Information Security

MEIL Asset Management Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Asset Management Policy
DOCUMENT NO.	MEIL- POL/ASM/10/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 Asset Management Policy is to define the responsibilities and establish the processes for the effective management of MEIL's information and associated assets. It aims to safeguard these assets against unauthorized use, disclosure, alteration, and destruction, thereby supporting the organization's operational integrity and maintaining the confidentiality and availability of critical information.

2. Scope

This policy applies to all assets owned, leased, or otherwise used by MEIL, including but not limited to hardware, software, documentation, and intellectual property.

3. Applicability

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

4. Terms and Definitions

Terms	Definitions
Asset Inventory	A comprehensive list that includes all information and associated assets of the organization, detailing asset type, location, owner, and other relevant information.
Asset Ownership	The assignment of responsibility for an asset to a primary owner, who is accountable for the asset's control, maintenance, and security throughout its lifecycle.
Handling Procedures	Documented guidelines that describe the processes for the storage, transmission, and secure destruction of information assets, in line with their classification.
Incident Response Procedures	The documented processes that outline the steps to be taken in response to security incidents, including the reporting and investigation of unreturned assets.
Reclassification	The process of reviewing and adjusting the classification of information to ensure it remains appropriate as organizational needs or the risk environment change.

5. Roles and Responsibility

Roles	Responsibilities
Information Technology	• Maintain a comprehensive and accurate inventory of all IT assets, documenting ownership, location, and status. • Implement security controls to protect IT assets and ensure their proper configuration and maintenance. • Monitor and enforce compliance with the Asset Management Policy, addressing any violations or security incidents.
Users	• Comply with all aspects of the Asset Management Policy, including acceptable use and security protocols. • Report any security incidents, loss, or suspected misuse of IT assets to the IT team immediately. • Return all IT assets and remove any stored information upon termination or reassignment, in accordance with the offboarding process. • Handle IT assets with care, avoiding any actions that could compromise asset security or integrity.
Human Resource	• Work with the IT team and management to enforce asset management policies, including addressing non-compliance as a disciplinary matter. • Integrate asset management responsibilities into onboarding and offboarding processes, including the return of assets.

6. Asset Management Policy

6.1 Inventory of Information and Other Associated Assets

- An up-to-date inventory of all information and associated assets shall be maintained, including details such as asset type, location, owner and other details.
- Asset ownership shall be clearly defined, with each asset assigned a primary owner responsible for its control and maintenance.
- The inventory shall be reviewed and updated regularly to reflect any changes in assets or ownership.
- Periodic audits shall be conducted to ensure the accuracy of the asset inventory and to reconcile any discrepancies.
- Information assets include assets in electronic, paper, voice, or any other media such as tapes, CDs, etc. IT assets include software assets (application and system software), hardware assets (desktops, laptops, servers, routers, switches/hubs, leased line modems, backup devices, etc.), removable media (backup tapes, CDs, Hard Drive etc.), and equipment (Access Control Machines, CCTV Cameras, Server Racks, UPS, Generators, Precision ACs, etc.).
- To maintain security and operational integrity, all IT assets must undergo structured, risk-based hardening before deployment and throughout their lifecycle. Hardening involves applying secure configurations to reduce vulnerabilities—such as disabling unused services, removing default accounts, enforcing MFA, using secure protocols, and applying patches.

- Baseline hardening standards shall be defined for each asset category, aligned with frameworks like CIS Benchmarks, NIST SP 800-82, and OEM guidance. These standards will be reviewed regularly to address evolving threats and requirements.

6.2 Acceptable Use of Information and Other Associated Assets

- Acceptable use policies shall be established to define proper use of information and associated assets.
- Installation, processing, handling, transfer, and storage of IT assets shall be in accordance with the classification levels assigned to those assets
- New server hardware installations shall be done in accordance with the process defined
- All users of information assets shall receive training on acceptable use policies and handling procedures.
- Customer access to information shall be granted only after security requirements are addressed, and all 'Confidential' and 'Internal' rated information shall be made available to other organizations only after obtaining a formal Non-Disclosure Agreement (NDA) or after including security clauses in the information exchange agreements/documentation.
- Confidential information received from any organization shall be classified as 'Confidential' and accorded the same level of security as MEIL's 'Confidential' information.
- Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
- Violations of acceptable use policies shall be addressed promptly and may result in disciplinary action.
  Refer Acceptable Usage Policy

6.3 Return of Assets

Commented [SM1]: TBD with MEIL IT

- Procedures shall be established for the return of all organizational assets upon the termination or change of employment, contract, or agreement.
- A formal process shall be established to ensure the timely return of assets and to account for all assets upon exit.
- The process shall include a checklist to verify the return of all issued assets and the removal of access rights.
- Unreturned assets shall be reported and investigated in accordance with the organization's incident response procedures.
- The HR department shall inform the corresponding IT, Finance, and Administration departments about employees leaving or being terminated from the organization to facilitate the full and final settlement and ensure the handover of IT and information assets.

6.4 Classification of Information

- An information classification scheme shall be developed to categorize information based on its need for confidentiality, integrity, and availability.
- The classification scheme shall be regularly reviewed and updated to reflect changes in the organizational environment or risk profile.
- Information owners shall be responsible for classifying information at the time of creation or receipt.

- Periodic reclassification reviews shall be conducted to ensure that the classification remains appropriate over time

6.5 Labelling of Information

- Labeling procedures shall be implemented to ensure that information is marked in a manner that indicates its classification and handling requirements.
- Labels shall be applied to both physical and electronic information assets where feasible and consequences are limited.
- Users shall be trained to recognize labels and to understand the associated handling requirements.
- The effectiveness of the labeling procedures shall be monitored, and non-compliance shall be addressed through awareness programs.
- Information classified as 'Confidential' or 'Highly Confidential' may be labeled as such, or location units can prepare their own labeling schema.

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.