of premises, including secure areas and equipment. - Maintain barriers to prevent unauthorized access and ensure restricted areas are clearly marked. - Oversee the issuance and collection of identification badges for employees, contractors, and visitors. - Ensure proper inspection and registration of incoming and outgoing materials.
Emergency Response Team	- Develop and implement response plans for security breaches, environmental threats, and disasters. - Conduct regular training drills and ensure emergency systems (e.g., alarms, fire extinguishers) are operational. - Coordinate with local authorities for serious threats requiring external intervention.
Administration Team	- Issue visitor passes and maintain access logs. - Monitor and report on the effectiveness of physical security systems in coordination with IT and security teams.

6. Physical and Environmental Security Policy

6.1 Physical Security Perimeters

- Physical barriers shall be established around the organization's business premises and information processing facilities to provide physical protection.
- The nature and extent of these barriers shall be determined by the specific requirements of each location, in accordance with the assessed risks.

6.2 Physical Entry

- All MEIL employees shall be issued identification badges to regulate access to the premises.
- Visitors and contractors shall receive temporary badges or gate passes.

- It is mandatory for all badge holders to wear and visibly always display their badges within MEIL premises.
- A visitor's pass shall be issued to all visitors. Visitors are permitted to carry their laptops, removable storage devices like pen drives, CDs, and photography equipment including mobile phones with cameras, etc., after declaring them.

6.3 Securing Offices, Rooms, and Facilities

- Access to various areas within the premises shall be categorized and controlled.
- Employees shall have access to work areas, while visitors on official business may enter only upon confirmation from the relevant MEIL Executive.
- Entry passes for regular third-party service providers shall be issued based on departmental recommendations.
- Areas will be classified as common area, work area, and restricted area.
- **Common Area**
 - Visitors will be allowed in this area, which includes the canteen, discussion rooms, and interconnecting passages outside buildings/workshops segregated from work areas and restricted areas.
- **Work Area**
 - Admin shall issue entry passes to third parties who are required to enter the work area regularly for rendering service based on the recommendations of the Departmental Head.
 - Admin shall include appropriate clauses in contracts with contractors to ensure the protection/safety of information assets.

6.4 Physical Security Monitoring

- Surveillance systems, including CCTV, shall be implemented and managed by the local admin.
- These systems shall provide monitoring of the organization's physical environment to detect and respond to security incidents.
- CCTV surveillance, if installed by the location, shall be managed by the Local admin head.

6.5 Protecting Against Physical and Environmental Threats

- The threats arising from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be analyzed & documented, and physical protection against these environmental threats shall be designed and applied.
- The locational DRP shall be referred to address such risks; in cases where such risks have already been addressed in documents complying with other standards (e.g., ISO 9001, ISO 14000, ISO 18000), the location representatives shall maintain and provide adequate reference of those documents to complement the BCP/DR plan prepared to address threats as per information security.

6.6 Working in Secure Areas

- Access to secure or restricted areas, where sensitive and critical information is processed or stored, shall be strictly controlled.
- Entry to these areas shall be regulated through mechanisms such as swipe cards or assigned security personnel, in accordance with the entity.

6.7 Clear Desk and Clear Screen Policy

- **Document and Media Storage**
 - All documents and computer media containing confidential or business-critical information shall be stored under lock and key.

6.8 Equipment Siting and Protection

- Equipment shall be properly protected to prevent loss, damage, or compromise of assets that leads to disruption of business activities.
- Proper controls shall be in place in the Data Centre/Server Room to ensure that power and telecommunication lines are protected from interception and damage.

6.9 Supporting Utilities

- Critical equipment shall be equipped with suitable backup power supplies to ensure continuous operation and protection against power failures.

6.10 Equipment Maintenance

- Maintenance of all equipment within the Data Centre/Server Room shall be conducted in accordance with the supplier's recommendations to ensure ongoing protection and operational integrity.

6.11 Secure Disposal or Re-use of Equipment

- The disposal or re-use of information processing equipment shall be conducted as per procedures defined by MEIL IT.
- This includes the secure formatting or physical destruction of storage devices to prevent the leakage of information.

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 this document is strictly prohibited and may be unlawful.