

Information Security

MEIL Human Resource Security Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Human Resource Security Policy
DOCUMENT NO.	MEIL- POL/HRS/04/V1

AUTHORISATION

	Prepared By	Reviewed By	Approved By
Name	Priyanka Haldankar	Kapil Nayak	Prashant Deshmukh
Designation	GRC Consultant	Deputy Manager - HR	Senior Manager- HR
Date	4-July-2025	29-July-2025	29-July-2025

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. Human Resource Security Policy	6
6.1 <i>Prior to Employment</i>	6
6.2 <i>During employment</i>	6
6.3 <i>Termination and Change of Employment</i>	7
7. Exception	7
8. Disclaimer	7

1. Purpose

The purpose of the Human Resource Security Policy for MEIL is to safeguard the organization's information assets by ensuring that all employees and contractors are aware of and adhere to the company's information security expectations. This policy outlines the responsibilities and expected behaviors of staff throughout their employment lifecycle, from pre-employment screening to post-termination obligations, to prevent unauthorized access, disclosure, alteration, or destruction of information assets. It serves as a foundation for maintaining a secure and trustworthy workforce that is aligned with MEIL Company's commitment to protecting sensitive information.

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
Access rights	Access Rights are the permissions an individual user or a computer application holds to read, write, modify, delete, or otherwise access a computer file.
Corrective & Preventive actions	Measures taken to fix identified issues and avoid the recurrence of problems to improve processes and performance.
Disciplinary Process	The formal procedure for addressing employee violations of company policies or standards, potentially leading to sanctions.
Human Resource	The department focused on managing and supporting a company's workforce, including recruitment, employee relations, and compliance with labor laws.
Information assets	Valuable data and knowledge owned by an organization that requires protection due to its importance to business operations.
Risk	The potential for adverse impacts to an organization, often necessitating strategies for assessment, mitigation, and management.
Screening	The evaluation process before hiring to ensure suitability and compatibility of candidates with job requirements and organizational culture.

5. Roles and Responsibility

Roles	Responsibilities
HR, Administration Team	• Maintain an up-to-date list of roles and responsibilities for positions within the organization to ensure clarity in job functions and security requirements. • Collect and verify legal documents such as identity proofs, educational qualifications, and work permits for applicants as part of the pre-employment screening process. • Conduct thorough background checks for final candidates, including previous employment verification, education verification, and work permit verification for foreign employees. • Administer confidentiality agreements and contractual documentation for new hires, ensuring that all information security obligations are communicated and understood.
Department Head/ Department Representative	• Oversee annual performance reviews for departmental employees, providing feedback on their work quality, reliability, and adherence to security practices. • Conduct additional performance reviews following the completion of an employee's probation period to ensure they meet the organization's standards and expectations. • Set and review performance goals during evaluative meetings, documenting outcomes, and new objectives for future assessment periods. • Ensure team members receive proper training and are aware of their information security responsibilities and manage improvement points highlighted during performance reviews.
Contractors, Suppliers, and Other Third-Parties	• Adhere to the terms and conditions stipulated in contracts, including confidentiality and security commitments. • Cooperate with MEIL's security protocols and report any security concerns or incidents to the appropriate teams. • Ensure that all necessary documents, including non-disclosure agreements, are signed, and kept updated. • Remain informed and compliant with the information security awareness programs provided by MEIL.
Employees	• Follow the security guide and other policies. • Sign confidentiality agreements and employment contracts. • Attend and complete information security training during induction. • Comply with information security & other responsibilities and contractual terms.

6. Human Resource Security Policy

6.1 Prior to Employment

- **Screening**
 - MEIL shall establish a formal process of on-boarding/off-boarding.
 - Background verification checks on candidates for employment shall be carried out prior to joining and in accordance with relevant laws, regulations, ethics, and proportional to the business requirements.
- **Terms and conditions of employment**
 - MEIL shall require all new employees, suppliers, and third-party associates to sign the terms and conditions of employment, which will clearly define their information security responsibilities.
 - The terms and conditions shall detail the legal responsibilities and rights of employees, ensuring compliance with legislative and regulatory requirements.
 - Signatories shall be responsible for the classification and management of MEIL's data, as per the terms and conditions, to maintain the integrity and confidentiality of company information.
 - A confidentiality agreement, forming part of the terms and conditions, will be mandatory for all signatories to uphold the security of proprietary and confidential information throughout and beyond the term of their engagement with MEIL.
 - The Human Resources department shall securely retain a signed copy of the terms and conditions, along with the confidentiality agreement, as evidence of the signatory's acknowledgment and acceptance of their information security obligations.
 - By signing these documents, all parties affirm their commitment to adhere to the security policies of MEIL and to protect the organization's information assets.

6.2 During employment

- **Management Responsibilities**
 - All MEIL and third-party employees shall receive thorough briefings on their roles and responsibilities regarding information security and the appropriate usage of MEIL's information assets and processing facilities.
 - MEIL employees, contractors, and other third-party personnel shall adhere to Information Security Policies
- **Information security awareness education and training**
 - Information Security Training and awareness Programs shall be provided to all the employees and third-party employees of MEIL to create awareness about the Information Security policies and processes.
 - Information Security Training shall include appropriate training to staff, including security breach response responsibilities.
 - Information security training shall be overseen by the respective department representative or head.
 - New employees will receive an initial information security sensitization as part of their induction program.
 - Subsequent comprehensive user training completion is the responsibility of the department representative or head following the employee's onboarding.
 - Information security cell shall spread awareness of information security through various mediums like posters, flash films, events, surveys, mailers etc.
- **Disciplinary process**
 - MEIL shall establish a formal disciplinary process for addressing violations of Information Security policies and procedures.
 - All employees and relevant personnel shall be subject to this process in the event of non-compliance or misconduct.

- Disciplinary actions shall be determined based on the severity of the violation and may include verbal warning, written warning, suspension of access, termination of employment, or legal action.
- All disciplinary actions related to information security shall be documented and retained by the HR department.

6.3 Termination and Change of Employment

- **Responsibilities after Termination or Change of Employment**

- A formal termination process shall be defined and implemented when a user is off boarded.
- Employment contracts and vendor agreements within MEIL shall include duties and responsibilities that shall be valid post termination of the contract or agreement.
- Upon termination, users of MEIL shall return or hand over all organizational information assets under their control. Such assets shall be handed over to MEIL in strict accordance with the defined and approved termination procedures.
- In the event of a change in employment status, the access rights and privileges granted to employees, contractors, and other third parties shall undergo formal review and subsequent adjustment as required.

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.