Information Security

MEIL Risk Management Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Risk Management Policy
DOCUMENT NO.	MEIL- POL/RM/13/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 establish a systematic approach to risk assessment and treatment, ensuring the achievement of its intended outcomes, the prevention or reduction of undesired effects, and the facilitation of continual improvement.

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
Residual Risk	Risks that remain after risk treatment measures have been applied and which may require approval and cannot be feasibly reduced further.
Risk Assessment	The process of identifying, evaluating, and prioritizing information security risks to manage them effectively within the organization.
Risk Owners	Individuals identified as responsible for managing specific risks and participating in the risk treatment process.
Risk Treatment	A strategy formulated to mitigate identified significant risks to an acceptable level, including measures for risk acceptance, mitigation, transfer, or avoidance

5. Risk Management Policy

5.1 Risk Assessment

- The MEIL IT is responsible for annual Risk Assessments within their respective areas to ensure that information security risks are managed effectively
- Organization-wide risk assessments will be conducted by MEIL IT to evaluate emerging threats and maintain security at acceptable levels
- Additional risk assessments shall be initiated in response to major changes, defined as the introduction of new technologies, significant enhancements, upgrades, or conversions that impact information security.

5.2 Risk Treatment

- When significant risks are identified, a Risk Treatment Plan will be formulated to mitigate these risks to an acceptable level
- MEIL IT identified Risk Owners, and InfoSec GRC will review and approve the Risk Assessment and Risk Treatment Plan, including the acceptance of residual risks
- For risks that cannot be feasibly reduced, the MEIL Business Head must review and approve the handling of residual risks

5.3 Reporting

- All risk assessments will be carried out in accordance with the Risk Management Policy document, and findings will be reported to the Business Head & Group CISO.
- Documentation detailing the risk assessment exercise, decisions on risk acceptance, mitigation actions, and action plans will be retained for at least three years for future reference and verification.
- Findings and decisions from the risk assessments shall be reported to the Business Head at regular intervals.
- The Business Head shall establish security objectives that align with the organization's strategic goals, risk tolerance, and the outcomes of the risk management process

6. 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.

7. 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.