MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Data Backup		
Policy: ☐ Procedure: ☒ Page: 1 of 3	Review Cycle: Biennial Author: Chief Information Officer	Adopted Date: 09.10.2024 Review Date:	Related Policies:

Purpose

The purpose of this procedure is to ensure that the organization's data is regularly backed up and can be restored in the event of hardware failure, cyberattack, disaster, or any other incident that may compromise the availability, integrity, or confidentiality of the data.

Procedure

This procedure applies to all data that is created, stored, processed, or transmitted by the organization, including but not limited to:

- Microsoft 365 data, such as email, contacts, calendars, SharePoint, OneDrive, Teams, and Box.
- Financial data, such as accounting, payroll, and invoicing records.
- Customer data, such as reports, lists, backups, etc.
- Employee data, such as personal information, performance reviews, and training records.
- Operational data, such as meeting notes, plans, website source code, etc.

This procedure does not apply to data classified as temporary, obsolete, or redundant, not retained for business, legal, or regulatory purposes and third-party software (such as iPrism, Intact, PCE) as the software provider is required per contract to conduct backup.

The following roles and individuals are responsible for implementing and maintaining this procedure:

- The Information Technology (IT) Service Provider is responsible for overseeing the organization's data backup strategy, selecting, and configuring the backup tools and services, ensuring the backup schedule and frequency are adequate and consistent, and verifying the backup quality and integrity.
- The IT Service Provider is responsible for performing the data backup operations, monitoring the backup status and performance, reporting any backup issues or failures, and restoring the data as needed.
- The Chief Information Officer (CIO) is responsible for identifying and classifying Mid-State Health Network (MSHN) data that needs to be backed up, ensuring the data is safely stored and organized, and requesting the data restoration in case of data loss or corruption.
- Employees are responsible for following the organization's data security and privacy policies, avoiding the unauthorized access, modification, or deletion of the data, and reporting any data incidents or anomalies.

Backup Frequency

The organization's data backup frequency depends on the type, value, and volatility of the data, as well as the available backup resources and the recovery time objectives. The following table summarizes the backup frequency for distinct types of data:

Data Type	Backup Frequency
Microsoft 365 data	Multiple Times per Day
Financial data	As determined in consultation with vendor: Maner
Consumer/Beneficiary data	As determined in consultation with vendor: PCE
Employee data	As determined in consultation with vendor: CoStaff
Operational data (Box)	Daily

The backup frequency may be adjusted as needed, based on the changes in the data volume, importance, or usage.

Backup Methods

The organization's data backup methods depend on the source, format, and size of the data, as well as the backup destination and the recovery point objectives. The following table summarizes the backup methods for distinct types of data:

Data Type	Backup Method
Microsoft 365 data	Cloud-to-cloud backup using a third-party service provider that supports Microsoft 365 backup and recovery
Financial data	As determined in consultation with vendor: Maner
Customer data	As determined in consultation with vendor: PCE
Employee data	As determined in consultation with vendor: CoStaff
Operational data (Box)	Full Image Based backup to an external hard drive with an offsite storage component, or direct to cloud. Incremental backups after first full.

The backup methods may be modified as needed, based on the availability, reliability, and compatibility of the backup tools and services. Backup data must be protected with strong encryption, per the Data Encryption Policy.

Restoration Procedures

The organization's data restoration procedures depend on the cause, scope, and impact of the data loss or corruption, as well as the backup location and the recovery time objectives. The following steps outline the general data restoration procedures:

1. Identify and report the data loss or corruption incident to the Chief Information Officer.
2. The CIO shall report all incidents to the IT Service Provider.
3. The IT Service Provider shall:
    a) Determine the extent and severity of the data loss or corruption, and the potential business, legal, or regulatory implications.
    b) Identify the backup source and destination, and the backup date and time that are closest to the data loss or corruption event.
    c) Verify the backup quality and integrity and ensure the backup data is not compromised or infected.
    d) Restore the backup data to the original or alternative location and verify the restoration status and performance.

e) Validate the restored data with the Chief Information Officer and ensure the data is accurate, complete, and functional.
f) Document and analyze the data loss or corruption incident and the data restoration process and identify the root cause and the corrective and preventive actions, including submission of said report to the Chief Information Officer

4. The CIO shall review the report and ensure corrective actions are implemented.

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

CIO: Chief Information Officer
IT: Information Technology
MSHN: Mid-State Health Network

Other Related Materials

N/A

References/Legal Authority

N/A

Change Log:

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