UNIVERSITY of West Georgia.

UWG PROCEDURE NUMBER: 8.2.3, Cybersecurity Awareness Training
Authority: UWG POLICY: 8.2, Data Security

The Chief Information Officer, pursuant to the authority of University of West Georgia (UWG) Policy 8.2, establishes the following procedures on Cybersecurity Awareness Training:

A. Definitions

1. **Personally Identifiable Information** - 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 his/her parent(s), Social Security Number, or other information that may allow a reasonable person to identify the Student with reasonable certainty.

B. Cybersecurity Training

This procedure defines the process for developing and delivering the cybersecurity training as required by the Board of Regents and the USG IT Handbook. This Procedure works in conjunction with the UWG Human Resources Procedure 6.1.5 Training and Compliance, the University System of Georgia (USG) Business Procedures Manual Section 12.5.2, and the USG IT Handbook Section 5.9.2.

Cybersecurity training is required for all new employees and semi-annual refresher training is required for all existing employees. Initial cybersecurity awareness training is delivered as a part of UWG's new employee on-boarding process administered by Human Resources. The semi-annual cybersecurity awareness refresher training is delivered by the Center for Business Excellence as a component of the annual mandatory refresher training in October and then again in April.

The content of the semi-annual cybersecurity training may be provided by the USG Office of Cybersecurity. The UWG Information Security Officer will review any USG provided content to ensure the semi-annual training meets the requirements established by the USG Office of Cybersecurity as well as any UWG requirements. Course content review occurs in late summer for delivery in fall and spring.
Failure to complete the BOR/USG required cybersecurity training may result in the suspension of network and computer access.

**Role Based Cybersecurity Training**

Additional 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 PCI, GLBA, or FERPA. All University department heads are expected to identify and document that their staff complete any required cybersecurity training.

*Issued by the Chief Information Officer, the 7th day of November, 2019.*

Signature, Chief Information Officer

Reviewed by President:

*Previous versions*
- UWG Procedure 8.2.3 Information Security Awareness Training, July 23rd, 2019
- 2016 Security Awareness Training, 2016