Information Security

MEIL System, Acquisition, Development and Maintenance Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Information System, Acquisition, Development and Maintenance Policy
DOCUMENT NO.	MEIL- POL/ISADM//07/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 objectives for the secure acquisition, development, and maintenance of information systems, with the aim of protecting organizational data, maintaining system integrity, and ensuring operational continuity and resilience across the system lifecycle.

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
Architecture and Engineering Principles	Guidelines and practices that inform the design and construction of systems to ensure they are secure, scalable, and resilient.
Change Management	The systematic approach to managing changes in a way that minimizes disruptions and ensures that modifications are implemented securely and efficiently.
Code Review	The systematic examination of application source code to identify and rectify security vulnerabilities, coding errors, and other issues.
Data Validation	The process of ensuring that data input into an application meets predefined criteria and is correct and secure.
Defence-in-Depth	A layered approach to security that establishes multiple barriers across different components of the information system.
Encryption	Encryption is the process of converting information or data into a code to prevent unauthorized access.
Secure Development Life Cycle (SDLC)	A process framework that incorporates security considerations and practices into every phase of software development.
Test Data	Data used during testing phases to simulate the operation of a program or system, which may be derived from or independent of live data.

5. Roles and Responsibility

Roles	Responsibilities
Developers	• Adhere to secure coding practices to prevent vulnerabilities such as SQL injection, cross-site scripting, and buffer overflows • Follow the secure coding guidelines provided by the organization and participate in training on secure coding best practices • Use only organization-approved software development frameworks and libraries and ensure they are regularly updated with the latest security patches • Conduct code reviews to identify and remediate security flaws before deployment • Collaborate with third-party vendors in compliance with the organization's security policies and standards, ensuring the security of the code developed
Users	• Comply with application security requirements, including adhering to access control protocols, data validation processes, and encryption standards. • Participate in security awareness training to understand the importance of information security within the project lifecycle. • Report any security incidents or vulnerabilities they identify in the course of using information systems. • Safeguard sensitive information during testing and ensure proper handling and destruction of test data as per policy guidelines

6. System Acquisition, Development and Maintenance Policy

6.1 Information security in project management

- Information security shall be integrated into project management to ensure that risks related to projects and deliverables are effectively addressed throughout the project lifecycle
- Project managers shall ensure that information security risks are assessed and treated at an early stage and periodically as part of project risks
- Information security requirements, including access control, data validation, and encryption, shall be addressed in the early stages of projects
- Information security risks associated with the execution of projects, such as the security of internal and external communication, shall be considered and treated throughout the project lifecycle
- Progress on information security risk treatment shall be reviewed, and the effectiveness of the treatment shall be evaluated and tested
- Responsibilities and authorities for information security relevant to the project shall be defined and allocated to specified roles
- Project management practices must align with the organization's overarching information security strategy to ensure consistent application of security measures across all projects
  Refer Encryption Policy

6.2 Secure development life cycle

- A Secure Development Life Cycle (SDLC) policy shall be established to guide the development of all software within the organization
- The SDLC shall include stages for requirements gathering, design, development, testing, deployment, maintenance, and disposal
- Security shall be embedded at each stage of the SDLC, with checkpoints to ensure compliance with security requirements

Commented [SM1]: TBU by Document Owner

- Secure development environments shall be specified for system development efforts based on risks associated with people, processes, and technology
- E-Business infrastructure, including web applications and database servers, shall be designed to give adequate protection against malicious code, hacking, defacing, and unauthorized access and shall ensure redundancy

6.3 Application security requirements

- Application security requirements shall be identified based on the data classification, business needs, and regulatory obligations
- Application security requirements shall include, but not be limited to, access control, data validation, authentication, and encryption
- Requirements shall be documented and communicated to all stakeholders, including developers and third-party vendors
- All e-business servers, including web applications and database servers, shall have the latest recommended updates and patches for the OS and applications

6.4 Secure system architecture and engineering principles

- Systems shall be designed using secure architecture and engineering principles that promote confidentiality, integrity, and availability
- Architectural designs shall consider segregation of duties, least privilege, and defense-in-depth strategies
- Security reviews of architecture shall be conducted periodically to ensure they remain robust against emerging threats
- All architectural decisions, especially those pertaining to security, must be well-documented, providing a clear rationale for future reference and audits
- The hardware and software configurations of E-business servers shall be documented

6.5 Secure coding

- Developers shall adhere to secure coding practices to prevent common vulnerabilities such as SQL injection, cross-site scripting, and buffer overflows
- A secure coding guideline shall be provided, and developers shall be trained on secure coding best practices
- Code reviews shall be conducted to identify and remediate security flaws before deployment
- Developers shall use only organization-approved software development frameworks and libraries that enforce secure coding practices, and these tools shall be regularly updated to incorporate the latest security patches and updates

6.6 Security testing in development and acceptance

- Security testing shall be integrated into the development process, with tests for vulnerabilities conducted at multiple stages
- Acceptance testing shall include security criteria, and no system shall be moved to production without passing these tests
- Automated and manual testing tools shall be used to ensure comprehensive coverage of security testing
- Implement incident response protocols specific to E-business infrastructure to swiftly address security breaches, data leaks, or service interruptions, ensuring minimal impact on business operations
  Refer Incident Management Policy

- Access to the e-business servers shall be logged. The logs generated shall be checked, reviewed, and archived in accordance with the operations security policy
  Refer Operation Security Policy

6.7 Outsourced Development

- When development is outsourced, contracts shall include clauses for information security, intellectual property rights, and the right to audit
- Third-party developers shall be required to adhere to the organization's security policies and standards
- The security of the code shall be assured, and the code shall be free from malicious content
- E-Business infrastructure shall be hosted at third-party facilities only after risk assessment and ensuring compliance with MEIL information security policies

6.8 Separation of development, test and production environments

- Development, test, and production environments shall be separated both physically and logically to prevent unauthorized access and data leakage
- Access controls shall be implemented to ensure that only authorized personnel have access to these environments as per their role requirements
- A formal change management process shall be implemented to manage and track changes across development, test, and production environments, ensuring traceability and accountability for all modifications
- Specific security controls for each environment, including firewall configurations, access control lists, and monitoring solutions, shall be documented and enforced to maintain the integrity and security of the environments
- The policy will include provisions for managing emergency changes, ensuring that such changes are subject to the same rigorous security controls as standard changes

6.9 Test Information

- Test data shall be carefully selected and sanitized to avoid the use of sensitive information
- If sensitive data must be used, it shall be appropriately masked or anonymized
- The extraction and use of test data shall be documented and monitored to prevent data leakage
- Upon completion of testing, all test data will be securely destroyed or de-identified to prevent any potential data leakage or unauthorized use
- Business-related critical data on the servers shall be regularly backed up and shall be kept in secure off-site storage

6.10 E-Business

- All business partners using the e-business websites for business transactions shall be presented with terms & conditions drafted in consultation with the Legal Department, and they shall agree to these terms & conditions to transact
- Functional heads shall identify owners for their respective E-business websites, and these owners shall ensure the integrity of information on the same
- All information published on publicly available sites shall go through a formal authorization process, validated and authorized by respective owners
- Monitor the performance and availability of E-business services to meet defined service level agreements (SLAs) and user expectations, ensuring high-quality service delivery
- Business partners transacting online shall enter into an agreement with MEIL

- Controls for non-repudiation, duplicity, fraudulent transactions, and authentication of orders placed shall be provided through unique User IDs
- Maintenance of IT Assets will be done by MEIL IT Maintenance of Non-IT Assets will be the responsibility of Admin. Maintenance of Specialized Equipment will be the responsibility of the department owning the asset

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.