

Auburn University at Montgomery

Policies and Procedures

Title: Information Security and Awareness Training

Responsible Office: Information Technology Services (ITS)

I. PURPOSE

Understanding the importance of computer security and individual responsibilities and accountability for computer security is paramount to achieving Auburn University at Montgomery's goals. This can be accomplished with a combination of general computer security awareness training and targeted, product-specific training.

The Information Security Awareness and Training policy identifies the steps necessary to provide employees of the University with awareness of IT system security and their responsibilities to protect University IT systems and data.

II. POLICY

The Information Security and Awareness Training program is mandatory for all University faculty, staff, and student workers, as well as contractors and vendors under the conditions described herein.

III. EFFECTIVE DATE

September 1, 2017

Revised: May 1, 2023

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, and student workers, as well as contractors and vendors who use University IT systems or data.

V. RESPONSIBILITY

Senior University leadership shall be responsible for ensuring compliance with this policy by employees under their supervision. Compliance by contractors and vendors shall be overseen by the contracting department.

Policy Responsible Office: Information Technology Services

Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). PCI DSS is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The standard was created to increase controls around cardholder data to reduce credit card fraud.

The **Health Insurance Portability and Accountability Act** of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

VII. PROCEDURES

A. All University Staff and Employees

Faculty, staff, student workers, contractors and vendors who use University IT systems as part of their regular duties must do the following:

1. Upon hire, complete the Security Awareness Training course within the first 30 days from date of hire.
2. Complete an annual online Security Awareness Training course every twelve (12) months
3. Additional Security Awareness Training may be required by all employees at other intervals when the IT infrastructure or environment changes and training is necessary.
4. Read and adhere to the Information Technology Appropriate Use Policy ensuring the employee is fully aware of security best practices and their associated roles in protecting the University's IT systems and data.

B. Supervisors, Managers, Deans and Directors

Supervisors, Managers, Deans and Directors must do the following:

1. Ensure each employee under their supervision has completed the Security Awareness Training course and should include completion of the training in the employee's annual performance evaluation.
2. Request from ITS that faculty, staff, student workers, contractors and vendors receive additional role-based information security training as deemed appropriate.

C. Additional Role-Based Security Awareness Training

Faculty, staff, student workers, contractors, and vendors who collect, maintain or have access to additional regulated or confidential information such as HIPAA or PCI-DSS credit card information on behalf of the University are subject to the following requirements:

1. Complete an annual online Security Awareness Training course every twelve (12) months to include relevant regulatory or compliance specific modules.
2. In addition, such contractors and vendors must submit a list of trained personnel to ITS including the individuals' names and dates the course was completed.

VIII. SANCTIONS

Violations of this policy or the protection standards created to implement this policy may result disciplinary sanctions, including ITS disabling University IT system access until the individual has completed the training.


IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Chancellor has the authority to interpret this policy.

APPROVAL TO PROCEED:



DATE:

4/12/23

APPENDICES

NONE