MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Document Sharing Policy		
Policy: ☒ Procedure: ☐ Page: 1 of 3	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 03.04.2025 Review Date:	Related Policies:

Purpose

This policy establishes the rules for sharing documents when the organization uses Box and/or Microsoft SharePoint as its document management systems. This policy aims to ensure that sensitive information is protected and that the approved methods and conditions for document sharing are followed.

Policy

This policy covers all types of Mid-State Health Network (MSHN) created or possessed documents, including but not limited to reports, proposals, presentations, protected health information, spreadsheets, and images.

The following are the policy statements for document sharing outside the organization:

- All documents must be classified according to their sensitivity and confidentiality level, such as public, internal, confidential, or restricted. Documents other than Public, stored in BOX must be marked with the appropriate classification.
- All documents must be shared with the awareness of the risks and responsibilities involved. The Document Owner must inform the Document Recipient of the expectations and obligations of the document sharing for all non-public classifications, such as not forwarding, copying, modifying, or disclosing the document without permission.
- Documents, other than public, may be shared only when there is a legitimate business need.
- Documents, other than public, may only be shared externally (outside of MSHN) through the approved methods and platforms, namely secure email attachments, Secure File Transfer Protocol (SFTP) servers and Box. Other methods and platforms, such as removable media or personal cloud storage such as DropBox are prohibited.
- Documents, other than public, may only be shared with the appropriate level of access and permissions, such as view-only, download, edit, or co-author. The Document Owner must select the minimum level of access and permissions required for the document sharing purpose.
- Documents, other than public, may be shared with external parties with the option to revoke access at any time. The Document Owner must set an expiration date for the document sharing link and monitor the document access activity. See the Information Protection Procedure for instructions on how to do this.
- Documents, other than public, may be shared with external parties but must have the appropriate disclaimer and confidentiality notice as follows: DISCLAIMER: This communication, and any attachments, is intended only for the use of the addressee and may contain legally privileged and confidential information. If you are not the intended recipient, please do not read it, reply to the sender that you received the message in error, and erase or destroy the message and its attachments without reading, printing, or saving. The Document Owner must include a statement that the document is the property of Mid-State Health Network (MSHN) and that it is intended for the authorized recipient only.

Responsibilities

- The leadership team is responsible for developing, implementing, and enforcing this policy and related procedures.
- The Document Owners are responsible for identifying and setting the document's classification level
- The document sharer is responsible for identifying the documents that need to be shared, obtaining the necessary approvals, and sharing the documents through the approved methods and platforms, setting the expiration date of the sharing link and including the disclaimers
- The Document Recipients are responsible for complying with the terms and conditions of the document sharing, respecting the confidentiality and integrity of the documents, and notifying the Document Owners of any issues or concerns.
- The Information Technology Service Provider is responsible for providing technical support and guidance for using Box and other tools as the document sharing platforms.
- All Users are responsible for adhering to this policy and related procedures, reporting any incidents or violations, and completing any required training and awareness sessions.

Applies to

☒ All Mid-State Health Network Staff

☐ Selected MSHN Staff, as follows:

☐ MSHN's CMHSP Participants: ☐Policy Only ☐Policy and Procedure

☐ Other: Sub-contract Providers

Definitions

Confidential: Data that belongs to or is provided by our clients, and whose sensitivity and confidentiality are determined by the client's own policies and agreements. Client Confidential Data must be protected according to the client's requirements and expectations and according to applicable laws such as Health Insurance Portability and Accountability Act (HIPAA).

Document Owner: is the MSHN staff member that is most responsible for the folder or document. In most cases this will be the person that created the document or folder. If the document comes from a source outside of MSHN staff, then the person that either received the file or decided to put it into BOX would be considered the owner.

HIPAA: Health Insurance Portability and Accountability Act

Internal: Data that is moderately sensitive and confidential, and whose unauthorized disclosure, modification, or loss could cause moderate damage to the organization, its clients, or its partners. Internal Data must be protected with a reasonable level of security and access control.

MSHN: Mid-State Health Network

Public: Data that is not sensitive or confidential, and whose disclosure, modification, or loss would not cause any damage to the organization, its clients, or its partners. Public Data can be freely shared and accessed by anyone without any restrictions.

Restricted: Data that is highly sensitive and confidential, and whose unauthorized disclosure, modification, or loss could cause severe damage to the organization, its clients, or its partners. Restricted Data must be protected with the highest level of security and access control.

SFTP: Secure File Transfer Protocol

Other Related Materials
N/A

References/Legal Authority
N/A

Change Log:

Date of Change	Description of Change	Responsible Party
10.01.2024	New Policy	Chief Information Officer