Information Security

MEIL Operation Security Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Operation Security Policy
DOCUMENT NO.	MEIL- POL/OS/06/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 Operational Security Policy at MEIL is to strengthen the organization's operational posture by instituting robust controls that ensure system reliability, data protection, and resilience against cyber threats. This policy underpins our commitment to maintaining operational excellence, minimizing risk, and upholding the highest standards of security and compliance.

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
Audit Testing	The process of evaluating the effectiveness of security measures through systematic review.
Capacity Management	The practice of ensuring that system resources meet current and future business demands efficiently.
Change Management	The structured approach to transitioning individuals, teams, and organizations to a desired future state.
Clock Synchronization	The coordination of system clocks within a network to the same time reference.
Information Backup	The process of copying and archiving data so it may be used to restore the original after a data loss event.
Logging	The recording of events, transactions, and other significant data within systems for monitoring and analysis
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems
Monitoring Activities	The ongoing oversight of operations and performance to detect and respond to incidents.
Technical Vulnerabilities	Weaknesses or flaws in systems that could be exploited to compromise security or functionality

5. Roles and Responsibility

Roles	Responsibilities
Information Technology (Helpdesk and IT Admin)	• Implement and maintain comprehensive malware defence strategies, including firewall architecture and anti-virus systems across the organization. • Conduct capacity planning and proactive monitoring of IT resources to prevent business disruptions due to insufficient IT capacity or resource shortages. • Maintain a robust information backup strategy, collaborating with information owners to identify data backup requirements and archival rules. • Control the installation of software on operational systems through an authorized process, ensuring all installations comply with licensing agreements and security standards. • Perform regular PC audits to ensure compliance with information security policies and maintain reports for action by local IT managers. • Conduct monthly reviews of logs for computer operator and system usage on critical servers and networking devices. • Coordinate with the central IT Security team for regular reviews of hosted website inventories within the network or cloud.
Network Team	• Ensure server time is synchronized with an NTP server, manually adjusting the clock if the difference exceeds the set threshold. • Implement and manage network security measures, including regular updates and patches to network infrastructure. • Monitor network traffic and behavior to detect any anomalous or unauthorized activity. • Coordinate with IT for the deployment of network-related changes and ensure minimal disruption to business operations.
Employees	• Ensure that backups of critical information and data stored on laptops or desktops are taken regularly. Adhere to the software installation policy and prevent unauthorized installations.

6. Operation Security Policy

6.1 Documented Operating Procedures

- Information security is integrated into operational management to ensure secure and reliable operations through consistently documented and adhered-to procedures.
- Operational procedures are subject to document control, including versioning, approval, distribution, and access, to maintain their integrity and availability.
- Roles and responsibilities for the creation, review, approval, and execution of these procedures are clearly defined and communicated to ensure accountability.
- Operational procedures shall be reviewed and updated regularly to adapt to technological advancements and evolving business processes.
- All operational activities shall be performed in strict accordance with the documented procedures to maintain the highest levels of security and reliability.

6.2 Capacity Management

- IT shall undertake comprehensive capacity planning to prevent any business disruptions due to insufficient IT capacity or resource shortages.
- The capacity planning process shall be proactive, considering both present and future IT resource requirements to align with MEIL's strategic business vision and anticipated growth.
- In the context of establishing new facilities, the IT Administrator is tasked with ensuring that capacity planning is rigorously approved according to the established approval process.
- Continuous monitoring of IT resources, such as servers, printers, and other critical infrastructure, shall be conducted to track maximum, minimum, and average usage levels. Any observed abnormalities, whether under-utilization or over-utilization, must be promptly reported to the IT administrator for necessary action.
- The scope of capacity planning shall be inclusive of human resources and manpower, in addition to physical devices and server room capacities, recognizing the integral role of personnel in maintaining operational efficiency.
- A formalized process for the assessment of capacity utilization shall be adopted, mandating monthly evaluations and a comprehensive review for planning purposes on an annual basis.

6.3 Protection against malware

- A comprehensive malware defense strategy shall be established to protect systems and data from malicious software threats.
- This strategy will include the deployment, enforcement, and management of firewall architecture and anti-virus systems across the organization.
- Regular risk assessments will be conducted to identify potential malware threats and evaluate the effectiveness of existing controls.
- Anti-malware solutions shall be kept up-to-date and continuously monitored to ensure they are effective against known and emerging threats.
- All servers, laptops, Macs, and desktops shall be updated with the latest versions of the anti-virus signature files.
- The malware protection mechanisms shall be reviewed and updated periodically to stay ahead of the evolving threat landscape.
- Systems will be securely configured to minimize the risk of malware infections, with configurations reviewed regularly to maintain security.
- Users shall be responsible for the content of information downloaded from the Internet and its use for business purposes. Software filters and other techniques shall be installed and used to restrict access to inappropriate websites/information on the Internet by users.
- Attempts to access restricted websites shall be reported to the appropriate authorities for further action.
- All files downloaded from email attachments, file-sharing, etc., shall be scanned for mobile codes.
- Users shall not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of or access to any IT assets.
- The organization's incident response plan will include specific procedures for responding to malware incidents, ensuring a coordinated and effective approach to containment, eradication, and recovery.
- All anti-virus servers shall be continuously available. The Anti-Virus Management Team & Local Help Desk shall ensure the continuous availability and updating of anti-virus solutions.
- Relationships with suppliers and third-party service providers will include requirements to adhere to the organization's standards for malware protection.
- All major virus incident responses shall be regularly reviewed and tested.
- Malware defense strategies will be integrated with business continuity planning to ensure that the organization can continue to operate effectively in the event of a malware attack.

- Any changes to the central anti-virus & firewall policy/configuration shall be approved by the IT department. Internet access shall be disabled from all key servers, with exceptions duly authorized by the IT department to ensure that malware does not affect critical data. The effectiveness of malware protection measures will be subject to regular audits, and the organization will comply with all relevant legal and regulatory requirements related to malware protection.

6.4 Management of Technical Vulnerabilities

- Vulnerability Assessment and Penetration Testing (VAPT) shall be routinely conducted on all existing and new external-facing web applications to ensure the security and safety of the sites accessed by end users.
- Updates and new versions of websites and applications shall undergo VAPT to maintain security standards.
- Remediation shall be prioritized based on the severity of the vulnerability and the potential impact on the organization, ensuring that the most significant risks are addressed promptly. Reporting mechanisms shall be established to keep relevant stakeholders informed about vulnerability findings.
- VAPT shall be a recurring activity with a defined schedule based on the criticality of the business operations at each location.
- Locations are required to submit an inventory of hosted websites within the MEIL network or cloud to the central IT Security team for regular reviews.
- Identified vulnerabilities must be remediated prior to the deployment of websites or applications.
- Contracts with external development agencies shall include clauses mandating adherence to secure coding practices, and their work must pass VAPT before acceptance.
- Project plans shall incorporate VAPT activities, including timelines and budgeting for associated costs.
- The installation of patches from legitimate sources shall involve a risk assessment to weigh the risks of the vulnerability against those posed by the patch installation.

6.5 Information Backup

- A robust information backup strategy shall be defined and implemented to prevent data loss and ensure the recoverability of critical information.
- The MEIL- IT hall collaborate with information owners to identify the data to be backed up, determine the minimum backup frequency, and establish archival rules.
- Backup copies of critical business information and software shall be stored in environmentally protected and access-controlled sites. Backup data, particularly when transported offsite or stored in the cloud, shall be encrypted and protected to prevent unauthorized access and ensure the confidentiality and integrity of the data.
- Backup procedures shall ensure that critical information and data stored on laptops or desktops are backed up regularly. It is the responsibility of the users to ensure that backups are taken on a regular basis.
- M&M Central Team shall ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration process. Additionally, the restoration testing of critical data from backup media shall be carried out periodically to verify the effectiveness of the backup process.
- The creation of copies of confidential paper documents shall be restricted, with detailed controls implemented.

  Refer Asset Management Policy
- Plans shall be developed and implemented to maintain or restore operations and ensure the availability of information at the required level and within the required time scales following an interruption to, or failure of, critical business processes.

- Clear roles and responsibilities for managing and executing the backup procedures shall be established to ensure organizational accountability. This includes the involvement of the central IT Security team in the regular review of hosted website inventories within the MEIL network or cloud.

6.6 Logging

- Logs for computer operator and system usage on critical servers and networking devices shall be meticulously maintained, capturing both administrator and operator activities. This includes the secure offline storage of information for investigation when computer crime or abuse is suspected.
- The IT Operations Manager or a designated technical specialist shall conduct monthly reviews of all logs and take necessary actions based on their findings. These logs shall be securely retained for at least 30 days to provide evidence for investigation, prosecution, and disciplinary action.
- Access to logged information shall be granted only after authorization by the MEIL IT department, ensuring protection from unauthorized access and tampering.

Commented [SM1]: TBU by Document Owner

6.7 Monitoring activities

- Monitoring systems shall be in place to detect any anomalous behavior, with immediate planning of appropriate actions to evaluate potential information security incidents.
- Users shall be informed about which actions are considered security violations, and that such violations will be logged and subject to review. Clear communication to users regarding security violations shall be maintained.
- Regular PC audits shall be performed by the Helpdesk to ensure compliance with information security policies.
- Reports generated from these audits shall be maintained for action by local IT managers and department heads. This activity shall be conducted for all desktops & laptops
- A proactive approach shall be taken to protect information assets by maintaining awareness of the evolving threat landscape through the collection, analysis, and dissemination of threat intelligence.
- Monitoring activities shall be regularly reviewed and audited to ensure their effectiveness, and findings shall be integrated into the organization's incident response plan to enhance incident management capabilities Incident mgmt.
- This includes gathering information on security threats from various sources, analyzing it to assess and prioritize threats, and ensuring continuous monitoring and updates to the threat intelligence program.

6.8 Clock Synchronization

- All system clocks within the organization shall be synchronized with a standardized time source to ensure uniform timekeeping.
- System and network administrators shall ensure server time is synchronized with an NTP server, manually adjusting the clock if the difference exceeds 90 seconds.
- Procedures to maintain clock synchronization shall be implemented and periodically reviewed to ensure their continued accuracy. Administrators shall repeat the time synchronization exercise every week to keep the server always running with the nearest NTP time.

6.9 Installation of software on operational systems

- The installation of software on operational systems shall be controlled through an authorized process that is well-documented and adhered to. This process shall be integrated with the organization's change management system to ensure that all risks associated with software changes are assessed and managed effectively.
- A comprehensive record of all software installations shall be maintained, ensuring that all installations comply with licensing agreements and security standards.
- A patch management process shall be established to ensure that all installed software is regularly updated with the latest security patches and updates to maintain system security and integrity.
- Software installations shall be evaluated and authorized based on their necessity for business operations, compatibility with existing systems, and adherence to security requirements.
- All software installations must undergo thorough testing to confirm compatibility and security and must be approved by authorized personnel before being deployed on operational systems.
- Users shall receive training and awareness on the software installation policy to prevent unauthorized installations and to understand the importance of adhering to authorized processes.

6.10 Change management

- All changes affecting information security across the organization, its processes, and IT systems shall be strictly controlled. Changes to the organization, business processes, information processing facilities, and systems that affect information security shall be controlled.
- Deployments of application systems and servers shall undergo thorough evaluation to ensure security and compatibility. The products shall be checked for necessary security features, and appropriate test reports shall be attached as required.
- Security features shall be a prerequisite for all products, with a formal change control procedure in place for any deployment. For major modifications to systems, networks, applications, and information processing facilities, a formal change control procedure shall be followed, thoroughly evaluating potential impact.
- Significant system, network, or application changes shall be subject to a rigorous evaluation process to assess impact, with oversight and approval by the MEIL Team. MEIL Team shall review and approve the setup of any new information processing facilities.
- Changes shall be accompanied by appropriate testing and risk analysis, with Service Level Agreements (SLAs) defined for each category of change. Risk analysis shall define the threats and their probability, with every impact analysis followed by auto-calculation of the underlying risk by the system-calculated score.
- Major system changes shall be tested in a controlled environment prior to live deployment, with documentation updated to reflect these changes and minimize operational disruption. All major changes in the existing application system shall be tested in a test environment (as far as possible) before deployment in the production environment. Risk due to not having a test environment should explicitly be accepted by the process owner.
- In the event of failure or unexpected issues during or after deployment, a rollback plan must be in place for all major changes.
  This plan should include:
  - Steps to revert the system to its previous stable state
  - Identification of responsible personnel for executing the rollback

Commented [PH2]: Roll back patches

6.11 Protection of information systems during audit testing

- Audit activities shall be carefully planned and managed to ensure they do not compromise the security or operations of information systems. The scope and objectives of audit activities shall be clearly defined to ensure that testing is focused, relevant, and aligned with the organization's information security goals.
- Audit testing shall be conducted in a manner that minimizes risks to the organization while protecting sensitive data and critical systems.
- When necessary, compensating controls shall be implemented to maintain the security and integrity of information systems during audit activities. Access control shall be strictly enforced during audit activities, ensuring that only authorized personnel are involved in the testing process and that sensitive data is protected.
- Audit activities shall be coordinated with relevant stakeholders, including system owners and IT personnel, to schedule testing at times that minimize disruption to business operations.

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.