MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Data Encryption		
Policy: ☒ Procedure: ☐ Page: 1 of 2	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 09.10.2024 Review Date:	Related Policies:

Purpose

This policy ensures that all data, both at rest and in transit, is encrypted and protected from unauthorized access, modification, or disclosure.

Policy

All data, both at rest and in transit, must be encrypted using approved encryption algorithms and standards. The encryption keys must be securely stored and managed, and only authorized personnel should have access to them. The encryption process must be documented and audited regularly. Any breach or suspected breach of this policy must be reported immediately to the Chief Information Officer (CIO).

The Chief Information Officer is responsible for ensuring Mid-State Health Network (MSHN) systems operate according to the following requirements and for testing all of the following:

- **All data in motion** transmitted over public networks, internal networks, or between our organization and external parties must be encrypted using secure protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption strength and protocols used for data in motion must align with industry best practices and relevant regulatory requirements. Any emails with sensitive information (e.g. person served protected information) must be encrypted.
- **All data at rest** must be encrypted using Advanced Encryption Standard-256 (AES-256) or higher encryption algorithm based on industry best practices and relevant regulatory requirements. This includes data stored on internal and external hard drives of laptops, desktops, tablets, servers, mobile devices of any kind, flash drives, CDs, DVDs, and cloud services. The encryption keys must be stored separately from the data and must be protected by strong passwords with multi-factor authentication. Backups of sensitive information are a form of data-at-rest and must be encrypted in a manner that protects the integrity of the data and prevents access by unauthorized individuals or information systems, like those used in data exfiltration and encryption attacks.
- **All encryption keys** must be generated, stored, and managed using approved encryption software and hardware. The encryption software and hardware must be updated regularly to ensure compliance with the latest security standards and best practices. The encryption keys must be backed up and restored securely and must be revoked or destroyed when no longer needed.
- **All encryption activities** must be logged and monitored using approved encryption tools and systems. The encryption logs and reports must be reviewed and audited regularly by authorized personnel. The encryption tools and systems must be configured to alert and notify the relevant parties in case of any encryption errors, failures, or anomalies.
- **Third-party service providers and cloud services:** MSHN CIO or designee will review the data encryption practices of any third-party vendor who handles sensitive information to be sure they meet our standards prior to engaging with them and conduct periodic reviews of their information security practices,

including data encryption. Data at rest, in motion, and in use within a cloud service must be encrypted using these same standards.

- **Compliance Monitoring:** MSHN CIO, or designee will regularly monitor and audit compliance with this Data Encryption procedure to ensure adherence to the established encryption requirements. Non-compliance with this procedure may result in disciplinary action, including termination of employment or contract.

Applies to

- ☒ All Mid-State Health Network Staff
- ☐ Selected MSHN Staff, as follows:
- ☐ MSHN's CMHSP Participants: ☐Policy Only ☐Policy and Procedure
- ☒ Other: IT Service Provider

Definitions

AES-256: Advanced Encryption Standard 256. One of the highest encryption standards in existence today and is used by the federal government to encrypt classified data.

CIO: Chief Information Officer

Encryption is storing sensitive information with a secret code. It scrambles the data so only those with the correct code can unlock it.

Data in motion refers to data that is actively moving from one device or system to another. An example would be sending an email with an attached document. The document and the email itself are considered data in motion.

Data at rest refers to data not actively being accessed or used. An example would be a document that was saved on the computer's hard drive. The document is not open or being modified but stored on the computer.

Data in use refers to information being accessed, processed, or used by individuals or computer systems. An example would be a document open and actively edited. Document editing, typing, or reading is considered data in use.

MSHN: Mid-State Health Network

SSL: Secure Sockets Layer

TSL: Transport Layer Security

Other Related Materials

N/A

References/Legal Authority

N/A

Change Log:

Date of Change	Description of Change	Responsible Party
07.01.2024	New Policy	Chief Information Officer