Information Security

MEIL Access Control Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Access Control Policy
DOCUMENT NO.	MEIL- POL/AC/09/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 Access Control Policy is to define the requirements for granting, managing, and revoking access to MEIL's information and information assets. This policy aims to ensure that access is provided in a secure and controlled manner, based on the principles of least privilege and need-to-know, to protect the confidentiality, integrity, and availability of information. It establishes a framework for identity management, authentication, access rights management, and the use of privileged utility programs, thereby safeguarding against unauthorized access and misuse of MEIL's information systems and resources.

2. Scope

This policy applies to all users, including employees, consultants, contractors, and third parties, who have access to MEIL's information systems and IT assets. It encompasses all hardware, software, network infrastructure, and data owned or managed by MEIL. The scope extends to all forms of use, whether conducted on-premises or remotely, and includes personal devices used for business purposes.

3. Applicability

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

4. Terms and Definitions

Terms	Definitions
Access Control	• The process of granting, managing, and revoking access to information and information assets based on defined procedures and requirements.
Access to Source Code	• Permission to view, modify, or manage the source code of applications or systems, which is restricted to prevent unauthorized changes.
Authentication Information	• Credentials used to verify a user's identity, such as passwords or other forms of authentication factors.
Identity Management	• The administrative process that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.
Information Access Restriction	• Controls put in place to limit access to applications, infrastructure, and data according to user roles and responsibilities.
Information Assets	• Any data, information, systems, networks, and physical files that are owned or used by MEIL.
Least Privilege	• The practice of providing the minimum levels of access - or permissions - needed for users to perform their job functions.
Need-to-Know Principle	

	• A security concept where access to information is restricted to individuals who need the information to perform their job duties.
Physical Access Control	• Measures and devices used to control physical access to MEIL's facilities and information assets, such as access cards.
Privileged Access Rights	• Special rights granted to certain users, allowing them to perform administrative tasks or access sensitive information.
Secure Authentication	• The process of verifying the identity of a user or system in a manner that ensures the credentials are protected and the session is secure.
Shared IDs	• User IDs that are shared among multiple users, permitted only for business or operational reasons with proper approval.
Unique User ID	• A specific identifier assigned to each user to uniquely authenticate and track their actions within the system.
User Registration Process	• The formal procedure through which a new user is granted access to MEIL's systems and information assets.

5. Roles and Responsibility

Roles	Responsibilities
End Users	• Adhere to the Access Control Policy by safeguarding authentication information, such as passwords, and using access privileges responsibly. • Report any suspected security incidents or policy violations to the appropriate authority within the organization. • Participate in security awareness training to understand their role in maintaining effective access control.
Department Heads	• Periodically review the access rights and privileges of users within their departments to ensure they are appropriate and necessary for job functions. • Report significant changes in user duties or employment status to Sector IT/MEIL IT to facilitate the adjustment of access rights. • Ensure that departmental practices align with the Access Control Policy and contribute to the organization's overall security posture.
System Administrators	• Execute user ID creation, deletion, and privilege change activities as directed by Sector IT/MEIL IT.

	• Securely log into the System Network and ensure the confidentiality and integrity of authentication information. • Manage the use of system utility programs, ensuring they are used in compliance with the Access Control Policy and only with prior approval.
Sector IT/Mahindra IT	• Administer user ID creation, deletion, and privilege changes for all servers and application systems in accordance with the Access Control Policy. • Conduct regular reviews of user access rights to ensure compliance with the principles of least privilege and need-to-know. • Monitor and log the use of privileged User-IDs and perform audits to detect and prevent unauthorized access.
HR Department	• Collaborate with Sector IT/MEIL IT to manage the user registration process and the issuance of physical access controls. • Promptly report changes in employment status, such as terminations or role changes, to ensure timely adjustment or revocation of access rights. • Ensure that access control procedures are followed during the onboarding and offboarding of employees.

6. Access Control Policy

6.1 Access Control

- Access to information and information assets shall be granted based on business requirements, the need-to-know principle, and the need to perform tasks, as well as upon the classification of the information and the risks to it.
- Procedures to authorize access shall be defined and documented, with the minimum level of privilege/access necessary to perform job responsibilities.
- Network access to MEIL IT resources is governed and details the security requirements for network connectivity and usage.
  Refer Asset Management Policy

6.2 Identity Management

- MEIL employees shall be granted access through a formal user registration process. Unique user IDs shall be used to enable users to be linked to and held responsible for their actions.
- The use of shared IDs shall be permitted only where necessary for business or operational reasons and must be approved and documented.
- The issuance of physical access control to MEIL users should be linked to the created user ID and initiated by the respective HR department or, in their absence, the head of the department responsible.
- User ID creation and deletion shall be executed promptly upon notification from the Human Resources Department and/or department head to ensure timely access control.

6.3 Authentication Information

- Each IT user shall be identified to the network/system by a unique User-ID and a personal secret password, which will be required for access to network/systems.
- No generic NT User-IDs shall be permitted except for administrators on specific applications.
- An interactive and quality password mechanism shall be deployed, and password usage shall be in

accordance with the recommended practices as per the MEIL Password management guidelines.

- The password mechanism shall be interactive and adhere to quality standards as outlined
  - Password Length – Minimum 12 characters
  - Password Complexity – At least one numeric character [0-9], At least one lowercase character [a-z], At least one special character [e.g. @, #, $], At least one upper character [A-Z], Password should not contain first or last name
  - Wrong Password Attempt – 5 wrong attempts (System will be locked)
  - Password cannot be used – Last 5 password cannot be used
  - Password valid till – 90 days (Must change within 90 days)
- Users are required to promptly report any suspected security incidents or vulnerabilities affecting MEIL's information systems to the IT helpdesk or designated security personnel.
- A clear process for incident reporting shall be established and communicated to all users to facilitate quick response and mitigation of security threats.
- Users shall not share their passwords with others and shall be accountable for any use or misuse by another party.

6.4 Access Rights

- Access rights shall be granted on a "Least Privilege" and "Need-to-Know" basis, reviewed regularly, and maintained in a central record.
- The privileges assigned to users shall be periodically reviewed by the department head/sector IT/MEIL IT as applicable.
- In the case of termination or change of employment, access rights/privileges shall be formally reviewed and accordingly removed or adjusted.
- Any changes in the employment status of users, including consultants, contractors, and temporary staff, must be reported immediately by the respective Human Resources Department to Sector IT/MEIL IT for appropriate adjustment of access rights.
- MEIL management reserves the right to revoke user privileges at any time for conduct that disrupts the normal operation of MEIL information systems or negatively impacts other users.
- Upon the departure or transfer of an IT user, their computer and paper files must be reviewed by their immediate superior to determine custodianship or appropriate disposal methods.
- Access privileges assigned to various roles shall be audited annually to ensure ongoing appropriateness and to identify any necessary adjustments.
- All access rights shall be reviewed quarterly to ensure that unauthorized access have not been obtained.

6.5 Privileged Access Rights

- Privileged access rights shall be granted only after approval from authorized personnel, with records maintained for all privilege access granted, changed, or revoked.
- The number of privileged User-IDs shall be strictly limited to those individuals who absolutely need such privileges for business purposes or system administration.
- Privilege access rights shall be reviewed quarterly to ensure that unauthorized privileges have not been obtained.
- All privileged User-ID activities shall be logged, and the logs shall be regularly reviewed and monitored by authorized personnel to ensure accountability and traceability of actions taken with elevated privileges.

6.6 Information Access Restriction

- Access to MEIL's applications and infrastructure shall be controlled to ensure that access is granted as per the user's job roles and responsibilities.
- Access to information asset configuration shall be restricted to administrators only.

- Appropriate controls shall be defined to restrict access to information and information assets, including role-based access control, read/write/delete/execute permissions, and physical/logical access controls to sensitive applications and data.
- For sensitive systems, a dedicated (isolated) computing environment shall be established.
- Access to production databases shall be through approved channels only, with direct database access utilities in the production environment prohibited unless authorized by MEIL IT.
- In-bound dial-up or Internet privileges for third-party vendors or business partners shall be granted only after a risk evaluation by MEIL IT and must be limited to specific individuals and time periods necessary for approved tasks.
- Inactive user sessions shall be automatically terminated after a predefined period of inactivity to reduce the risk of unauthorized access.
- Connection time restrictions shall be implemented for high-risk applications to provide additional security and control over access times.
- Sensitive systems shall be hosted within a dedicated computing environment, established and maintained.

6.7 Access to Source Code

- Access to program source code shall be restricted to prevent unauthorized changes and protect sensitive information.
- Program source code libraries shall be maintained in a secure environment and accessible only to authorized personnel.
- An appropriate version management process shall be implemented, and audit trails shall be enabled and reviewed periodically to prevent unauthorized access.
- Access to program source code shall be restricted and managed.
  Refer System Acquisition, Development and Maintenance Policy

6.8 Secure Authentication

- Logon to domains and applications through terminals shall be conducted in a secure manner, disclosing minimum information about the system.
- A general notice warning that the system shall be accessed only by authorized users shall be displayed.
- The number of unsuccessful attempts shall be limited, as well as the maximum and minimum time required for the log-on procedure.
- Details of the last successful/unsuccessful logon shall be displayed and logged.

6.9 Use of Privileged Utility Programs

- The use of system utility programs, maintenance software, and other products that allow bypassing of application controls shall be strictly controlled and used only by authorized personnel with prior approval from the Head of Business Solutions. Privileged users (System Administrators) shall be securely logged to the System Network, and all general User-IDs not used for a period of 90 days shall be temporarily suspended.
- System privileges shall be granted only under special circumstances with explicit permission from Mahindra IT.
- Use of system utility programs and maintenance software shall be strictly controlled, requiring prior approval from the Head of Business Solutions. to prevent unauthorized bypassing of application controls.
- User IDs that have not been utilized for a period of 90 days shall be temporarily suspended to maintain system security.
- The use of system utility programs and maintenance software shall be strictly controlled and only used

by authorized personnel with prior approval from the Head of Business Solutions.

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.