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

A. Purpose
The purpose of this policy is to establish the procedures necessary to ensure that access to information systems is:

1. approved by the appropriate Data steward and/or Authorized Approver based on the defined roles and responsibilities of the end user,
2. only approved after the requester/end user receives proper training (for example, FERPA, GLBA, HIPAA), and
3. accounts with information system access are reviewed twice a year and revoked by the Data Steward and/or Authorized Approver when access is no longer appropriate due to resignation, termination, or change in role.

This procedure shall apply to all data stewards, authorized approvers, supervisors and end users of UWG information systems.

B. Definitions

1. Authorized Approver - An individual that has been given the technical ability to grant, change, or revoke access rights to an information system based on direction from the Data Steward.
2. Data Steward – the individual identified by the data trustee as responsible for the data read, created, collected, reported, updated or deleted and the technology used to do so, in their data areas. See BPM Section 12.2.1 for complete roles and responsibilities.
3. Confidential Information - is information maintained by a USG organization that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. As such, it is considered “need to know” information.
4. Family Educational Rights and Privacy Act (FERPA) - is a federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.
5. Gramm-Leach-Bliley Act (GLBA) - Governs the treatment of nonpublic personal information about consumers by financial institutions.
6. Health Insurance Portability and Accountability Act (HIPAA) - U.S. law designed to provide privacy standards to protect medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
7. Information System - is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Federal
8. **Information Technology** - Any computer, telephone, messaging system, e.g., voicemail, e-mail, etc., electronic media, computer application, protocol, or other equipment utilized on a public or private internetwork.

9. **Protected Health Information (PHI)** - any information (under U.S. law) about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

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

11. **Principle of Least Privilege (PoLP)** - describes the minimal user profile or access privileges to information resources based on allowing access to only what is necessary for the end user to successfully perform their job requirements. (Source: SP 800-179)

12. **Role-Based Access** - A type of system access which fulfills the **Principle of Least Privilege**. Under role-based access a user is assigned access through a system role. This role must be designed based on a specific job function and must be given no more privileges than are reasonably necessary to fulfill the user's job responsibilities. Ensuring least privilege requires defining a category or categories of information required to fulfill the role, determining the reasonable and appropriate minimum set of privileges required to access the electronic PHI commensurate to the defined role, and implementing reasonable and appropriate methods to restrict the user to the defined category or categories of information.

13. **User/End User** - Any person who is authorized to use and/or otherwise access UWG information systems, to include those information systems containing data covered by PHI, FERPA, GLBA or other regulations. *End users* include, but is not limited to, faculty, staff, students, volunteers, trainees, independent contractors, vendors, physicians, other clinical personnel, or and business partners.

C. **Procedure**

Login-based access to all UWG information systems must be carefully controlled in order to protect confidential and sensitive information. The following minimum requirements must be met before access is granted:

1. End user access to an information system must be requested by the immediate supervisor and submitted to the appropriate data steward for approval.

2. Data stewards and/Authorized Approver will approve or deny end user access based on the roles and responsibilities of the end user, as outlined in the request from the supervisor.

3. End users must submit evidence of completing any required training before access is granted by the data steward. This includes training required to meet regulatory compliance, or compliance statute governing the data that the end user may access, as well as general training on how to protect, share and manage the data contained in the information system.
The **Authorized Approver** will ensure that all *end users* are assigned a unique username that can be used to uniquely identify and track end user activity in the *information system*.

5 The **Data Steward** and/or **Authorized Approver** will ensure end user access is granted using the principle of least privilege.

6 The **Data Steward** and/or **Authorized Approver** will ensure that *end user* access is reviewed and confirmed by the supervisor twice per calendar year.

7 The **Authorizer Approver** will ensure *end user* access is be revoked within 5 days of termination from the University.

8 The **Authorizer Approver** will ensure *end user* access is adjusted or revoked within 30 days of a change of position or job duties.

*Issued by the Chief Information Officer, the __ day of __, 2020.*

Signature, Chief Information Officer

Reviewed by President: Stuart Rayfield

*Previous version: N/A*