Langslide

Encryption and Key Management Policy

Version 1.0

PURPOSE

This policy defines Rudramsa Systems Pvt. Ltd. (hereby referred to as organization) security control requirements for encryption and the key management lifecycle to protect data at rest and in transit against unauthorized access or disclosure.

SCOPE

This policy covers all data stored (at rest) and/or transmitted across networks, including data on writable media, databases, and cloud storage. It applies to employees, contractors, and third parties of the organization. It includes sensitive information (personal data, proprietary information) that requires protection from unauthorized disclosure.

DEFINITION

- **Sensitive Information:** Data whose unauthorized disclosure may result in privacy, security, or compliance risks to an individual or the organization.
- **Encryption:** Transforming data into a scrambled format to prevent unauthorized access.
- **Key Management:** The lifecycle handling of cryptographic keys, including their generation, distribution, rotation, storage, and retirement.
- **Public Network:** Any network (e.g., the Internet) not controlled exclusively by the organization
- **Private Cryptographic Keys:** Keys must be kept secret (e.g., private keys in asymmetric encryption), and they are typically stored in secure hardware tokens or vaults.

RESPONSIBILITIES

- **IT Head & DevOps Head**
  - Overall responsibility for implementing, monitoring, and maintaining this policy.
  - Approve cryptographic technologies, methods, and key lengths before deployment.
  - Ensure interoperability of cryptographic solutions across the organization.
- **All Employees, Contractors, and Third Parties**
  - Must follow the encryption guidelines and procedures outlined in this policy.
  - Report any suspected compromise of cryptographic keys or unauthorized decryption attempts.
- **Information Technology / Security Teams**
  - Document cryptographic methods in use to ensure they are secured from unauthorized access.
  - Review encryption algorithms, key lengths, and message digest lengths annually.
  - Provide a recovery mechanism for encrypted data in the event of lost keys or for forensic investigations.

POLICY

Identification of Storage Media

- All data and information storage media (e.g., disks, USBs, cloud volumes) must be categorized and assessed for encryption needs.

Best Practices and Documentation

- Document and secure cryptographic methods from unauthorized access.
- Implement industry best practices (e.g., AES-compatible standards) where feasible.

Approval of Cryptographic Technologies

- All new cryptographic protocols, algorithms, or parameters require IT approval.
- Ensure chosen technologies are interoperable with existing systems and meet legal requirements in relevant jurisdictions.

Legal and Regulatory Compliance

- Cryptographic solutions must align with regional and international laws, regulations, and organizational security standards.

Algorithm Requirements

- AES-compatible or partially AES-compatible algorithms are preferred for symmetric encryption.
- Key and hash value (message digest) lengths must be reviewed annually and updated as necessary.

Data/Key Recovery

- Recovery logic (e.g., key escrow, data recovery methods) must be implemented to ensure authorized personnel recovers encrypted data.
- A forensic investigation recovery mechanism must be in place to comply with law enforcement requests if needed.

ENCRYPTION

Disk Encryption

- Hard disk encryption solutions should use hardware tokens for key management to prevent unauthorized decryption.

Data Exchange

- When transmitting sensitive information (e.g., personal data, cryptographic keys), apply heightened security measures (e.g., multi-factor authentication, encrypted channels).

Key Restoration

- A process shall exist to decrypt data or restore encryption keys if the original key is lost or inaccessible.

Network Communication

- Where feasible, TLS (Transport Layer Security) is required for network-based data transmission.

Approved Encryption Methods

- Only organization-approved encryption methods and solutions may be used.
- Symmetric cryptosystems: Use keys of at least 128 bits.
- Asymmetric cryptosystems: Use key lengths of at least 1024 bits, although higher lengths (2048 bits or more) are strongly recommended.

DATA IN TRANSIT

Data in transit includes, but is not limited to:

- Internet-based data transfers.
- Email transmissions.
- Remote access (VPN) connections.
- File transfers to external third parties.
- Administrative access sessions (e.g., SSH, TLS/HTTPS).
- Encryption Methods (examples):
- TLS for browser-based encryption.
- VPN (using RSA encryption methods) for secure remote connections.
- SFTP (with SSH) for secure file transfers.
- SSH or TLS is used by system administration to encrypt credentials and traffic.

DATA IN STORAGE

Includes, but is not limited to:

- Backup and removable media (tapes, USB drives).
- Disk drives on laptops, mobile phones, and tablets.
- Application and database fields/tables containing sensitive data.

KEY MANAGEMENT

Key Protection

- Keys must be safeguarded against unauthorized use, modification, or loss.
- Symmetric and asymmetric key lengths should align with industry best practices or as technically feasible for each system/app.

Confidential Classification

- Keys are classified as confidential and must be centrally managed wherever possible.
- Private cryptographic keys for applications or sensitive information exchange must reside on secure hardware tokens.

Secure Disposal

- Private and shared keys must be securely deleted before disposing of cryptographic hardware or software to prevent retrieval by unauthorized parties.

Recovery and Escrow

- Critical encryption keys should be held in formal escrow or recovery procedures to facilitate data retrieval if they are lost or compromised.

CERTIFICATE MANAGEMENT

Procurement

- Certificates for non-authorized users and devices must be purchased from and managed by a publicly trusted Certificate Authority (CA).

Server Authentication

- All servers performing authentication must present a valid certificate signed by a known, trusted provider.
- SSH/TLS usage on servers must also employ trusted, valid certificates.

Renewal and Revocation

- Certificates must be renewed or replaced before their expiration date.
- Certificates must be revoked if:
    - The private key is compromised.
    - The service is retired or decommissioned.
    - The private key is no longer in use.

ENFORCEMENT AND COMPLIANCE

Monitoring

- To ensure compliance, The IT and DevOps Head (or designated Security Team) may monitor encryption usage and key management processes.

Non-Compliance

- Violations of this policy may result in disciplinary action, including termination of employment or contract, and/or legal consequences depending on severity.

Review and Updates

- This policy and the associated cryptographic solutions must be reviewed annually or upon significant legal/technical standards changes.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya