**Title:** Cybersecurity Awareness Program Policy
**Effective Date:** April 2, 2025
**Issuing Authority:** Senior Vice President for Administration and Finance
**Policy Contact:** Assistant VP of Information Technology and Chief Information Officer
helpdesk@mercer.edu, 478-301-7000

## Purpose

This policy establishes Mercer University with a comprehensive and measurable cybersecurity awareness program. Based on the globally recognized NIST SP800-16 and NIST SP800-50 standard for Information Technology Security Training and industry recommended practices, the program will help to ensure that Mercer University is proactively identifying and addressing the security risks presented by people.

## Scope

The program is designed to address the security awareness and training needs of all Mercer departments, divisions, locations, roles, and responsibilities. The program assists Mercer with designing, planning, and implementing a security awareness and training program. The intended audiences include but are not limited to employees, faculty, staff, student employees, and third parties. An awareness program should be aimed at all levels of the organization, which also includes senior management/leadership.

A successful security awareness and training program identifies and explains the proper behaviors when handling different devices and information. Success also relies on security awareness and training to become part of the organization's culture. The program will communicate the guidelines, policies, and best practices that need to be followed.

## Exclusions

Students are excluded unless employed at Mercer University with responsibilities that require this program.

## Policy Statement

### Requirements

The following requirements have been established to ensure consistency, reliability, and operational effectiveness across Mercer's systems, processes, and actions. They are based on NIST 800-171, Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Compliance with these requirements, and the processes described in this document, is mandatory.

| NIST 800-171 Control Number | Control Family | Control Text |
|---|---|---|
| **3.2.1** | **Awareness and Training** | Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. |
| **3.2.2** | **Awareness and Training** | Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. |
| **3.2.3** | **Awareness and Training** | Provide security awareness training on recognizing and reporting potential indicators of insider threat. |

**Program Considerations**
Mercer has taken the following areas into consideration when designing and implementing a security awareness program:

- The employee or team that will be responsible for overseeing the implementation and maintenance of the program;
- Timeframe for completion of the security training for new hires;
- A need for training due to a compliance or regulatory requirement to meet;
- Frequency of training and testing (e.g., annually, quarterly, monthly);
- The type of training content and methods by which training will be delivered;
- Employees to include in the training;
- Time constraints and availability;
- Senior management/leadership buy-in to carry out training and testing; and
- How non-compliance will be handled and enforced.

While this program describes the collective awareness efforts across all Mercer departments, it is anticipated that specific role-based training and awareness may be required for each audience.

**Roles and Responsibilities**

- Executive Director of IT Client Support Services – Responsible for:
    - Providing oversight for the overall Awareness Program for Mercer.
    - Coordinating with organizational/institutional departments and units to ensure participation and completion of training.

- Director of IT Help Desk – Responsible for:
    - Providing administration of awareness campaigns, scheduling and conducting online training and/or performing any social engineering testing.

- Tracking attendance of training sessions and obtaining and filing any attestations or post-training quizzes or tests.

**Awareness and Training Strategy**
At a minimum, all employees are required to take general security awareness training at least annually. All new hires of the organization have 14 days to complete their security awareness training.

**Information Security and Cybersecurity Best Practices**
This training may be conducted using different techniques and formats, and all based on the NIST SP800-16 (See References) standard and recommended practices. At a minimum, the training must address:

- Current Threats and Common Attacks
- Data Protection
- Modified Security Policies and Procedures
- Recommended Security Best Practices
- Identifying and Responding to Incidents
- Regulation, Laws, or Commercial Requirements

**Training Metrics**
The security awareness program should capture metrics that measure the overall human risk and behaviors. The metrics should ensure that the organization's awareness program is compliant with regulatory requirements and if human behavior is changing. Additional metrics that can be captured but not limited to are:

- Number of users that attended last training;
- Number of users falling victim to phishing attacks;
- Number of security events reported to IT or Information Security; and
- Number of users who fail sanctioned phishing tests.

Additional assessments may be necessary to capture the overall effectiveness of the security awareness program.

**Testing/Assessments**
Social Engineering – In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.
Social engineering tests should be conducted on a regular basis to continuously measure the susceptibility of employees, faculty, staff, students to common attacks. Tests and assessments may be delivered in the following formats:

- Phishing – Sending e-mails with links, attachments, and other requests.
- Physical – Physical impersonation or intrusion to access control areas or physical walk-through of office space to detect security deficiencies or violations.

Results of social engineering tests will be incorporated into the overall program and tracked.

| Title | Description | Audience | Frequency |
|---|---|---|---|
| General Security Awareness | Covers fundamental security principles, including password security, social engineering risks, safe browsing habits, and physical security measures. Ensures employees understand their role in protecting company data. | All Employees | Annually |
| GLBA Training | Focuses on the Gramm-Leach-Bliley Act (GLBA) compliance requirements, emphasizing data privacy, protection of student records, and responsibilities in safeguarding personal information. | All Employees with access to student records. | Annually |
| Phishing Exercises | Simulated phishing attacks designed to test employees' ability to recognize and report phishing attempts. Provides feedback and training based on results to improve cybersecurity awareness. | All Employees | Monthly |
| Payment Card Industry (PCI) Training | Educates employees handling payment card data on PCI-DSS compliance requirements, secure payment processing, and methods to prevent fraud and data breaches. | Employees handling Credit Cards, or "Cashiers" | Annually |
| Incident Response Tabletop | A simulated cybersecurity incident exercise where key personnel walk through response protocols to test the effectiveness of the organization's Incident Response (IR) and Business Continuity Plan (BCP). | Defined Roles in IR & BCP Plan | Annually |

**Non-Compliance**

The Executive Director of IT Client Support Services works in conjunction with Human Resources to ensure all employees complete their required training. If an employee fails to complete their security training the organization will take the following actions:

- Employees will be notified of their non-compliance, and their manager or supervisor will be notified. The employees' time to complete the training will be extended by 1 week.
- Failure to complete training after additional notification may lead to loss of access to the organization's systems and/or additional sanctions as deemed appropriate by Human Resources.

**Enforcement**
Any employees found to have violated this procedure may be subject to disciplinary action up to and including termination of employment.

## Website Address
Information Technology: http://it.mercer.edu

## History
Approved by Assistant VP of Information Technology and Chief Information Officer on April 2, 2025.
Revised June 5, 2025