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

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

Data Storage and Use

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

~~A. Procedure~~

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

B. Scope

All UWG employees and contractors ~~granted authorization~~authorized to access ~~the~~ University~~'s~~ data and information assets ~~have a~~are responsibility ~~to protect those assets~~for protecting these resources from unauthorized access, modification, disclosure, destruction, ~~disclosure, modification~~ or transmission~~; and.~~ Individuals are expected to be familiar with and ~~comply with~~adhere to UWG and USG security policies and procedures ~~for protection and security of records. The University strongly encourages the use of UWG equipment when accessing and storing Confidential and/or Sensitive data.~~

1. ~~Data Trustees and Data Stewards are responsible for the data being read, used, created, collected, reported, updated, or deleted at UWG. Data Users have specific usages and purposes for data and should only use data as part of their responsibilities for conducting institutional business.~~
2. ~~The Data User will adhere to all current UWG and USG policies and procedures.~~
3. ~~Only employees who have authorization from the relevant Data Steward(s) may have access to~~

Confidential and/or Sensitive data.

4. The Data User will only use Confidential and/or Sensitive data to support the duties authorized by UWG for the Data User to perform.
5. Data Users will not use, disclose, or publish Confidential and/or Sensitive data other than approved official University business.
6. Neither Confidential nor Sensitive information may be transferred by any method to persons not authorized to access or receive such information.
7. 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.
8. Data Users are not authorized to store Confidential and/or Sensitive information in non-UWG approved cloud locations (e.g., DropBox, Box, etc.).
9. Storage of Confidential and/or Sensitive data should remain in the system designated to store the data. If necessary to store Confidential and/or Sensitive data outside of the designated system, the data should be stored on University-owned network storage locations (e.g., UWG Domain Network Shared Drives) or University approved cloud storage locations (e.g., UWG Approved Secured Google Drive). Confidential and/or Sensitive information should not be stored locally on UWG endpoint devices, including desktop computers, laptops, removable media, etc., that is not encrypted.
10. Data Users should never send Confidential data via email, chat, or any other non-secure method of communication.
11. Confidential information must be encrypted while in transit and at rest, consistent with the USG IT Handbook 5.11 and Georgia Law.
12. Confidential and/or Sensitive data must be disposed of in a way that renders the information permanently destroyed. (see UWG PL #1008 Records Information Management and associated procedures)
13. Confidential and/or Sensitive information must not be taken off-campus unless the Data User is authorized to do so and only if the data is encrypted or other approved security precautions have been applied.
14. Sharing Confidential and/or Sensitive information with a non-UWG third party (e.g., vendor, contractor, consultant, software platform, data reporting entity, etc.) requires a signed Data Sharing Agreement before Confidential and/or Sensitive information is shared with the third party. See UWG PL #1007 associated procedure Contract Administration and follow the contract routing and submission instructions found on the Contract Management webpage.
15. Regardless of format, paper, or electronic, all information must be secured in a way to prevent any unauthorized access. The Data User is expected to prevent unauthorized access via an appropriate mechanism, such as the use of a locking file cabinet, file encryption, or logging out of computer systems or applications when not in use.
16. Regardless of format, any media containing Confidential and/or Sensitive information or Personally Identifiable Information (PII) must be labeled as such.

C. 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.

D. 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.

E. 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.

F. 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.

G. 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

H. 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.

I. 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.

J. 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.

K. Compliance

~~Failure to comply with this policy may result in disciplinary actions under applicable UWG and State policies, procedures, and laws.~~

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 - ~~the individual identified by the~~individuals designated by data trustees ~~to be~~as responsible for the data ~~being~~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, ~~in their functional areas~~if applicable.

Data Trustee - ~~the~~ executives of the ~~organizations~~organization who have overall responsibility for the data ~~being~~processed (i.e., read, created, collected, reported, updated or deleted ~~by the~~) 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 ~~of the institution~~).

Data User - ~~are~~ 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 Approved Secured Google Drive** - General use of Google Drive (personal or shared drives) is not authorized for storage of confidential and/or sensitive information; however, a request for a 'secured Google Drive' can be submitted to ITS and a Google Shared drive can be configured to allow for the storage of confidential and/or sensitive information when the scenario warrants its use. Use of a Secured Google Drive does not remove any of the other requirements listed in this procedure.~~

- **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

~~Business Procedures Manual, Data Governance and Management~~

~~UWG PL #1008 Records Information Management and associated procedures~~

- 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