Policy Approval/Review Form

This form is used for the approval, amendment, removal or review of a Gordon State College policy. Once authorized with the President's Signature, the policy will be posted to the Gordon State Website. This approval form will be filed in the Office of the President with Cabinet minutes noting approval.

Policy Title *	Information Security Awareness and Training Policy
Department/Organization	Information Technology
Policy Editor	Doug Stewart
Request Type	New ☐ Amended/Edited ☑ Removed ☐ Reviewed Only ☐

OBJECTIVE (Briefly state your purpose.)

This Information Security Awareness and Training Policy is maintained to comply with:
University System of Georgia (USG) Board of Regents (BOR) Policy 11.3 & USG Information Technology (IT) Handbook, Section 5.9: Security Awareness, Training, andEducation

RESOURCES AND CONSULTATION (Briefly describe the resources (i.e. website, link) used in developing, amending, removing, or reviewing the policy. Include names of other individuals who assisted with this change.)

https://www.usg.edu/policymanual/section11/C430

https://www.usg.edu/assets/information_technology_services/documents/IT_Handbook.pdf#page=84

COMMUNICATION PLAN (Identify how information about how the policy will be communicated to the college as well as training plans if applicable.)

Policy will be added to the Gordon State website under the IT Poliies and Guidelines section of the Information Technology Department.

Authorizations

Chair/Dean/or Supervisor Signature and Date: Douglas Stewart Digitally signed by Douglas Stewart Date: 2023.05.11 15:57:54 -04'00'

Cabinet Sponsor (VP) Signature and Date: Lee Fruitticher Digitally signed by Lee Fruitticher Date: 2023.05.15 08:50:59 -04'00'

President Signature and Date: Kirk A. Nooks Digitally signed by Kirk A. Nooks Date: 2023.05.18 14:17:09 -04'00'

***Policy Template mustbe submitted with this form.**

GORDON STATE COLLEGE
INFORMATION TECHNOLOGY

Information Security Awareness and Training Policy

Document ID:
Policy type: Administrative
Effective date: 2018-04-20
Last revised: 2023-04-20
External requirement for review:
Compliance reporting:
Policy owner: Gordon State College (GSC) Information Technology Department
Policy contact: Douglas Stewart, douglass@gordonstate.edu

1 Reason for Policy

This Information Security Awareness and Training Policy is maintained to comply with:

- **University System of Georgia (USG) Board of Regents (BOR) Policy 11.3 Information Security Policy**: *all USG institutions…shall create and maintain an internal information security technology infrastructure consisting of an information security organization and program that ensures the confidentiality, availability, and integrity of all USG information assets.*
- **USG Information Technology (IT) Handbook, Section 5.9: Security Awareness, Training, and Education**

2 Policy Statement

This Information Security Awareness and Training Policy establishes Gordon State College's program to promote awareness of, and provide training for, security of institutional information assets. The policy defines the roles and responsibilities for security awareness and training, and the supporting policies, processes, plans, procedures, and standards that must be followed.

Essential characteristics of GSC's information security training and awareness program are:

- The program is focused on the institution's *entire* user population.
- All users must be appropriately trained in how to fulfill their security responsibilities *before* being allowed to access their authorized systems. User training must be periodically refreshed for their *continued* access to systems.
- The program is considered *the* vehicle for disseminating information that employees need to do their jobs, *the* vehicle for informing users in general of proper rules of behavior for the use of information systems and information, and *the* vehicle for communicating security policies and procedures that need to be followed.

- Learning about information security is a *continuum*: for all users it starts with awareness, then builds to training; for security specialists it evolves into education and may culminate in certification.
- The program has a *life cycle*:
    - Program design: needs are assessed, a strategy and plan are developed, approved, and funded.
    - Training material development: focused on the security behavior to reinforce, and the skills to be learned and applied.
    - Implementation: communication and roll-out, delivery.
    - Post-implementation: keeping the program current, monitoring its effectiveness.

3 Scope

All Gordon State College IT resource users, and all Gordon State College IT resources, are covered by this policy.

4 Plans

This policy is implemented in an associated plan.

Subject	**Plan**
Information Security Awareness and Training	Information Security Awareness and Training Plan

5 Responsibilities

This section establishes the roles and responsibilities necessary to manage GSC's Information Security Awareness and Training program.

5.1 President

The GSC President is responsible for ensuring that appropriate and auditable information security controls are in place to include awareness, training, and education. [IT Handbook Section 5.9.1]

5.2 Information Security Officer (ISO)

The ISO shall provide leadership in security awareness, training and education as well as work with the academic, administrative and information technology leadership to:

1. Establish overall strategy for security awareness, training, and education.
2. Understand program maturity and compliance.
3. Provide evidence that all users accessing information or information systems are trained in their security responsibilities.

[IT Handbook Section 5.9.1]

The ISO shall ensure that the security awareness and training program includes:

- Maintenance of an annual information security awareness and training component for all employees and contractors, as specified in Section 5.9 of the USG IT Handbook. [IT Handbook Section 5.1.1]

- The objective of increasing user awareness of information security issues and responsibilities. [IT Handbook Section 5.2.1]
- Training that covers:
    - Information security policy and guidelines and the need for cybersecurity
    - Data governance and management as well as roles and responsibilities
    - Importance of personal information security
    - Threats to cybersecurity and incident reporting

  [IT Handbook Section 5.9.2]
- Training that is conducted annually, with mandatory attendance, with completion that is documented, and that provides practical and simple guidance pertaining to user roles and responsibilities. [IT Handbook Section 5.9.2]
- Additional role-based security training for IT specialists, developers, security management and users having unique or specific information security responsibilities. [IT Handbook Section 5.9.2]
- Training that is completed annually by each employee and individuals who through formal, informal, contract, or other types of agreements interact with USG organizational information and information systems. [IT Handbook Section 5.10.2]
- Learning objectives that users, contractors, and third parties having access to state or USG computerized information resources are informed of, and abide by, the USG IT/IS Risk Management Standard and the GSC information security plan, and are informed of applicable local, state, and federal policies, laws, regulations, and/or codes related to computerized information resources. [IT Handbook Section 5.5.1]

5.3 Users

Users requiring access to information and information systems must:

1. Understand and comply with USG organizational security policies and procedures.
2. Be appropriately trained in the acceptable use of the systems and applications to which they have access.
3. Work with management to meet training needs.
4. Be aware of actions to better protect USG organizational information and information systems.

[IT Handbook Section 5.9.1]

6 Enforcement

The GSC Information Technology and Information Security Governance Committee is responsible for the enforcement of this policy. Any employee found to have violated this policy may be subject to suspension of all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.

7 Related Information

Resource	Link
USG ITS IT Handbook	http://www.usg.edu/information_technology_services/it_handbook/
NIST Special Publication 800-50, Building An Information	https://csrc.nist.gov/publications/detail/sp/800-50/final

Technology Security Awareness and Training Program	

8 Policy History

Revision date	Author	Description
2018-04-20	Kelly Carter	Initial version
2023-04-20	Douglas Stewart	Updated links to external sources and reveiwed content