POLICIES AND PROCEDURE MANUAL

Chapter:	**Information Technology**		
Title:	**Controlled Access and Least Privilege**		
Policy: ☒ **Procedure:** ☐ **Page:** 1 of 2	**Review Cycle:** Biennial **Author:** Chief Information Officer	**Adopted Date:** 09.10.2024 **Review Date:**	**Related Policies:**

Purpose

This policy ensures that Mid-State Health Network (MSHN) employees have access only to the information and resources necessary for their job roles. This policy minimizes the risk of threats and accidental data exposure by enforcing strict access controls.

Policy

The following statements define the principles and rules for implementing and enforcing controlled access and least privilege in the organization:

- Access to data, systems, and networks shall be granted on a need-to-know and need-to-use basis, in accordance with the user's job role and responsibilities.
- Access to data, systems, and networks shall be limited to the minimum level and duration necessary for the user to perform their assigned tasks and functions.
- Access to data, systems, and networks shall be authorized by the respective data, system, or network owner, or their designated delegate.
- Access to data, systems, and networks shall be reviewed and verified periodically, at least biennially, to ensure its validity, appropriateness, and compliance.
- Access to data, systems, and networks shall be revoked or modified promptly when the user's job role or responsibilities change, or when the user leaves the organization or no longer requires access.
- Access to data, systems, and networks shall be monitored and logged for audit and investigation purposes, and any unauthorized or suspicious access attempts or activities shall be reported and escalated.
- Access to data, systems, and networks shall be protected by strong authentication and encryption mechanisms, and users shall not share, disclose, or compromise their access credentials or devices.

Responsibilities

The following roles and responsibilities are assigned for the implementation and enforcement of this policy:

- The Leadership Team through the guidance of the Chief Information Officer (CIO) is responsible for overseeing the development, review, and approval of this procedure and ensuring its alignment with the organization's strategic goals and objectives.
- The Information Technology (IT) Service Provider is responsible for managing the access control processes and procedures, conducting regular audits and assessments, and reporting on the effectiveness and compliance of this policy (as identified through contractual language).
- Supervisors are responsible for identifying and classifying the data under their custody, determining the access requirements and permissions for the data, and approving or denying access requests, using the Computer Access form.

- The IT Service Provider is responsible for identifying and configuring the systems under their management, determining the access requirements and permissions for the systems, and approving or denying access requests.
- The IT Service Provider is responsible for identifying and securing the networks under their management, determining the access requirements and permissions for the networks, and approving or denying access requests.
- The Users are responsible for complying with this policy and the access control processes, requesting access only for legitimate business purposes, and safeguarding their access credentials and devices.

Exceptions

Any exceptions to this policy must be justified by a valid business or operational reason and approved by the supervisor, in writing, prior to granting the exception, which is at the discretion of the Chief Information Officer. Exceptions shall be documented by the CIO and reviewed periodically, at least biennially, to ensure their continued validity and appropriateness.

Non-Compliance

Any violation of this policy may result in disciplinary action, up to and including termination of employment or contract, legal action, or civil or criminal liability, as applicable.

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

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