MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	**Information Technology**		
Title:	**Information Protection Procedure**		
Policy: □ **Procedure:** ☒ **Page:** 1 of 7	**Review Cycle:** Biennial **Author:** Chief Information Officer	**Adopted Date: 03.04.2025** **Review Date:**	**Related Policies:** **Document Sharing Policy**

Purpose

The purpose of this procedure is to ensure documentation stored in BOX is classified appropriately to strengthen information sharing protections for Mid-State Health Network (MSHN). BOX utilizes labels to classify and handle data according to sensitivity and confidentiality. In addition, this procedure supports privacy and security of the data and compliance with legal and contractual obligations.

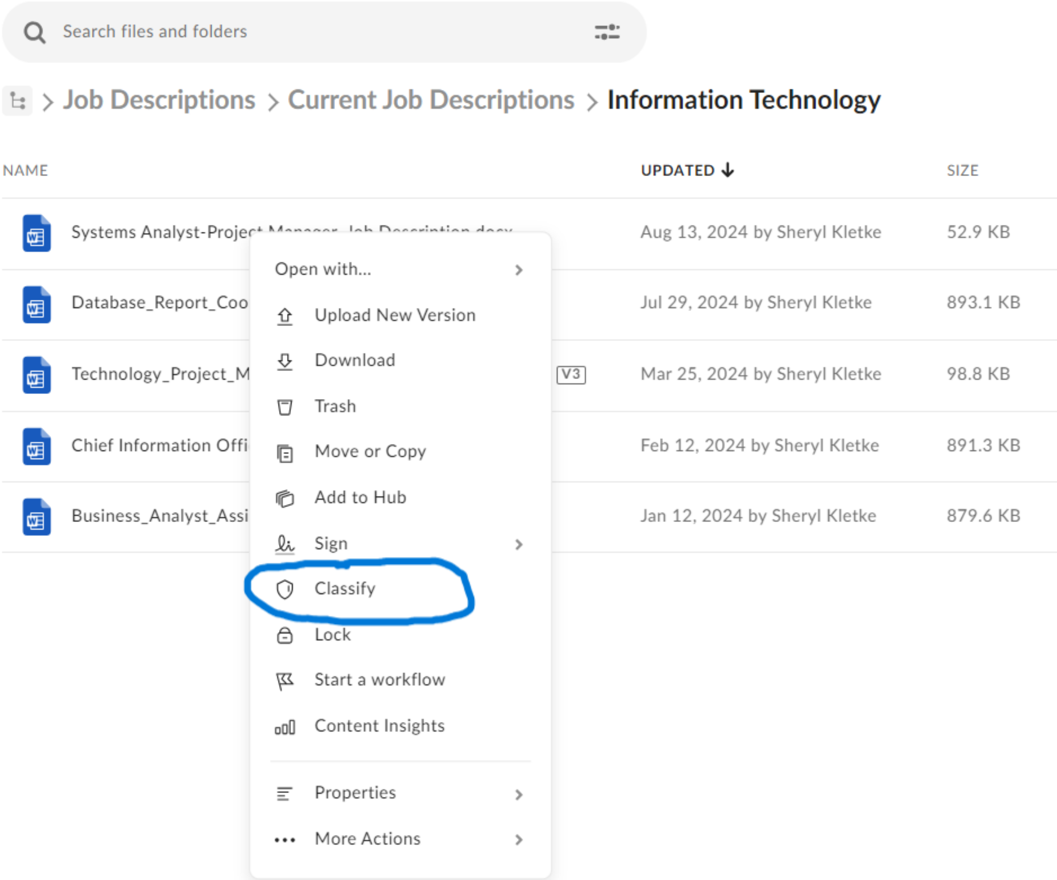
Procedure

The classification labels in BOX include the following:

1. Restricted
2. Internal
3. Public
4. Confidential

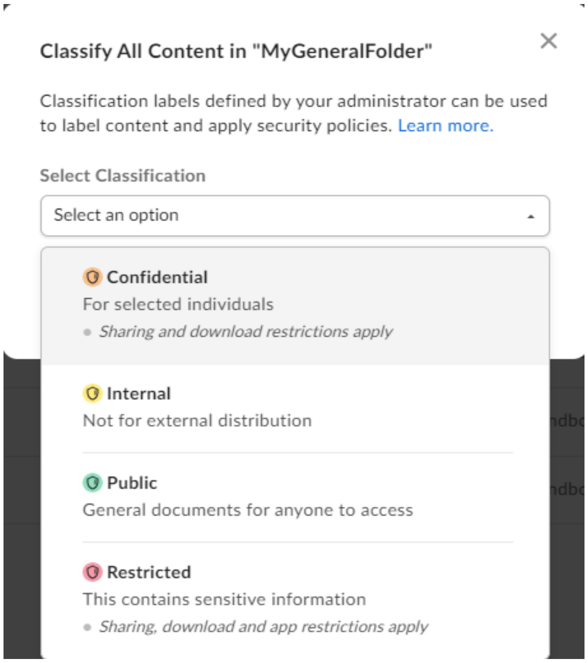
- All documents stored in BOX must be labeled with the appropriate classification. THIS INCLUDES ALL BOX FOLDERS INCLUDING PERSONAL FOLDERS.
- The responsible Chief/Director must ensure that their staff are correctly classifying all documents and confirming they have the correct label for their area of responsibility.
- The Document Owner must classify the document according to the table below.
- Anyone sharing the document is responsible for ensuring that the data is handled in compliance with the applicable laws, regulations, standards, and contracts, taking note of the classification label.
- The staff sharing the document must set an expiration date for the document sharing link and enable the option to revoke access at any time. (THERE MAY NEED TO BE AN INSTRUCTION/STEP-BY-STEP LANGUAGE HERE ON HOW TO DO THIS).
- The staff sharing the document must include a disclaimer and confidentiality notice in the document or in the email that contains the document sharing link. The Chief Information Officer shall provide the required disclaimer for use. (RECOMMEND INCLUDING THE DISCLAIMER HERE).
- The staff sharing the document must send the document sharing link to the Document Recipient and inform them of the expectations and obligations of the document sharing.
- The staff sharing the document must monitor the document access activity and revoke access if needed. This is accomplished by right-clicking the file and choosing More Actions and then Manage Collaborators from the fly-out. This shows who the file has been shared with. If there is someone that should not have access, choose the link in the Permission column and then choose Remove. This should be done at an interval this is consistent with the sensitivity and usefulness of the document.
- Staff must report any incidents or violations of this policy to the Chief Information Officer.

To add a classification label to a document or folder, right-click on the object and choose classify.



NAME	UPDATED ↓	SIZE
Systems Analyst-Projec	Aug 13, 2024 by Sheryl Kletke	52.9 KB
Database_Report_Coo	Jul 29, 2024 by Sheryl Kletke	893.1 KB
Technology_Project_M V3	Mar 25, 2024 by Sheryl Kletke	98.8 KB
Chief Information Offi	Feb 12, 2024 by Sheryl Kletke	891.3 KB
Business_Analyst_Assi	Jan 12, 2024 by Sheryl Kletke	879.6 KB

A dropdown box will appear with the available labels to select from.



Classify All Content in "MyGeneralFolder"

Classification labels defined by your administrator can be used to label content and apply security policies. Learn more.

Select Classification

Select an option

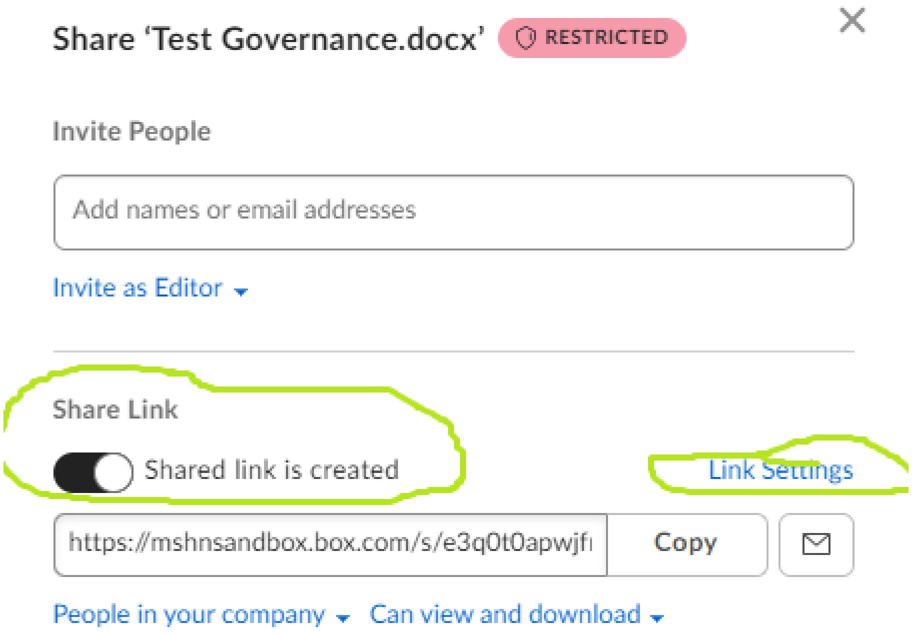
Confidential
For selected individuals
Sharing and download restrictions apply

Internal
Not for external distribution

Public
General documents for anyone to access

Restricted
This contains sensitive information
Sharing, download and app restrictions apply

To set an expiration date, when the shared dialog comes up there is a Link Settings to the right. You may need to toggle on the Shared Link button.



Share 'Test Governance.docx' RESTRICTED ×

Invite People

Add names or email addresses

Invite as Editor ▾

Share Link

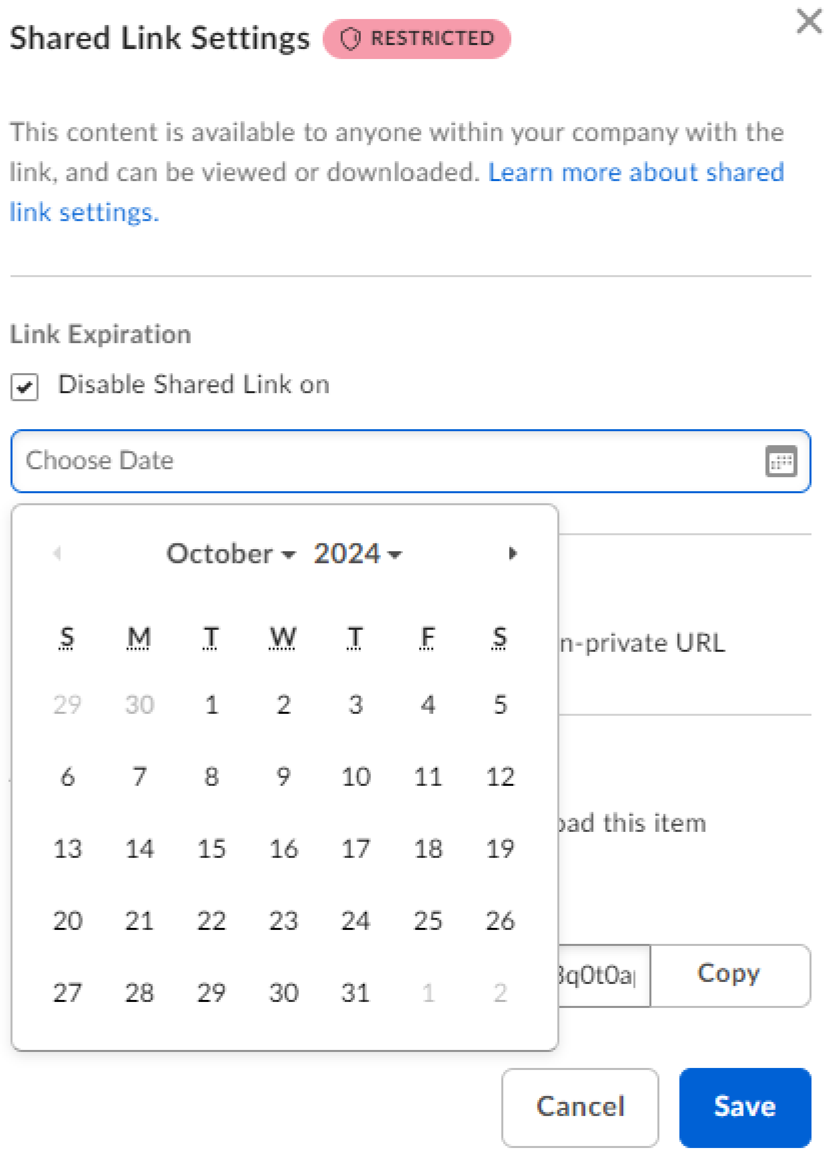
● Shared link is created

Link Settings

https://mshnsandbox.box.com/s/e3q0t0apwjf

People in your company ▾ Can view and download ▾

Click the first option in the new dialog for link expiration, click the box to access the date picker. Click the box that says Link Expiration.



Shared Link Settings RESTRICTED

This content is available to anyone within your company with the link, and can be viewed or downloaded. Learn more about shared link settings.

Link Expiration

☑ Disable Shared Link on

Choose Date

The following table summarizes the four data classification labels and their definitions. The table also provides some examples of data types that fall under each label. The examples are not exhaustive and are only meant to illustrate the general characteristics of each label. The Document Owner is responsible for determining the appropriate label for each folder or document item based on its content and context.

Label	**Definition**	**Examples**
Restricted Data	Data that is highly sensitive and confidential, and whose unauthorized disclosure, modification, or loss could cause severe damage to the organization, its consumers, or its provider network. Restricted Data must be protected with the highest level of security and access control.	Personal data of employees, medical information, suppliers, financial data, legal documents, security logs, encryption keys, passwords, etc.

Confidential Data	Data that belongs to or is provided by our consumers or employees. Confidential Data must be protected according to the consumer's requirements and expectations and according to applicable laws such as Health Insurance Portability and Accountability Act (HIPAA) and applicable human resources standards.	Individual consumer data (services, utilization, progress notes, assessments, etc.) Note: Excludes aggregate information Employee information (Performance reviews, resumes, applications)
Internal Data	Data that is moderately sensitive and confidential, and whose unauthorized disclosure, modification, or loss could cause moderate damage to the organization, its consumers, or its provider network. Internal Data must be protected with a reasonable level of security and access control.	Internal policies and procedures; business plans and strategies; project reports and proposals; meeting minutes; etc. Internal email exchanges or any other written communication that should not be exposed to external sources.
Public Data	Data that is not sensitive or confidential, and whose disclosure, modification, or loss would not cause any damage to the organization, its consumers, or its provider network. Public Data can be freely shared and accessed by anyone without any restrictions.	Public website content; marketing materials; press releases; newsletters; brochures; etc.

The following guidelines provide some general best practices for how to handle data according to its classification label. The guidelines are not exhaustive and are meant to provide examples of the rules and procedures that apply to each data item.

All Data

- Store non-public data only on authorized and approved devices and servers that are protected by adequate security measures. Examples of approved devices include the MSHN provided laptop and BOX. Examples of unapproved devices include external storage devices (Thumb drive, etc) and personal computers.
- Encrypt non-public data at rest and in transit using standard encryption methods and algorithms. Examples of acceptable encryption are on employee's laptop using the encryption included in Outlook. Examples of unencrypted methods are personal computers, external storage devices and general emails not using the Encrypt option in Outlook. Encrypt is found in the menu under Options when composing a message.
- Use secure and encrypted channels and methods to share Restricted Data, such as Virtual Private Network (VPN), Secure Hypertext Transfer Protocol (HTTPS), Secure File Transfer Protocol (SFTP), etc.
- Do not store or share non-public data on any personal or unapproved devices, servers, or cloud services.
- Do not send or receive non-public data via standard email, instant messaging, or social media.
- Report any suspected or actual breach, loss, or misuse of non-public data immediately to the Chief Information Officer and the Privacy Officer.

Restricted Data

- Share Restricted Data only with authorized and authenticated recipients who have a legitimate need to access the data.
- Do not copy, print, or download Restricted Data unless absolutely necessary.

- Do not disclose or discuss Restricted Data with anyone who is not authorized or involved in the data processing.
- Dispose of Restricted Data securely and permanently using approved methods and tools, such as shredding or wiping.

Confidential Data

- Share Confidential Data only with authorized and authenticated recipients who meet the allowed definition according to the Health Insurance Portability and Accountability Act (HIPAA).
- Do not copy, print, or download Confidential Data unless absolutely necessary to fulfill the job function and ensure complete removal when the need is removed.
- Do not disclose or discuss Confidential Data with anyone who is not authorized or involved in the data processing.
- Dispose of Confidential Data securely and permanently using approved methods and tools, such as shredding, wiping, or deleting.

Internal Data

- Share Internal Data only with authorized and authenticated recipients who have a business need to access the data.
- Do not disclose or discuss Internal Data with anyone who is not authorized or involved in the data processing.
- Dispose of Internal Data securely and permanently using approved methods and tools, such as shredding or wiping or deleting.

Public Data

- Store Public Data on any devices and servers that are accessible and convenient for the intended audience.
- Share Public Data freely and openly with anyone who is interested or affected by the data.
- Use any channels and methods to share Public Data, such as email, instant messaging, social media, etc.
- Do not store or share Public Data on any devices, servers, or cloud services that are not secure or unreliable.
- Do not send or receive Public Data via email, instant messaging, social media or via methods that are not secure or unreliable.
- Dispose of Public Data as needed or required by the data owner or the data retention policy.
- Report any suspected or actual loss, or misuse of Public Data to the IT department.

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

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

HIPAA: Health Insurance Portability and Accountability Act

HTTPS: Secure Hypertext Transfer Protocol

IT: Information Technology

MSHN: Mid-State Health Network

SFTP: Secure File Transfer Protocol
VPN: Virtual Private Network

Other Related Materials

N/A

References/Legal Authority

N/A

Change Log:

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