Information Security Awareness Training Policy

I. Introduction

This policy was created to comply with the University System of Georgia's (USG) information technology policies, specifically USG Information Technology Handbook, 5.9.2.

In the event that any information contained within this policy conflicts with any Board of Regents (BOR) policy, the BOR policy controls.

II. Purpose

This purpose of this policy is to increase the awareness of the workforce through the implementation of an Information Security Awareness Training program. Albany State University (ASU) cannot protect the confidentiality, integrity and availability of information and information systems without ensuring that each person involved understands their roles and responsibilities. ASU will provide adequate training for all faculty and staff to perform their roles and responsibilities using the security awareness-training program. The human factor is critical to the success of protecting information assets.

The ASU Information Security Awareness Training Policy applies to all ASU faculty and staff that access information or ASU information Systems. Topics covered must include:

1) Cybersecurity policy and guidelines and the need for cybersecurity
2) Data governance and management as well as roles and responsibilities
3) Importance of personal cybersecurity
4) Threats to cybersecurity and incident reporting

I. Definitions

Definitions associated with this policy are available in the Information Technology and Data Security Glossary.

II. Policy

Awareness training shall be conducted annually, attendance shall be mandatory, completion shall be documented and shall provide practical and simple guidance pertaining to user roles and responsibilities. Additional role-based security training shall be provided to IT specialists, developers, security management and users having unique or specific cybersecurity responsibilities.

III. Exceptions

Exceptions to the ASU Information Security Awareness Training Policy, other than those previously discussed, are to be evaluated on a case-by-case basis by the Vice President and Chief Information Officer.

IV. Applicability

ASU Campus Community
ASU Faculty and Staff

V. Accountability

Failing to complete the Information Security Awareness Training in the time scheduled will result in Network and Information Systems access being removed until the user has completed the mandatory Information Security Awareness Training. ASU's CISO will provide evidence that all users accessing information or information systems are trained in their security responsibilities.

VI. Contacts

Albany State University Chief Information Officer
Albany State University Chief Information Security Officer

VII. References

USG BOR IT Handbook, http://www.usg.edu/information_technology_handbook
O.C.G.A. § 16-9-150 (2019), Georgia Security Act of 2005
NIST SP 800-16 IT Security Training Requirements
NIST SP 800-50 Building an IT Security Awareness and Training Program

Last Update

Aug 2019