Title:	**Simulated Phishing Policy**
Status:	**Final, Effective Date: 2024-April-1**
Last Revised:	**2024-March-14, Reviewed 2024-March-28**
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.

The institution will conduct monthly simulated phishing campaigns with all employees to evaluate the current cybersecurity awareness culture and tailor education to meet the needs of the institution.

Standard

This purpose of this policy is to increase information security / cybersecurity awareness amongst South Georgia State College's (SGSC) employees through Simulated Phishing Campaigns. SGSC cannot protect the confidentiality, integrity and availability of information and information systems without ensuring each employee understands their roles and responsibilities related to information security / cybersecurity. SGSC will submit simulated phishing campaigns 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 Simulated Phishing Policy applies to all SGSC employees, including part-time employees and student workers, who access SGSC / USG information systems.

Employees who fail two or more simulated phishing campaigns in a six-month period will have their accounts placed into a review cybersecurity awareness training course. Employees have two weeks to complete the review course. Employees that fail to complete the review course within the allotted time will have their network and information systems access disabled until they complete the training.

Employees that fail four or more simulated phishing campaigns in a six-month period will receive an automatic written warning from their supervisor and Human Resources. Please see Appendix A - Disciplinary Process for Failed Phishing Outcomes. De-escalation will occur when six consecutive passes have taken place.

SGSC's VP of Enrollment Management & Information Technology will provide evidence, if requested, related to simulated phishing campaign failures.

Appendix A Disciplinary Process for Failed Phishing Outcomes

Failure Count	Resulting Level of Remediation Action
First Failure	No Action Required
Second Failure	Mandatory completion of Cyber Security Awareness Training Review and receive additional cybersecurity awareness information through email from the Vice President of Enrollment Management and Information Technology.
Third Failure	Mandatory completion of Cyber Security Awareness Training Review and face to face meeting with their supervisor and the Vice President of Enrollment Management and Information Technology.
Fourth Failure	Mandatory completion of Cyber Security Awareness Training Review, face to face meeting with their manager and Head of Human Resources and receive a written warning and the Vice President of Enrollment Management and Information Technology.
Fifth Failure	Mandatory completion of Cyber Security Awareness Training Review, face to face meeting with the Head of Human Resources and Vice President of Enrollment Management and Information Technology and receive a second written warning. - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events.
Sixth Failure	Mandatory completion of Cyber Security Awareness Training Review, face to face meeting with the Head of Human Resources and Vice President of Enrollment Management and Information Technology, and President and receive a third written warning. - Possibility that additional administrative and technical controls will be implemented to prevent further Failure events.
Seventh Failure	Potential for Termination of Employment or Employment Contract