“Your Company Name”
Data Encryption Policy

1. Overview

“Confidential Information” and Personally Identifiable Information (“PII”) must be protected while stored at rest and in transit. Appropriate encryption technologies must be used to protect the PII.

2. Purpose

The purpose of this policy is to provide guidance on the use of encryption technologies to protect data, information resources, and other Confidential Information or PII while stored at rest or transmitted between parties. This policy also provides direction to ensure that regulations are followed.

3. Scope

This policy applies to all staff that create, deploy, transmit, or support applications and system software containing Confidential Information or PII. It addresses encryption policy and controls for Confidential Information or PII that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

4. Policy

A. ACCESS

- The [Insert Appropriate Role] or their designee shall ensure:
- Policies, procedures, scenarios, and processes must identify Confidential Information or PII that must be encrypted to protect against persons or programs that have not been granted access.
- Implements appropriate mechanisms to encrypt and decrypt Confidential Information or PII whenever deemed appropriate. Internal procedures shall specify how [YOUR COMPANY] transmits sensitive information as well as how often the information is transmitted.
- When encryption is needed based on data classification to protect Confidential Information or PII during transmission. Procedures shall specify the methods of encryption used to protect the transmission of Confidential Information or PII.

B. ENCRYPTION KEY LENGTH

“Your Company” uses software encryption technology to protect Confidential Information or PII. To provide the highest-level security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information or PII.

The use of proprietary encryption algorithms is not allowed unless reviewed by qualified experts outside of the vendor in question and approved by Company management.

C. AT-REST ENCRYPTION

- Hard drives that are not fully encrypted (e.g., disks that one or more un-encrypted partitions, virtual disks) but connect to encrypted USB devices, may be vulnerable to a security breach from the encrypted region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing Confidential Information or PII.
- Confidential Information or PII at rest on computer systems owned by and located within [Your Company] controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:
- Disk/File System Encryption (e.g. Microsoft EFS technology)
- Use of Virtual Private Networks (VPN's) and Firewalls with strict access controls that authenticate the identity of those individuals accessing the Confidential Information or PII
- Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring PII)
- Supplemental compensating or complementary security controls including complex passwords, and physical isolation/access to the data
- Password protection to be used in combination with all controls including encryption
- File systems, disks, and tape drives in servers and Storage Area Network (SAN) environments are encrypted using industry-standard encryption technology
- Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal

D. PORTABLE DEVICE ENCRYPTION

- Portable devices (e.g. smartphones, flash cards, SD cards, USB file storage) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of Confidential Information or PII are the result of stolen or lost portable computing devices. The most reliable way to prevent exposure is to avoid storing Confidential Information or PII on these devices.
- As a general practice, Confidential Information or PII shall not be copied to or stored on a portable computing device or [Your Company]-owned computing device. However, in situations requiring Confidential Information or PII to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen. The following procedures shall be implemented when using portable storage:
- Hard drives (laptops, tablets, smartphones and personal digital assistants (PDAs)) shall be encrypted using products and/or methods approved by [YOUR COMPANY] [Insert Appropriate Roles]. Unless otherwise approved by management, such devices shall have full disk encryption with pre-boot authentication.
- Devices shall not be used for the long-term storage of any Confidential Information or PII.
- All devices shall have proper and appropriate protection mechanisms installed including approved anti-malware/virus software, personal firewalls with unneeded services and ports turned off, and properly configured applications.
- Removable media including CD's, DVD's, USB flash drives, etc. shall not be used to store Confidential Information or PII.

E. IN-TRANSIT ENCRYPTION

In-transit encryption refers to the transmission of data between end-points. The intent of these policies is to ensure that Confidential Information or PII transmitted between companies, across physical networks, or wirelessly is secured and encrypted in a fashion that protects Confidential Information or PII from a breach.

The [Insert Appropriate Role] or their designee shall ensure:

- Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information through the use of all types of communication and transmission facilities.
- Users follow [YOUR COMPANY] acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential Information or PII received from non-[YOUR COMPANY] staff.
- Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard Confidential Information or PII during transmission over open public networks. Such controls include:
- Public networks include but are not limited to the Internet, Wireless technologies, including 802.11, Bluetooth, and cellular technologies.
- Confidential Information or PII transmitted in e-mail messages are encrypted. Any Confidential Information or PII transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with [YOUR COMPANY] must be encrypted or transmitted through an encrypted tunnel (VPN) or point-to-point tunneling protocols (PPTP) that include current transport layer security (TLS) implementations.
- Wireless (Wi-Fi) transmissions used to access [YOUR COMPANY] computing devices or internal networks must be encrypted using current wireless security standard protocols.
- Encryption or an encrypted/secured channel is required when users access [YOUR COMPANY] Confidential Information or PII remotely from a shared network, including connections from a Bluetooth device to a [YOUR COMPANY] PDA or cell phone.
- All non-console administrative access such as browser/web based management tools are encrypted using SSL based browser technologies using the most current security algorithm.

F. ENCRYPTION KEY MANAGEMENT

Effective enterprise public and private key management is a crucial element in ensuring encryption system security. Key management procedures must ensure that authorized users can access and decrypt all encrypted Confidential Information or PII using controls that meet operational needs. [YOUR COMPANY] key management systems are characterized by the following security precautions and attributes:

- [YOUR COMPANY] uses procedural controls to enforce the concepts of least privilege and separation of duties for staff. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor staff.

- [Insert Appropriate Role] shall verify backup storage for key passwords, files, and Confidential Information or PII to avoid a single point of failure and ensure access to encrypted Confidential Information or PII.
- Key management should be fully automated. [YOUR COMPANY] [Insert Appropriate Role] should not have the opportunity to expose a key or influence the key creation.
- Keys in storage and transit must be encrypted.
- Private keys must be kept confidential.
- Application and system resource owners should be responsible for establishing data encryption policies that grant exceptions based on demonstration of a business need and an assessment of the risk of unauthorized access to or loss of Confidential Information or PII.

The [Insert Appropriate Role] or their designee shall ensure:

- Decryption keys are not associated with user accounts.
- Documentation and procedures exist to protect keys used to secure stored Confidential Information or PII against disclosure and misuse.
- Restrict access to cryptographic keys to the fewest number of custodians necessary.
- Cryptographic keys are stored in the fewest possible locations.
- Key management processes and procedures for cryptographic keys are fully documented.
- Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.

Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived. Archived cryptographic keys should only be used for decryption/verification purposes.

Cryptographic key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of [YOUR COMPANY] operational methodology.

- [YOUR COMPANY] shall inventory and audit encrypted devices and validate the implementation of encryption products at least annually.
- At-Rest encryption procedures exist and can be demonstrated.
- Exception logs exist and can be produced for those resources that are excluded from this policy.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

This policy is to be distributed to all [YOUR COMPANY] staff and contractors using [YOUR COMPANY] Confidential Information or PII resources.

7. Policy Version History

Date of Change	Responsible	Summary of Change
July 1 2022		First Draft