St. Clair County Community Mental Health
Providing Opportunities for Health, Wellness, & Connection

Administrative Policy

Policy Title: **Loss Prevention & Recovery of Data and Information**

Policy #: **08-001-0015**

Effective Date:	11/26/2024
Approved by:	Telly Delor, Chief Operating Officer
Functional Area:	Administrative
Responsible Leader:	Dann Hayes, IT & Security Director
Policy Owner:	Chase Sherman, IT Technician
Applies to:	All SCCCMH Staff, SCCCMH Board Members, All Directly Operated Programs, Contracted Network Providers

Purpose: To ensure back-ups are created for the recovery of data and information in times of hardware failure, data corruption, or human error.

I. Policy Statement

It is the policy of St. Clair County Community Mental Health (SCCCMH) to ensure that all data gathered and stored in a *digital format*, or information converted to a digital format for storage, indexing, retrieval, and eventual archival shall reside on server platform(s) controlled by SCCCMH. Data will be backed up at intervals no longer than once every business day. All data backups shall be performed on identified media and replicated to an off-site location for thirty days in accordance with the Information Technology Disaster Recovery Plan.

II. Standards

A. Backups are verified for success at the beginning of each business day.

B. If backups have not been successful, every effort is made to perform the backup immediately. If the backup deteriorates network or server performance, the backup is performed as soon as it can be scheduled without degrading server or network performance.

C. *Backup replication* is done daily, Monday through Friday. There will be daily, weekly, monthly, quarterly, and annual backup replications.

D. The weekly Backup Replication shall be stored at an off-site location for thirty days.

E. The monthly and quarterly Backup Replication shall be replicated and stored at an offsite location on the next business day as outlined in the IT Disaster Recovery Plan.

F. A log of all weekly, quarterly, and annual backups will be maintained within the backup application utility for auditing purposes.

III. Procedures, Definitions, and Other Resources

A. Procedures

Responsibilities

Position	Responsibilities
IT Staff	Ensure all data is backed up successfully during scheduled times.

Actions

Action Number	Responsible Stakeholder	Details
1.0	IT Staff	1. Ensure that network backups are completed on a daily basis. 2. Verify that all backups completed successfully. 3. Ensure that backups are stored off-site on a weekly basis; or monthly, quarterly, and annually, as appropriate.

B. Related Policies

N/A

C. Definitions

1. *Digital Format:* Information stored within the computer system in a database or document file format.

2. *Electronic Protected Healthcare Information (ePHI):* Any individually identifiable health information stored on hard drives, laptops, desktops, memory sticks and mobile devices; contained in e-mail; or transmitted from or to the Covered Entity.

3. *Backup Replication:* Backup replication is the act of copying and then moving data from one company site to another. This is done for an immediate and smooth resumption of business operations after a disaster.

D. Forms

N/A

E. Other Resources (i.e., training, secondary contact information, exhibits, etc.)

N/A

F. References

1. Disaster Recovery Plan

IV. History

- Initial Approval Date: 02/2002
- Last Revision Date: 10/2024 BY: Chase Sherman
- Last Reviewed Date: 11/2023 BY: Tommy Rankin
- Non-Substantive Revisions: N/A
- Key Words: Loss Prevention, Data, Recovery