MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

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

Purpose

The purpose of this policy is to protect the organization's information assets from unauthorized access, disclosure, modification, damage, or loss that may result from the use of removable media devices such as USB drives, CDs, DVDs, external hard drives, flash memory cards and other portable storage devices.

Policy

The following statements define the rules and policies for using removable media devices in the Mid-State Health Network (MSHN) organization:

- Removable media devices with an unknown origin, such as a thumb drive found on the floor, desk, breakroom, conference room, etc., must NEVER be mounted on any organization's computer to look at what data the device may contain. A common cyber-attack scheme is to leave anonymous devices infected with malware in places where employees will find them, then when the employee is curious to see what is on the drive, their computer becomes infected.
- Removable media devices must not be used with MSHN devices.
- Removable media devices must not be used to bypass or circumvent any security controls or measures implemented by Mid-State Health Network or its network or systems.
- Removable media devices must not be connected to or used on any unauthorized, untrusted, or insecure computer, network, or system.

The organization reserves the right to confiscate, inspect, or erase any removable media device or its contents that are suspected of violating this procedure or posing a security risk.

The Chief Information Officer's (CIO) role is responsible for developing, maintaining, and updating this policy, and for providing guidance and support on the use of removable media devices.
The Information Technology (IT) Service Provider is responsible for providing the technical controls and tools for managing and monitoring the use of removable media devices, and for responding to any information security incidents or issues involving removable media devices.

MSHN supervisors are responsible for ensuring that their staff comply with this policy and for reporting any violations or exceptions to the Chief Information Officer.

Employees who utilize removable media devices are responsible for following this procedure and for protecting the organization's information or data on removable media devices from unauthorized access, disclosure, modification, damage, or loss.

Exceptions
Any exceptions to this procedure must be justified by a compelling business or operational need and approved by the Chief Information Officer in writing. Exceptions must be documented and reviewed periodically by the CIO to ensure that they are still valid and necessary.

- Removable media devices must be encrypted using the approved encryption software and methods and must have a strong password or passphrase to access the encrypted data.
- Removable media devices must be scanned for malware, viruses, spyware, or ransomware before they are connected to the organization's network or systems.
- Removable media devices must be labeled with the owner's name and contact information and must have a unique identifier or serial number.
- Removable media devices must be stored in a secure location when not in use and must not be left unattended or exposed to theft, loss, or damage.
- Removable media devices must be disposed of or destroyed in a secure manner when they are no longer needed or authorized and must be wiped or erased of any residual data.
- Removable media devices must not be shared with or loaned to other users or third parties without prior authorization from the Chief Information Officer.
- Removable media devices must not be used to store or transport any information or data classified as confidential, restricted, or sensitive, unless there is a valid business need and written approval from the Chief Information Officer.

Non-Compliance
Any violation of this policy will be reported to the CIO and the Deputy Director. Depending on the violation, next steps may result in disciplinary action, up to and including termination of employment or contract, legal action, or criminal prosecution, depending on the severity and impact of the violation and in accordance with the Personnel Manual.

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 Policy	Chief Information Officer