Cybersecurity Awareness and Training Policy

Responsible Office: Office of the CIO

I. POLICY STATEMENT

All users are required to participate in the Auburn Cybersecurity Awareness and Training Program.

This includes mandatory new hire training as part of onboarding, annual cybersecurity training, and role based training based on regulatory or government requirements (HIPAA, PCI-DSS, GLBA, CMMC, etc.) as determined by the Chief Information Security Officer (CISO).

II. POLICY PRINCIPLES

This policy guides the establishment and operation of a cybersecurity awareness and training program throughout Auburn University to implement security best practices.

This policy defines the roles and responsibilities necessary for effective Auburn University information security awareness and training processes and procedures.

This policy guides the establishment of processes and procedures for implementing best practices with respect to the cybersecurity awareness and training program.

III. DEFINITIONS

Auburn University IT Unit: Any IT entity that is responsible for the management, operation, and security of Auburn University IT resources, to include systems, applications, IT infrastructure, and data. For Auburn University, this includes the Office of Information Technology (OIT) and associated Distributed Information Technology (DIT) units.

Awareness: A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure. Source: NIST SP 800-16

Awareness and Training Program: Explains proper rules of behavior for the use of agency information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed. (i.e., NSTISSD 501, NIST SP 800-50) Source: CNSSI No. 4009

Process: A specific procedural activity that is required and performed to achieve a capability level. Processes detail maturity of institutionalization of the practices. Source: CMMC

IV. GLOSSARY

CMMC: Cybersecurity Maturity Model Certification

CNSSI: Committee on National Security Systems Instruction

CUI: Controlled Unclassified Information

DIT: Distributed Information Technology

FERPA: Family Educational Rights and Privacy Act

FIPS: Federal Information Processing Standards

GLBA: Gramm-Leach-Bliley Act

HIPAA: Health Insurance Portability and Accountability Act

NIST: National Institute of Standards and Technology

OIT: Office of Information Technology

PII: Personally Identifiable Information

PCI-DSS: Payment Card Industry – Data Security Standards

SSP: System Security Plan

V. EFFECTIVE DATE

August 25, 2020

VI. APPLICABILITY

Applicable to all individuals who utilize Information Technology (IT) resources owned or operated, which includes information that is processed, transmitted, or stored, on behalf of Auburn University.

VII. POLICY MANAGEMENT

Responsible Office: Office of the Chief Information Officer
Responsible Executive: Chief Information Officer
Responsible Officer: Chief Information Security Officer

VIII. ROLES and RESPONSIBILITIES

The Chief Information Security Officer is responsible for:

1. Ensuring that appropriate information security awareness and training policies, plans, and procedures are developed, maintained, published, and disseminated to appropriate Auburn University personnel.
2. Ensuring that all affected Auburn University IT units develop, adopt, or adhere to formal, documented information security awareness and training procedures that addresses purpose, scope, roles, responsibilities, management, and coordination among organizational entities.

The **Cybersecurity Awareness and Training Program Leader** is responsible for:

1. Providing basic security and privacy awareness training to system users (including managers, senior executives, and contractors)
    a. As part of initial training for new users

b. When required by system changes; and
c. One year thereafter

2. Providing security awareness training on recognizing and reporting potential indicators of insider threats.

The **AU IT Unit** is responsible for:

1. Understanding their role and responsibilities related to protecting Auburn University's critical information systems and data.
2. Ensuring cybersecurity awareness and training policies and procedures are effectively communicated and understood by all constituent groups.
3. Coordinate, develop, adopt, deliver or adhere to formal, documented cybersecurity awareness and training procedures that addresses purpose, scope, roles, responsibilities, management, for specific areas within their area of responsibility such as HIPAA, GLBA, PCI-DSS, CMMC, etc.

Employees, Faculty, and Students are responsible for:

1. Understanding their role and responsibilities related to protecting Auburn University's critical information systems and data.
2. Completing all required cybersecurity awareness and training requirements on time.

IX. COMPLIANCE GUIDELINES

1. Cybersecurity Maturity Model Certification (CMMC), Department of Defense
2. DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
3. NIST Cybersecurity Framework (CSF), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
4. NIST Special Publication (SP) 800-171 Revision (Rev) 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, U.S. Department of Commerce National Institute of Standards and Technology (NIST)
5. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
6. Payment Card Industry Data Security Standard (PCI-DSS)

X. EXCLUSIONS

None.

XI. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.