Information Security

MEIL Encryption Policy

DOCUMENT CONTROL

DOCUMENT NAME	MEIL Encryption Policy
DOCUMENT NO.	MEIL/POL/EP/03

AUTHORISATION

	Prepared By	**Reviewed By**	**Approved By**
Name	Priyanka Haldankar	Anil Khedulkar	Giriraj Mohta
Designation	Consultant	Manager - IT	MEIL- CFO
Date	08-July-2025	24-Feb-2026	24-Feb-2026

SECURITY CLASSIFICATION: Internal

VERSION HISTORY

VERSION	DATE	PREPARED BY	CHANGES & REASONS FOR CHANGE
1.0	08-July-2025	Priyanka Haldankar	Initial Release

Table of Contents

1. Purpose

The purpose of the Encryption Policy at MEIL is to define the required protection level to maintain the confidentiality, integrity and authenticity of the information assets and sensitive application systems of MEIL. The policy applies to all systems, networks, applications, and users handling sensitive information to mitigate risks and ensure secure data protection.

2. Scope

Commented [PM1]: To be updated by document owner

This policy applies to all users, systems, applications, and devices that store, process, or transmit sensitive, confidential, or proprietary information owned or managed by MEIL. It encompasses data at rest, data in transit, and data in use across all IT and non-IT environments, including on-premises infrastructure, cloud services, mobile devices, and third-party platforms. The policy also applies to personal devices used for business purposes and to any external entities handling MEIL's data under contractual agreements.

3. Applicability

Commented [PM2]: To be updated by document owner

This policy is applicable to all the locations of MEIL.

4. Terms and Definitions

Terms	Definitions
Backup	Files, devices, data and procedures available for use in case of failure or loss, or in case of deletion or suspension of their original copies.
Cryptography	Cryptography is a method of protecting information by transforming it into an unreadable format, only to be made readable again with the correct decryption key.
Encryption	Encryption is the process of converting information or data into a code to prevent unauthorized access.
Key Management	Key management refers to the administration and control of the complete lifecycle of cryptographic keys. It includes the processes and methodologies necessary for the generation, distribution, storage, rotation, backup, recovery, revocation.

5. Roles and Responsibility

Roles	Responsibilities
Department Head	• Ensure departmental compliance with the Encryption Policy and related procedures. • Allocate necessary resources for implementing encryption measures. • Approve departmental encryption requirements in consultation with the Infosec team. • Review reports on encryption effectiveness and address gaps within their departments.

Supporting IT Operations Teams	• Deploy and maintain encryption solutions for systems, applications, networks, and storage • Manage cryptographic key infrastructure in collaboration with the Infosec team • Troubleshoot and resolve encryption-related technical issues • Regularly update encryption configurations to ensure alignment with policy standards
End Users	• Use encryption tools and techniques as mandated by the policy (e.g., using secure channels like VPNs) • Safeguard private keys, passwords, and other cryptographic credentials assigned to them • Refrain from sharing cryptographic keys or credentials via unsecured methods • Report any encryption-related incidents, such as key compromises, to the department representative or Infosec team

6. Encryption Policy

6.1 Encryption Standards and Cryptographic Solutions

- The Information System/Data Owner, in consultation with security team, shall determine encryption requirements based on:
  - Information classification
  - Risk assessment results
  - Business and regulatory obligations
- Encryption must use approved algorithms like AES-256, RSA-2048 and comply with organizational and legal standards.
- Cryptographic keys (e.g., secret keys, public/private keys) must be securely generated, stored, and managed to prevent unauthorized access or misuse.
- Third-party vendors handling sensitive information must adhere to the organization’s encryption and key management requirements, as outlined in service-level agreements (SLAs).

6.2 Encryption requirement during Data in Transit

- When MEIL electronic information is classified as 'highly confidential' or 'confidential' as per MEIL's information classification.
- When law or regulation requires encryption of data in transit.
- When remotely accessing the MEIL's network or devices over a shared (e.g., Internet) or personal network.
- Transmission through corporate wireless network.

6.3 Encryption requirement during Data at Rest

- Sensitive information, including personal, financial, or health data, must be encrypted throughout its lifecycle, including storage and backup.
- Stored data classified as Highly Confidential or Confidential must be encrypted using approved techniques per the organizational backup policy.
- Encryption must be implemented on all storage devices containing sensitive data, including mobile devices and removable media.

6.4 Cryptographic Key Management

- Cryptographic keys must be securely managed throughout their lifecycle to prevent unauthorized access or misuse.
- Key management processes must include:
  - Secure generation, activation, storage, distribution, revocation, and destruction of keys.
  - Backup and recovery mechanisms for lost or corrupted keys.
  - Secure storage using approved methods (e.g., Hardware Security Modules).
- Keys must have defined activation and expiration periods, with periodic reviews for compliance.
- Secret keys (symmetric encryption) and private keys (asymmetric encryption) must be strictly protected against unauthorized disclosure.
- Logs of key management activities must be maintained and audited regularly.

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