MSHN
Mid-State Health Network

POLICIES AND PROCEDURE MANUAL

Chapter:	Information Technology		
Title:	Cybersecurity Awareness Training and Phish Testing Procedure		
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 procedure is to establish the requirements and guidelines for cybersecurity awareness training and phishing testing for all employees of Mid-State Health Network. The goal of the training and testing is to enhance the security posture of the organization by educating employees on the best practices and common threats related to cybersecurity, as well as assessing their ability to recognize and report phishing attempts.

Procedure

Phishing attacks are deceptive communications that trick employees into giving up sensitive information or installing harmful software. They can harm the organization and the employees in many ways. Therefore, all employees must complete an initial cybersecurity awareness training session of one hour within the first week of their employment, so that they can properly follow security guidelines for their devices and accounts. This is set up and assigned by the organization's Information Technology (IT) Service Provider. This will help the organization stay safe and secure.

The training session will cover the following topics:

- The importance and benefits of cybersecurity for the organization and the individual.
- The organization's cybersecurity policies and procedures.
- The roles and responsibilities of employees in protecting the organization's information and assets.
- The common types and sources of cyberattacks and how to prevent, detect, and respond to them.
- The best practices for creating and managing passwords.
- The indicators and consequences of a cybersecurity breach and how to report and escalate incidents.

After the initial training session, all employees must complete monthly online cybersecurity awareness training sessions of 8-13 minutes each. The monthly sessions will provide updates and refreshers on the topics covered in the initial session, as well as introduce new topics and scenarios relevant to the current threat landscape and the organization's needs. The monthly sessions may also include quizzes and assessments to measure the employees' knowledge and retention of the training material.

In addition to the training sessions, all employees will be tested with bi-monthly phishing testing exercises. The phishing testing exercises will involve simulated phishing emails sent to the employees' work email accounts, designed to mimic real-world phishing campaigns and techniques. The phishing emails will test the employees' ability to identify and report phishing attempts, as well as their compliance with the organization's policies and procedures. The phishing emails will not contain any malicious links or attachments but will record the employees' actions and responses.

With the assistance of the organization's IT Service Provider, MSHN will collect and analyze the data from the training and testing sessions and provide feedback and remediation to the employees as needed. The feedback and remediation may include:

- Individual and aggregate reports on the employees' performance and progress in the training and testing sessions.

- Recognition and rewards for the employees who demonstrate an elevated level of cybersecurity awareness and behavior.
- Additional training and coaching for the employees who show low levels of cybersecurity awareness and behavior.
- Refer to Deputy Director and Supervisor for appropriate disciplinary actions for the employees who repeatedly fail or violate the training and testing requirements or the organization's policies and procedures.

The data from the training and testing sessions will be used to evaluate and improve the effectiveness and relevance of the training and testing program, and to identify and address any gaps or weaknesses in the organization's cybersecurity posture.

The organization's IT Service Provider will conduct regular audits and monitoring to detect any violations of the Cybersecurity Awareness Training and Phish Testing policy and report such to the Chief Information Officer and Deputy Director.

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

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