GEORGIA
COLLEGE
GEORGIA'S PUBLIC LIBERAL ARTS UNIVERSITY

Georgia College & State University

Cybersecurity Awareness and Training Plan

Version 1.1

Author: Hance Patrick, Information Security Officer

August 2022

Revision & Sign-off Sheet

Change Record

Date	Author	Version	Change Reference
05/2022	Hance Patrick	1.0	Initial Document
08/2022	Hance Patrick	1.1	Fit into USG template

Reviewers

Name	Version Approved	Position	Date
Susan Kerr	1.1	CIO	08/2022

Distribution

Name	Location
Online	www.gcsu.edu/technology

Document Properties

Item	Details
Document Title	Cybersecurity Awareness and Training Plan
Document Type	Plan (Internal Use Only)
Author	Hance Patrick
Document Manager	Hance Patrick
Creation Date	05/2022
Last Updated	08/2022
Document Classification	Sensitive

Table of Contents

Executive Summary

Georgia College & State University (GCSU) is the State's only designated public liberal arts university; centrally located with one campus setting in Milledgeville, we have approximately 6,500 students, 1,000 full-time faculty and staff, and 4 colleges (College of Education, College of Business, College of Arts and Sciences, and College of Health Sciences). Securing campus information plays a key role in protecting the campus image while facilitating the campus mission and vision of providing an expansive educational experience, fostering highly intentional engagement, promoting diversity and inclusive excellence, and preparing students for leadership.

This document provides a framework for how Georgia College & State University (GCSU) educates and provides cybersecurity awareness training and information security training to all campus personnel.

Introduction

USG organizations cannot protect confidentiality, integrity, and availability of information, information systems, products, or services without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. Consequently, all organizations shall develop, document, and disseminate to all faculty and staff a cybersecurity awareness and training plan following Board Policy 10.4.2 *Institutional and Organizational-Level Responsibilities.*[1] This document provides a general framework to illustrate how GCSU implements modes of training, retains records, and provides reporting as required in the USG *IT Handbook (ITHB)*, Section 5.10 Required Reporting.

Purpose

Cybersecurity awareness and training is a University System of Georgia (USG) strategy, which is designed to help GCSU's information systems users understand the role they play in helping the USG mitigate cyber risks. This strategy is implemented through the process of formally educating the workforce on the various cyber threats that exist, how to recognize them, and what steps to take to keep themselves and GCSU secure.

Scope

The procedures for training and educating personnel on the changing cybersecurity threat landscape that we work within apply to all sectors of GCSU and all employees of the University.

Distribution

Distribution is recorded within the document's "Revision & Sign-Off" page. The Information Security Officer (ISO) shall be responsible for posting the plan on the GCSU technology website.

Continuance

This plan is a living document and may be modified at any time by the Chief Information Officer (CIO) or the Information Security Officer (ISO).

Authority

The administration of GCSU fully supports this plan. The Office of Information Security, within Information Technology, manages and administers this plan, which is currently in effect for all GCSU employees (student workers, faculty, staff, contractors, etc.). The Georgia Constitution grants the Board

[1] https://usg.edu/policymanual/

of Regents the exclusive right to govern, control, and manage the USG and all USG institutions. The Board exercises and fulfills its constitutional obligations, in part, by promulgating rules and policies for the governance of the USG and its constituent units. To accomplish this, Section 10.4 of the *Board of Regent Policy Manual* states, "Information created, collected, or distributed using technology by the University System Office (USO), all University System of Georgia (USG) institutions and the Georgia Public Library Service (GPLS) is an asset and must be protected from unauthorized disclosure, modification, and destruction. The degree of protection needed is determined by the nature of the resource and its intended use. The USO, all USG institutions, and the GPLS shall employ prudent cybersecurity policies, standards, and practices to minimize the risk to the confidentiality, integrity, availability, and privacy of data and information and shall create and maintain an internal cybersecurity program…. The USG chief information security officer shall maintain cybersecurity implementation guidelines that the USO, all USG institutions, and the GPLS shall follow in the development of their individualized cybersecurity plans."

Responsibilities

The Office of Information Security is responsible for the adherence to and use of this plan. Additionally, any changes to this plan are to be communicated with the Document Manager for inclusion or exclusion.

Chief Information Officer (CIO)

The Chief Information Officer and senior leadership are responsible for ensuring that appropriate and auditable cybersecurity controls are in place to include awareness, training, and education as stated within *Board of Regents Policy 10.4*.

Information Security Officer (ISO)

The Information Security Officer shall provide leadership in cybersecurity awareness, training, and education as well as work with the academic, administrative, and information technology leadership to:

1. Establish an overall strategy for cybersecurity awareness, training, and education.
2. Review and make updates to the current cybersecurity awareness and training plan annually.
3. Ensure consistency with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
4. Identify who within the organization has the data privacy role and coordinate the implementation of cybersecurity data privacy support responsibilities.

Users (all faculty, staff, student workers, and contractors)

Users are the largest audience and most important group to help reduce unintentional errors and vulnerabilities. Users requiring access to information and information systems, products or services must:

1. Understand and comply with USG organization's cybersecurity policies and procedures.
2. Participate fully in the training plan and modes of training identified below.

Modes of Training

Awareness Training

Cybersecurity awareness training for all employees who use GCSU systems, products, or services (including managers, senior executives, and contractors) is mandatory. The training coordinator shall:

1. Provide training as required by the *Human Resources Administrative Practice Manual,* Employment Orientation[2].
2. Provide training as part of initial training for new employees, contractors, etc.
3. Schedule biannually thereafter following the ITHB, Section 5.10 Required Reporting Calendar.
4. Deliver USG provided baseline training module with the option to augment with additional modules.
5. Incorporate lessons learned from internal or external incidents or breaches.

Role-Based Training

The Office of Information Security shall provide role-based cybersecurity training for personnel. The training coordinator shall include:

1. Compliance-based training for information system users that access protected information (e.g., FERPA, PCI-DSS, HIPAA, GLBA).
2. Establish the frequency and availability of the training.
3. Incorporate lessons learned from internal or external incidents or breaches.

Phish-Based Testing

The Office of Information Security will perform phish-based testing for all employees (including managers, senior executives, and contractors) and shall:

1. Provide phish and fraud testing campaigns monthly to evaluate the effectiveness of the training.
2. Deploy the Phish Alert Button in Outlook.
3. Incorporate lessons learned from internal or external incidents or breaches.
4. Enroll users in a more frequent fraud and phish campaign to further reinforce the lessons provided in the training when that user clicks on a phish-based test.
5. Enroll users in a mandatory phish and fraud identification program when that user clicks on two (or more) phish-based tests.

Departmental Information Security Plans

Each department at GCSU has designated a Data Security Coordinator to implement, supervise, and maintain the Departmental Information Security Plan (ISP). This designated employee will serve as the Data Security Coordinator with responsibilities to:

1. Implement the ISP, including all provisions outlined in Section VII: Daily Operational Protocol.

[2] https://usg.edu/hr/manual/

2. Provide the ISP to all departmental employees on an annual basis and provide training as needed. Each employee will sign that they have received the ISP and understand it.
3. Submit the signed ISP to the ISO once all employees have signed.

Training Record Management

For all information systems users, including managers, senior executives, and contractors, the Office of Information Security shall:

1. Document and monitor cybersecurity training activities, including cybersecurity awareness training and specific role-based training.
2. Retain individual training records for five years following the *Records Retentions Schedule* Number: 0472-04-017.

Required Reporting

The Office of Information Security shall provide GCSU's training results and reports to USG Cybersecurity upon request. Training feedback shall include awareness training, role-based training, and phish testing results. All documentation will be stored on GCSU's Secure Institution Folder at the USG Cybersecurity SharePoint site (credentials required). Questions should be submitted to USG Cybersecurity through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697.