Data Storage and Use

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

A. Procedure

This procedure defines the usage and security requirements of confidential and sensitive data at the University of West Georgia (UWG). It provides guidance to ensure the security of confidential and sensitive information and is essential for compliance with federal, state, and University System of Georgia (USG) regulations.

All employees and contractors who are granted authorization to access the University's data and information assets have a responsibility to protect those assets from unauthorized access, destruction, disclosure, modification or transmission; and are expected to be familiar with and comply with UWG and USG procedures for protection and security of records.

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 BOR-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 Sensitive data in support of the duties authorized by UWG has authorized the Data User to perform.

5. Data users will not use, disclose, or publish confidential or sensitive data for any reason other than approved official University business.

6. Neither confidential nor sensitive information may be transferred by any method to persons who are 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.
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** and **while in transit**, consistent with the USG IT Handbook 5.11 and Georgia Law.

12. Confidential and **sensitive** data must be disposed of in a way that renders the information permanently destroyed. *(see Records Information Management (#1008) and associated procedures)*

13. Confidential **and 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.**

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 or Sensitive or **Personally Identifiable Information (PII)** must be labeled as such.

**B. Compliance**

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

**Definitions**

**Confidential information** - 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 data trustees to be responsible for the data being read, used, created, collected, reported, updated or deleted, in their functional areas.

**Data trustee** - the executives of the organizations who have overall responsibility for the data being read, created, collected, reported, updated or deleted by the units reporting to them. These individuals are normally cabinet-level positions reporting directly to the 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** - 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.

**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.

**Forms**

Data Sharing Agreement posted on the Contract Management web page.

**Guidelines/Related material**

Records Information Management (#1008) and associated procedures

**Attachments**

No Attachments