UNIVERSITY of West Georgia.

UWG PROCEDURE NUMBER: 8.2.2 Data Storage and Use
***Authority*: UWG POLICY: 8.2 Data Security**

The Chief Information Officer, pursuant to the authority of UWG Policy 8.2, establishes the following procedure on data storage and use.

A. Definitions

1. **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.
2. **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.
3. **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.
4. **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.
5. **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 od accuracy and completeness.
6. **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.
7. **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.

B. Procedure

This procedure defines the usage and security requirements of confidential and sensitive data at 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. The data user will adhere to all current UWG and BOR USG policies and procedures.
2. Only employees who have authorization from the relevant data steward(s) may have access to confidential data.
3. The data user will only use confidential and sensitive data in support of the duties UWG has authorized the data user to perform.
4. Data users will not use, disclose, or publish confidential or sensitive data for any reason other than official University business.
5. Neither confidential nor sensitive information may be transferred by any method to persons who are not authorized to access that information.
6. Data users must ensure that adequate security measures are in place at each destination when confidential data is transferred from one location to another.
7. Confidential information must be encrypted while at rest and while in transit, consistent with the USG IT Handbook 5.11 and Georgia Law.
8. Confidential and sensitive data must be disposed of in a way that renders the information permanently destroyed.
9. Confidential 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.
10. Regardless of format, paper or electronic, all information must be secured in a way to prevent any unauthorized access. The data user is expected 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.
11. Regardless of format, any media containing confidential or sensitive information or PII must be labeled as such.

C. Compliance

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

Issued by the Chief Information Officer, the 15 day of March 2018.

Signature, Chief Information Officer

Reviewed by President:

Previous version:

UWG Procedure 8.2.2 data Storage and Use, 2017.

Additional Resources

UWG Procedure 8.1.1 Acceptable Use for Computers and Network Procedure
UWG Procedure 8.2.7 USG Media Hardware Disposal
USG IT Handbook Sections 5.11 and 9.2
State of Georgia Fair Business Practices Act (OCGA §10-1-393.8)