US Solutions Pvt Ltd. - Encryption Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-02-02
- **Author:** IT & Infosec Department - Sophia Khan
- **Approved By:** Gregory Walsh, Security Infrastructure Manager
- **Effective Date:** 2024-03-01
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that encryption is a fundamental security control for protecting the confidentiality and integrity of sensitive information. This Encryption Policy establishes the guidelines and requirements for encrypting data at rest and in transit across all Company systems and applications. All employees, contractors, and authorized users ("Users") are required to adhere to this policy to ensure the security of our information assets.

2. Purpose

The purpose of this policy is to:

- Establish a consistent approach to data encryption.
- Protect sensitive information from unauthorized access and disclosure.
- Ensure compliance with applicable laws and regulations.
- Define the responsibilities of data owners and custodians regarding encryption.
- Minimize the risk of data breaches and security incidents.

3. Scope

This policy applies to all data owned, processed, or transmitted by US Solutions Pvt Ltd., including:

- Electronic data stored on Company devices (laptops, desktops, servers).
- Data transmitted over Company networks and the internet.
- Data stored on removable media (USB drives, external hard drives).
- Data stored in cloud-based services.
- Data stored in databases and applications.
- Any sensitive information that requires protection.

4. Encryption Requirements

- **Data at Rest:**
    - Sensitive data stored on Company devices must be encrypted using approved encryption algorithms (e.g., AES-256).
    - Full disk encryption must be enabled on laptops and mobile devices.
    - Databases and applications containing sensitive data must be encrypted.
    - Removable media containing sensitive data must be encrypted.

- **Data in Transit:**
    - Sensitive data transmitted over Company networks and the internet must be encrypted using secure protocols (e.g., TLS/SSL, HTTPS, IPsec).
    - Email communication containing sensitive information must be encrypted (e.g., S/MIME, PGP).
    - VPNs must be used for secure remote access.
    - File transfers must be done using SFTP or FTPS.
- **Key Management:**
    - Encryption keys must be generated, stored, and managed securely.
    - Key management systems must be used to protect encryption keys.
    - Keys must be rotated regularly.
    - Keys must be backed up securely.
- **Approved Algorithms:**
    - Only industry standard and company approved encryption algorithms are to be used.

5. Data Classification and Encryption

- Data must be classified according to the Company's Data Classification Policy.
- Encryption requirements vary based on the data classification level:
    - **Public:** No encryption required.
    - **Internal:** Encryption recommended for sensitive internal data.
    - **Confidential:** Encryption required for data at rest and in transit.
    - **Restricted:** Strong encryption required for data at rest and in transit, with strict key management.

6. Responsibilities

- **Data Owners:**
    - Determine the encryption requirements for their data.
    - Ensure that data is encrypted in accordance with this policy.
    - Approve access to encrypted data.
- **Data Custodians:**
    - Implement and maintain encryption controls.
    - Ensure that encryption keys are managed securely.
    - Report any encryption-related security incidents.
- **IT Department:**
    - Provide encryption tools and support.
    - Manage encryption keys and key management systems.
    - Monitor and audit encryption controls.
    - Provide training to users on encryption best practices.
- **All Users:**
    - Comply with this Encryption Policy.
    - Protect encryption keys and passwords.
    - Report any suspected encryption-related security incidents.

7. Legal and Regulatory Compliance

- This policy complies with all applicable data privacy laws and regulations (e.g., GDPR, CCPA, HIPAA).
- Encryption controls must be consistent with legal and regulatory requirements.

8. Training and Awareness

- All Users will receive training on this Encryption Policy.
- Regular security awareness training will be provided to reinforce encryption best practices.

9. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

10. Monitoring and Enforcement

- The IT department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

11. Acknowledgement

- By accessing Company information assets, Users acknowledge that they have read, understood, and agree to comply with this Encryption Policy.

This Encryption Policy is designed to protect US Solutions Pvt Ltd.'s sensitive information and ensure compliance with applicable laws and regulations. By adhering to these guidelines, Users contribute to a secure and compliant work environment.