Status **Draft** PolicyStat ID **18566946**

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

Data Storage and Use

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

This procedure defines the requirements for handling and securing Confidential, Personally Identifiable Information (PII), and/or Sensitive data at the University of West Georgia (UWG). It serves as an outline to safeguard such information and to ensure compliance with applicable federal and state laws, as well as policies and best practices established by the University System of Georgia (USG) including the USG Business Procedures Manual and the USG Information Technology (IT) Handbook.

A. Scope

All UWG employees and contractors authorized to access University data and information assets are responsibility for protecting these resources from unauthorized access, modification, disclosure, destruction, or transmission. Individuals are expected to be familiar with and adhere to UWG and USG security policies and procedures.

B. Security Expectations

To maintain the highest level of data security, the University strongly encourages the use of UWG-issued equipment when accessing or storing Confidential, PII, and/or Sensitive information.

C. Roles and Responsibilities

- **Data Trustees and Data Stewards:** Oversee the management of the data that is read, used, created, collected, reported, updated, or deleted at UWG.
- **Data Users:** Access and utilize data solely for tasks related to their institutional responsibilities.
- **Data Users** will adhere to all UWG and USG policies and procedures.

D. Permitted Use and Access

- Only **Data Users or Affiliates** authorized by the relevant Data Steward(s) may access Confidential and/or Sensitive data.
- **Data Users** must use only use Confidential and/or Sensitive data exclusively for duties authorized by UWG and refrain from any unauthorized use, disclosure, or publication.
- Transferring Confidential, and/or Sensitive information to unauthorized individuals by any method is strictly prohibited.

E. Data Transmission

- **Data Users** must ensure that adequate security measures are in place at each destination when Confidential and/or Sensitive data is transferred from one location (physically or electronically) to another.
- Never send Confidential data via unsecured methods.
- Ensure Confidential information is encrypted during transmission and at rest, consistent with the **USG IT Handbook 5.8 End Point Management** and applicable federal, state, and applicable regulations.

F. Data Storage

- **Data Users** are prohibited from storing Confidential and/or Sensitive information in non-UWG approved cloud locations.
- Confidential and/or Sensitive data should be stored within designated systems. If external storage is necessary, use only University-owned network storage locations (e.g., UWG Domain Network Shared Drives) or University-approved cloud storage services (e.g., UWG-approved Microsoft OneDrive, or SharePoint Drive).
- Storing such data on local devices (e.g., desktops, laptops, removable media) is prohibited unless the device is University-owned and encrypted.

General use of **Microsoft OneDrive and SharePoint** (personal or shared drives) is **not authorized** for storing Confidential and/or Sensitive information. However, if necessary, a request may be submitted to Information Technology Services (ITS) for a '**Secured Microsoft OneDrive and SharePoint Drive**.' When approved, ITS can configure the drive to allow for the storage of Confidential and/or Sensitive information. Use of a secured Microsoft OneDrive or SharePoint Drive does not eliminate any of the other responsibilities or requirements outlined in this procedure

G. Data Disposal and Off-Campus Use

- Dispose of Confidential, PII, and/or Sensitive data in a manner that ensures permanent destruction, following UWG PL #1008 Records Information Management and associated procedures.
- **Do not** take Confidential, PII, and/or Sensitive information off-campus unless authorized and

appropriate security measures, such as encryption or other approved security precautions, are in place.

H. Third-Party Data Sharing

Before sharing Confidential and/or Sensitive information with non-UWG third parties (e.g., vendors, contractors, consultants), a signed Data Sharing Agreement is required.

Refer to UWG PL #1007 Contract Administration and associated procedure. Follow the contract routing and submission instructions on the Contract Management webpage.

I. Physical and Digital Security Measures

- Secure all information, regardless of format, to prevent unauthorized access. This includes using locking file cabinets, file encryption, and logging out of systems when not in use.
- Label all media containing Confidential and/or Sensitive information or Personally Identifiable Information (PII) appropriately.

J. Compliance

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

- Formal warnings or reprimands
- Suspension of access to university-provided devices and services
- Termination of employment or other contractual relationships
- Referral to legal authorities for potential civil or criminal proceedings

All disciplinary measures will be executed in accordance with UWG's established procedures and applicable laws.
(Refer to the UWG Employee Handbook)

Definitions

Confidential - information maintained by the institution that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

Data Steward - individuals designated by data trustees as responsible for the data processed (i.e., read, used, created, collected, reported, updated or deleted) within their functional area(s) and including the technology used to perform these actions, if applicable.

Data Trustee - executives of the organization who have overall responsibility for the data processed (i.e., read, created, collected, reported, updated or deleted) by their functional areas/units reporting to them. These individuals are normally cabinet-level positions reporting directly to the Data Owner (i.e., University President).

Data User - any faculty or staff, authorized by the appropriate institutional authority, to access enterprise data or data related to their institutions. This authorization should be for specific usages and purposes, and designed solely for conducting institutional business.

Personally Identifiable Information (PII) - any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the institution. Some PII is not sensitive, such as the PII on a business card, while other PII is considered Sensitive Personally Identifiable Information (Sensitive PII), as defined below.

Sensitive - information maintained by the institution that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss or deletion. Sensitive information may be public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness.

- **Sensitive Personally Identifiable Information (Sensitive PII)** - personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as a Social Security number or alien number (A-number). Sensitive PII requires stricter handling guidelines because of the increased risk to the individual if compromised.

UWG Domain Network Shared Drives - network storage locations that are maintained by UWG and assigned to individuals based on user type (student, employee, vendor, etc.), department, or role. These drives are normally mapped letter drives (e.g. Y:, W:, Z:, etc.) on Windows-based computers or mounted drives on Mac OS computers and require authorized UWG VPN access to reach when off-campus.

Guidelines/Related material

- USG Business Procedures Manual (BPM), Section 12.0 Data Governance and Management
- USG Information Technology (IT) Handbook, Section 5.8, End Point Management
- UWG PL #1007 Contract Administration and associated procedure
  Follow the contract routing and submission instructions on the Contract Management webpage
- UWG PL #1008 Records Information Management and associated procedure
  See the Records Information Management webpage for the USG Records Retention Schedules and Certificate of Records Destruction Form
- UWG Employee Handbook

Approval Signatures

Step Description	Approver	Date