UNIVERSITY of West Georgia.

UWG PROCEDURE NUMBER: 8.2.3, Information Security 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 Information Security 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. Annual Information Security Training

This procedure defines the process for developing and delivering the annual information security training as required by the Board of Regents (BOR) and the University System of Georgia (USG) Information Technology (IT) Handbook. This Procedure works in conjunction with the Human Resources *Procedure 6.1.5 Training and Compliance*, the USG Business Procedures Manual Section 12.5.1, and the USG IT Handbook Section 5.9.

Information security training is required for all new employees and an annual refresher is required for all existing employees. Initial security awareness training is delivered as a part of UWG's new employee on-boarding process administered by Human Resources. The annual information security awareness refresher training is delivered by the Center for Business Excellence as a component of the annual mandatory refresher training.

Content for the information security training will be developed by the Information Security Officer. Content is based on the topics required by the USG IT Handbook. A review of security related incidents or security questions received over the prior year also informs the course content. Content review occurs in late summer for delivery in fall.

Failure to complete the BOR/USG required information security training may result in the suspension of network and computer access.

Role Based Information Security Training

Additional role-based information security 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 (PCI), 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 information security training.

Issued by the Chief Information Officer, the 23 ***day of*** July ***, 2019.***

Signature, ***Chief Information Officer***

Reviewed by President:

Previous versions:
-2016 Security Awareness Training, 2016