Title: Cybersecurity Awareness and Training Policy
Effective Date:
Amended:
Issuing Authority: Board of Commissioners
Responsible Officer: Director of Information Technology

Category: 500
Number: 501

Purpose

To establish a mandatory comprehensive cybersecurity awareness and training program for anyone that has been assigned a County of Saginaw email account, ensuring understanding of critical information security practices, with specific focus on compliance with Federal Regulations.

Responsibility

Users: Anyone who has an assigned County email account is responsible for actively participating in Cybersecurity and Privacy Learning training and adhering to all outlined County of Saginaw cybersecurity policies.

Management: County of Saginaw Leaders are responsible for ensuring their teams receive and complete the mandatory cybersecurity awareness and training program and address any reported security concerns promptly.

Information Technology: The content of the cybersecurity awareness and training program must be reviewed and updated annually by the I.T. Department, or when significant changes to the enterprise occur.

Scope

This policy applies to all County of Saginaw Elected Officials, Judges, employees, contractors, third-party vendors, or anyone else who has access to the County's protected network. Anyone mentioned who fails to comply with this, or any County of Saginaw policy, is subject to disciplinary action outlined in the County of Saginaw Standards of Conduct and/or respective collective bargaining agreement.

Policy

Develop, Implement, and maintain a mandatory program for performing security awareness and training. The program must contain the following elements:

1. The cybersecurity awareness and training must be administered, at least quarterly, to all County of Saginaw users, who at a minimum, have a County of Saginaw email account or network access.
2. All new County of Saginaw users must complete cybersecurity awareness training prior to being granted access to enterprise assets (including remote access). The training must include:
    a. Identifying, storing, transferring, archiving, and destroying sensitive data.
    b. Any legal and / or regulatory obligations of the above.

3. All County users must receive training on understanding of social engineering attacks such as Phishing, Spear Phishing, Whaling, Smishing, and Vishing.
4. All County users must be trained in the best practices for authentication in the enterprise and best practices for handling enterprise data including Personal Identifying Information (PII) and Protected Health Information (PHI).
5. All County users must be trained on how to recognize and report security incidents, including insider threats.
6. All County users must be trained on the dangers of connecting to and transmitting enterprise data over insecure networks.
7. All County users with privileged access will receive and complete specialized security awareness training annually.
8. All County users that fail test Phishing events are required to complete the auto assigned refresher course, within 10 business days of notification.

County Administrator / Legal Counsel Review

The County Administrator has determined that this Policy, as submitted to the Board of Commissioners, contains the necessary substance in order to carry out the purpose of the policy. County Civil Counsel has determined that this Policy, as submitted, contains content that appears to be legal activities of the Saginaw County Board of Commissioners.

Approved as to Substance: Saginaw County Administrator	Approved as to Legal Content: Saginaw County Civil Counsel

ADOPTED: April 15, 2025

Regulatory Information

Category: HIPAA Administrative Safeguards
Type: Standard
Reference: 45 CFR §164.308(a)(5)(i), §164.308(a)(6)(ii), §164.308(a)(5)(ii)(A), §164.308(a)(5)(ii)(C), §164.308(a)(5)(ii)(D)
Category: HIPAA Physical Safeguards
Type: Standard
Reference: 45 CFR §164.310(d)(2)(i)
Category: CJISSECPOL
Version: 6.0
Reference: AC-3, AC-17, AC-22, AT-2, AT-3, AT-4, CP-3, IA-4, IR-2, IR-4, IR-7, PL-4, PS-7, PS-8, PS-9, SA-3, SA-8, SA-11, SI-12, SR-5, SR-6, SR-11
Category: CIS
Version: 8.1
Reference: IG 1, IG 2

Definitions

Cybersecurity Awareness Training is a program that can be dispensed to an organizations computer workforce that provides an in-depth understanding of the potential practical cyber threats they may encounter.

ePHI or PHI are any of 18 HIPAA identifiers used in conjunction with a person’s physical or mental health condition, health care, or a person’s payment for health care, which can be stored on paper or electronically.

Phishing is a type of social engineering where an attacker sends a nefarious message designed to trick a user into revealing sensitive information to the attacker or to deploy malicious software on the victim’s infrastructure such as Ransomware.

PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Smishing is a type of social engineering that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to threat actors.

Spear Phishing is a type of social engineering that involves sending personalized emails to specific people or organizations in an effort to share sensitive information.

Vishing is a type of social engineering that uses a phone scam to trick people into giving away sensitive information over the phone.

Whaling is a type of social engineering that involves tricking a high-profile executive or official into giving sensitive information or taking an action.