Information Security

MEIL Acceptable Usage Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Acceptable Usage Policy
DOCUMENT NO.	MEIL- POL/AU/01/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 Acceptable Usage Policy is to establish clear guidelines for the use of MEIL's information and IT assets to ensure they are utilized in a secure, ethical, and lawful manner. It aims to protect the organization's technological infrastructure from misuse while supporting the achievement of business objectives. This policy delineates the responsibilities of users and the consequences of non-compliance, thereby safeguarding the integrity and value of MEIL's information systems.

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
Acceptable Usage Policy (AUP)	A set of rules and guidelines that outline the proper use of an organization's information technology (IT) resources and assets to ensure they are not misused.
Business Purpose	Activities that support or contribute to the operation and objectives of the organization, including but not limited to administrative, operational, or direct customer-related functions.
BYOD (Bring Your Own Device)	A policy that allows employees to use their personal devices, such as smartphones, tablets, and laptops, for work-related activities.
Information Systems	The combination of hardware, software, infrastructure, and trained personnel organized to facilitate planning, control, coordination, and decision-making in an organization.
Intellectual Property	Legal rights that result from intellectual activity in the industrial, scientific, literary, or artistic fields. This includes copyrights, patents, trademarks, and trade secrets.
Remote Access	The ability to access a computer or a network from a remote location. This can include accessing company data, applications, or services from outside the organization's primary location.

5. Roles and Responsibility

Roles	Responsibilities
Information Technology	• Monitor and audit network and system usage to ensure compliance with the policy. • Provide support for incident reporting and response and manage remote access security. • Oversee the installation of software, manage IT assets, and ensure secure disposal of information and assets as per policy.
Human Resource	• Develop and enforce disciplinary processes for policy violations. • Coordinate with IT to facilitate training and awareness programs for all users.
Users	• Adhere to the Acceptable Usage Policy by using MEIL's information and IT assets for business purposes. • Maintain confidentiality of passwords, access cards, and tokens, and report any security incidents or risks to the IT helpdesk team. • Participate in training programs to understand the policy and comply with all relevant legal and regulatory requirements.

6. Acceptable Usage Policy

6.1 Acceptable Use

- All users are expected to use MEIL's information and IT assets primarily for business purposes.
- Each user is personally responsible for the control of his/her company provided equipment, including the installed software.
- All communications conducted using MEIL facilities will be the property of MEIL, and it reserves the right to record and access all communications, monitor, and audit networks and systems when deemed necessary.
- For security and network maintenance purposes, authorized individuals within MEIL will monitor equipment, systems, and network traffic at any time.
- The primary purpose for the MEIL's Information systems is for MEIL's business use. Users will make limited, infrequent, or incidental use of MEIL systems for personal use.
- Users found in breach of this policy may face disciplinary action as outlined in the processes developed by the Human Resources Team.
- The circulation, storage, or creation of obscene, vulgar, or inappropriate material is strictly prohibited.
- Users are required to report and remove such content if encountered.
- Passwords, access cards, and tokens must not be shared, and any form of access rights circumvention is forbidden.
- Only authorized software may be installed on MEIL's IT systems. The use of unauthorized, freeware, shareware, and games are not permitted unless approved by the Compliance Manager after a VAPT. Server-grade software must only be installed on designated servers.
- Users must adhere to confidentiality and data protection agreements, ensuring that no confidential or internal-use information is disclosed to unauthorized individuals.
- Employees shall adhere to all intellectual property and copyright law. Users shall always obtain copyright holder's permission before downloading information from internet or other public computer system.
- Users will inform the IT helpdesk team of any communication, system problem or other circumstance

that may indicate a breach of security or other risk to the integrity of MEIL's information system.

- No customer related information of any kind and no confidential information regarding any third party will be sent over any public computer system unless the customer or third party have specifically agreed to it.
- Personal storage of files on MEIL's computer systems is discouraged, and mobile computing devices are to be used for business purposes in accordance with the detailed Information Security Policy.
- Users are responsible for maintaining a clear desk and screen by logging off from systems when not in use.
- Users must be aware of and comply with relevant legal, statutory, regulatory, and contractual requirements concerning the use of information assets.
- Regular training and awareness programs will be conducted to ensure users understand their responsibilities and the consequences of non-compliance.
- The use of cloud services, social media, and the handling of customer data must be conducted in a secure and responsible manner, with users adhering to specific guidelines and best practices to protect sensitive and personal information.
- Sensitive data must be encrypted during storage and transmission to prevent unauthorized disclosure and ensure data integrity.
- Personal devices used for business purposes must adhere to the organization's Mobile Device policy, ensuring the security of company data.
- Users are required to follow the information classification and handling procedures to correctly manage the security of information based on its classification level.
- Users must report any changes or movements of IT assets to maintain accurate asset management and facilitate asset tracking.
- Compliance with software licensing agreements is mandatory, and users must ensure that all software used is properly licensed and authorized.
- Information and IT assets that are no longer required must be disposed of securely in accordance with data protection laws and company policies.
- The policy will be enforced through regular audits and reviews, and any deviations or security incidents must be reported and addressed in accordance with the incident management process.
- Compliance with this policy is mandatory, and non-compliance may result in disciplinary action. This policy will be reviewed regularly to ensure ongoing relevance and effectiveness.

6.2 Mobile Device Policy

- Mobile devices must operate on Android 10 or later, iOS 15 or later, and Windows 7 or later.
- User-saved passwords on devices must be stored in an encrypted format.
- All devices should be secured with passwords that adhere to the organization's guidelines.
- Devices not managed by MEIL IT are prohibited from direct connections to the internal corporate network.
- Users are required to report lost or stolen devices to MEIL IT without delay.
- Any suspicion of unauthorized access to company data through a mobile device must be reported to IT Team. Devices must not be jailbroken or modified to expose unauthorized functionality.
- The installation of pirated software or illegal content onto devices is strictly forbidden.
- Only install applications from official, platform-owner approved sources. Users must contact MEIL IT if they are uncertain about the legitimacy of an application source.
- Devices should be regularly updated with the latest patches provided by the manufacturer or network, at a minimum on a weekly check and monthly application basis.
- Devices must not be connected to PCs lacking up-to-date and active anti-malware protection or not in compliance with corporate policy.
- Users should exercise caution when managing personal and work email accounts on their devices, ensuring that company data is sent exclusively through the corporate email system.
- Immediate notification to MEIL IT is required if there is a suspicion that company data has been sent from a personal email account.

6.3 Internet Usage Policy

- Internet access is primarily provided for legitimate business use, such as research, communications, and access to authorized business tools and applications.
- Personal use of the internet should be limited, infrequent, and appropriate. It must not interfere with business operations, consume excessive bandwidth.
- All internet activity is monitored and logged by authorized MEIL personnel. MEIL reserves the right to audit browsing history, downloads, and data usage to ensure compliance.
- Accessing websites that are illegal, inappropriate, or offensive — such as those related to pornography, gambling, violence, or hate speech — is strictly prohibited.
- Users must not attempt to bypass or disable internet filters, firewalls, or proxy servers unless explicitly authorized by MEIL IT.
- Downloading or uploading of large files for non-business purposes (e.g., movies, music, or personal media) is discouraged and may be restricted.
- Any suspicious internet activity, including phishing, malware downloads, or unauthorized access attempts, must be reported to the IT helpdesk immediately.
- Use of personal email accounts, file-sharing services, or cloud platforms for work-related tasks must be explicitly approved and configured in line with data security requirements.
- Guest users, vendors, or third-party visitors may only access the internet through designated guest networks. Access to MEIL's internal systems is strictly prohibited unless authorized.
- All remote access to MEIL’s internal systems must occur through company-approved and secured VPN connections.
- To ensure secure remote access to organizational resources, employees must use Zscaler Private Access (ZPA) or other approved secure access solutions.
- Access to internal applications is granted based on user identity, device posture, and contextual policies, minimizing exposure to potential threats.
- Multi-factor authentication (MFA) is mandatory, and access is segmented according to job roles and business requirements.

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.