

| | | | | | |
|---|---|-------------|-----|------|---|
|  |  | Last | N/A | Area | Information Technology/ Management (Procedures) |
| | | Approved | | | |
| | | Effective | N/A | | |
| | | Next Review | N/A | | |
| Chief Or Responsible Office | | | | | Information Technology Services |

Cybersecurity Awareness Training

Authority for Procedure granted by UWG [Policy #5002, Data Security](#).

This procedure defines the process for developing and delivering cybersecurity training as required by the Board of Regents (BOR) and the University System of Georgia (USG) Information Technology (IT) Handbook. This procedure is aligned with and supports the [USG Business Procedures Manual \(BPM\)](#), Sections 12.4, 12.5.2, and the [USG IT Handbook](#), Section 5.9 Cybersecurity Awareness, Training and Education.

A. Cybersecurity Training Content Review Process

The semi-annual cybersecurity training content may be provided by the [USG Office of Cybersecurity](#). The UWG Information Security Officer is responsible for reviewing any USG provided content to ensure it meets both the USG Office of Cybersecurity and institutional requirements. This review is conducted in late summer to prepare for training delivery each fall and spring.

B. Cybersecurity Training Requirements

Cybersecurity training is mandatory for all UWG employees. This includes:

- **Initial Training:** Delivered during the onboarding process by the Office of Human Resources (OHR) for all new employees.
- **Refresher Training:** Required for all employees and conducted semi-annually by Information Technology Services (ITS) each October and April.

Note: All mandatory training shall comply with Board of Regents (BOR) [Policy 8.2.5, Employee Orientation and Training](#).

1. Role-Based Cybersecurity Training

In addition to general cybersecurity training, role-based cybersecurity training shall be delivered to information technology professionals and other employees who are responsible for or have access to Personally Identifiable Information and/or data that is governed by specific rules and regulations such as Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA), or Family Educational Rights and Privacy Act (FERPA). All University department heads are expected to identify and document that their staff complete any required cybersecurity training.

C. Compliance

All actively employed individuals (i.e., faculty, staff, and students) are required, as a condition of employment, to complete all mandated USG and institutional training, including cybersecurity and ethics training, both during onboarding and on an ongoing basis within the designated time frame. (See [USG Human Resources Administrative Practice Manual \(HRAP\)](#), General Criteria for Employment and Mandatory Employee Training)

Failure to complete mandatory cybersecurity training may result in the suspension of computer and/or network access. Additionally, failure to complete required training, such as USG Ethics Certification or other compliance training, may result in disciplinary action, up to and including termination of employment.

All disciplinary measures will be executed in accordance with UWG's established procedures and applicable laws.

Definitions

Personally Identifiable Information (PII) - for the purposes of these procedures, Personally Identifiable Information shall have the same meaning as 20 U.S.C. 1232g(b)(4)(A), which includes the Student's name, the name(s) of the Student's parent(s), the permanent address of the Student or their parent(s), Social Security Number, or other information that may allow a reasonable person to identify the Student with reasonable certainty.

Guidelines/Related material

Policy, Procedure, and Handbooks

- Board of Regents (BOR) Policy Manual, [Policy 8.2.5, Employee Orientation and Training](#)
- Board of Regents (BOR) Policy Manual, [Policy 10.4.2, Institutional- and Organizational-Level Responsibilities](#)
- [University System of Georgia \(USG\) Business Procedures Manual \(BPM\)](#)
 - 12.4 Cybersecurity
 - 12.5 Compliance
- [USG Information Technology \(IT\) Handbook](#), Section 5.9 Cybersecurity Awareness, Training

and Education

- [USG Human Resources Administrative Practice Manual \(HRAP\)](#), General Criteria for Employment and Mandatory Employee Training

Webpages

- [USG Office of Cybersecurity webpage](#)
- [USG Mandatory Trainings webpage](#)

Approval Signatures

Step Description

Approver

Date