Title:	**Cybersecurity Awareness Training Policy**
Status:	**Final, Effective Date: 2022-May-18**
Last Revised:	**2022-May-15, Reviewed 2022-May-15**
Policy Point of Contact:	**VP of Enrollment Management and Information Technology**
Synopsis:	South Georgia State College policy regarding Cybersecurity Awareness Training.

Policy Statement

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

Awareness training shall be conducted bi-annually. Participation by all SGSC employees is mandatory, and completion shall be documented and shall provide practical and simple guidance about user roles and responsibilities. Additional role-based security training may be provided to IT specialists, developers, security management and others users that have unique or specific cybersecurity responsibilities.

Standard

This purpose of this policy is to increase information security / cybersecurity awareness amongst South Georgia State College's (SGSC) employees through Cybersecurity Awareness Training. SGSC 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. SGSC 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 SGSC Cybersecurity Awareness Training Policy applies to all SGSC employees, including part-time employees and student workers; who access SGSC / USG information systems. Topics covered in the training include, but are not limited to:

- Cybersecurity policy and guidelines and the need for cybersecurity
- Data governance and management as well as roles and responsibilities
- Importance of personal cybersecurity
- Threats to cybersecurity and incident reporting

SGSC employees that fail to complete a scheduled Cybersecurity Awareness Training by an announced deadline will have their network and information systems access disabled until they complete the training.

SGSC's VP of Enrollment Management & Information Technology will provide evidence if requested, that SGSC employees have completed a respective Cybersecurity Awareness Training.