Auburn University at Montgomery
Policies and Procedures

Title: Information Security and Awareness Training

Responsible Office: Office of Technology

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, student workers and contracted personnel.

III. EFFECTIVE DATE

September 1, 2017

IV. APPLICABILITY

This policy applies to all departments, faculty, staff, student workers and contracted personnel who use University IT systems or data.

V. RESPONSIBILITY

Senior University leadership shall be responsible for ensuring compliance with this policy.

Policy Responsible Office: Office of Technology
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.

VII. PROCEDURES

The IT security roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles as long as the multiple roles assignments provide adequate separation of duties, provide adequate protection against the possible fraud, and do not lead to conflict of interest.

A. All University Staff and Employees

Faculty, staff, student workers and contracted personnel who use University IT systems as part of their regular duties are subject to the following requirements:

1. Complete the online Security Awareness Training course.
2. All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from date of hire.
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 are subject to the following requirements:

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

C. Employees Subject to Payment Card Industry (PCI)

Faculty, staff, student workers and contracted personnel who collect, maintain or have access to 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 PCI specific modules.
2. In addition, the Vendor providing contracted personnel will submit a list of trained personnel to ITS including the individuals' names and dates the course was completed.

VIII. SANCTIONS

Deliberate disregard of this policy or the protection standards created to implement this policy my result in ITS disabling University IT system access until the individual has completed the training.

IX. EXCLUSIONS

NONE

X. INTERPRETATION

The Office of Technology CIO has the authority to interpret this policy.

APPROVAL TO PROCEED: ______________ **DATE:** 8/11/17