Status **Draft** PolicyStat ID **18565063**

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

Data Access Control

Authority for Procedure granted by UWG Policy #5002, Data Security.

~~A. Purpose~~

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

The purpose is established to ensure that access to University of West Georgia (UWG) Information Technology and/or Systems are:

1. **Authorized by the Appropriate Personnel:** Access must be approved by the ~~appropriate~~designated Data ~~steward~~Steward and/or Authorized Approver, based on the defined roles and responsibilities of the ~~end user~~End User,
2. ~~only approved after the requester/end user receives proper training (for example, FERPA, GLBA, HIPAA), and~~**Contingent Upon Completion of Required Training:** Access is granted only after the requester/End User has completed necessary training programs (e.g., FERPA, GLBA, HIPAA, Cybersecurity) pertinent to their role and the data they will access, and
3. ~~accounts~~**Subject to Regular Review and Revocation:** Accounts with ~~information system~~ access to Information Technology and/or Systems are reviewed ~~twice a year and~~biannually. Access is revoked by the Data Steward and/or Authorized Approver when ~~access~~it is no longer appropriate due to changes in the User's role (e.g., resignation, termination, ~~or change in role~~etc.).

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

~~B. Procedure~~

This procedure applies to all Data Stewards, Authorized Approvers, supervisors, and End Users of UWG

Information Technology and/or Systems.

C. Access Control Requirements for Information Technology/Systems

Login-based access to ~~all~~ UWG ~~information systems~~Information Technology and/or Systems must be ~~carefully~~strictly controlled ~~in order~~ to protect ~~confidential and sensitive information~~Confidential, Personally Identifiable Information (PII), and/or Sensitive data. 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.~~

~~4. 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.~~

1. **Access Request Initiation:** The End User's immediate supervisor shall initiate the access request and submit it to the appropriate Data Steward for approval.
2. **Approval Based on Role:** The Data Steward and/or Authorized Approver shall review the request and approve or deny access based on the End User's roles and responsibilities as outlined by the supervisor.
3. **Mandatory Training Requirements:** End Users are required, as a condition of continued employment and to maintain data access privileges, to complete all mandatory and any additional training prescribed by UWG.

   Before access is granted, End Users shall provide documentation confirming the completion of all mandatory and any additional training. This includes:

   i. Mandatory compliance training (e.g., FERPA, GLBA, HIPAA, Cybersecurity)

   ii. Training specific to protecting, managing, and sharing the data within the system

iii. Any additional training mandated by applicable laws or policies

4. **Unique User Identification:** The Authorized Approver shall ensure each End User is assigned a unique username for accountability and activity tracking within the system.
5. **Principle of Least Privilege (PoLP):** The Data Steward and/or Authorized Approver shall ensure Role-Based Access is limited to the minimum necessary privileges required to perform the User's job duties.
6. **Biannual Access Review:** Supervisors shall review and confirm End User access biannually to ensure it remains appropriate.
7. **Termination of Access:** Authorized Approver shall revoke End User access within five days of the User's separation from the University.
8. **Change in Role:** Authorized Approver shall update or revoke access within 30 days of any change in the End User's job duties or position.

D. Non-Compliance

Non-compliance with the above procedure by may result in disciplinary actions, including but not limited to:

- Formal warnings or reprimands
- Suspension of data access to privileges and services
- Termination of employment or other contractual relationships

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

Definitions

Authorized Approver - ~~An~~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.

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.

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.

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.

Gramm-Leach-~~8/iley~~Bliley Act (GLBA) - Governs the treatment of nonpublic personal information about consumers by financial institutions.

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.

Information System - is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Federal Information Processing Standards ~~Ff PS~~FIPS 199&200; SP 800-18; SP 800-37; SP 800-53A; SP 800-60 and 44 U.S.C Section 3502.)

Information Technology - ~~Any~~any computer, telephone, messaging system, e.g., voicemail, e-mail, ~~etc.~~cloud and AI platforms, electronic media, computer application, protocol, or other equipment utilized on a public or private internetwork.

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.

Personally ~~Identified~~Identifiable Information (~~PI~~/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.

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)

Role-Based Access - ~~A~~a type of system access which fulfills the Principle of Least Privilege. Under rolebased 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.

User/End User - ~~Any~~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.

Approval Signatures

Step Description	Approver	Date