Information Security Awareness Training Policy

Adopted by President’s Cabinet 8/24/21

I. Introduction

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

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

II. Purpose

This purpose of this policy is to increase information security / cybersecurity awareness amongst East Georgia State College’s (EGSC) employees through Information Security Awareness Training. EGSC cannot protect the confidentiality, integrity and availability of information and information systems without ensuring that each employee understands their roles and responsibilities as it relates to information security / cybersecurity. EGSC will provide biannual information security / cybersecurity training to all employees as a function of performing their respective roles and responsibilities. The human factor is critical to the success of protecting information assets.

The EGSC Information Security Awareness Training Policy applies to all EGSC employees who access EGSC / USG information systems. Topics covered in the training 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. Policy

Awareness training shall be conducted bi-annually. Participation by all EGSC employees is mandatory, and 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.

II. Exceptions

Exceptions to the EGSC Information Security Awareness Training Policy, other than those previously discussed, are to be evaluated on a case-by-case basis by EGSC’s Vice President of Information Technology and/or the Information Security Officer (ISO).
III. Applicability

All EGSC employees, including part-time employees and student workers.

IV. Accountability

Failure to complete the biannual Information Security Awareness Training in the time scheduled will result in the EGSC’s employee’s network and information systems access being removed until the employee has completed the training. EGSC’s ISO will provide evidence that all EGSC employees have completed the respective Information Security Awareness Training.

V. Contacts

East Georgia State College Vice President for Information Technology

East Georgia State College Information Security Officer

VI. References


NIST SP 800-16 IT Security Training Requirements

NIST SP 800-50 Building an IT Security Awareness and Training Program Last Update

Last Update

August 2021