Status **Draft** PolicyStat ID **18511233**

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

Data Stewardship and Classification

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

A. Procedure

Information is a strategic asset of University of West Georgia (UWG), ~~and is critical to institutional~~essential for effective administration, planning and decision-making. ~~Effective and~~To ensure the responsible use of information ~~requires that data is secure~~, ~~well documented, and accessible for use by authorized, trained personnel~~UWG has implemented a Data Governance Framework aligned with the University System of Georgia (USG) Information Technology (IT) Handbook and the USG Business Procedures Manual (BPM) Section 12. Data Governance and Management. ~~To that end, UWG will implement a data governance framework that meets the requirements of the USG IT Handbook and the USG BPM Section 12.~~

~~The data governance and management framework will consist of at least the following functions:~~

1. Data Governance

~~The~~UWG's data governance structure ~~will demonstrate accountabilities for the~~establishes accountability for the university's data assets ~~of the organization to ensure~~, ensuring proper use and handling of data ~~being~~throughout its lifecycle (e.g., created, collected, read, ~~created, collected,~~ reported, updated, or deleted). The structure will identify the offices and positions responsible for data ~~governance structure documentation should identify the offices and positions responsible for the data~~ management, cybersecurity and compliance, as outlined in USG BPM Section 12.2.1 Governance and Organizational Structure.

2. Data Management

~~For data to be properly managed, appropriate data system documentation, data elements definitions,~~

~~data classification, data quality and data availability must be developed and maintained.~~

Effective data management at the University of West Georgia (UWG) necessitates the development and maintenance of several key components:

- **Data System Documentation**: Comprehensive documentation of data systems ensures clarity in data handling processes and facilitates efficient system management.
- **Data Element Definitions**: Clearly defined data elements promote consistency and understanding across the institution, aiding in accurate data interpretation and usage.
- **Data Classification**: Categorizing data based on sensitivity and importance allows for the implementation of appropriate security measures and compliance with relevant regulations.
- **Data Quality**: Maintaining high data quality involves ensuring accuracy, completeness, reliability, and timeliness, which are critical for informed decision-making. (See Data Storage and Use procedure)
- **Data Availability**: Ensuring that data is accessible to authorized personnel when needed supports operational efficiency and responsiveness. (See Data Access Control procedure)

By focusing on these areas, UWG aims to uphold the integrity, security, and utility of its data assets, aligning with best practices in data governance and management.

3. Data Classifications

UWG classifies institutional data to ensure appropriate security measures are applied based on the sensitivity and criticality of the information. These classifications, as outlined in USG BPM Section 12.4.2. Classification, include:

- **Confidential**: Highly sensitive information that requires strict access controls due to legal, regulatory, or contractual obligations. Unauthorized disclosure could result in significant harm to individuals or the institution. Examples include Social Security numbers, financial records, and health information.
- **Sensitive**: Information (e.g., **Personally Identifiable Information (PI/) and Sensitive Personally Identifiable Information (Sensitive PI/)** that is not classified as confidential, but still requires protection due to ethical, privacy, or proprietary considerations. Unauthorized disclosure could cause reputational damage or moderate harm. Examples include student grades and internal memos.
- **Unrestricted/Public**: Information intended for public disclosure and not subject to confidentiality requirements. While this data is accessible to the public, it should still be managed to ensure accuracy and integrity. Examples include press releases and course catalogs.

All Data Users are responsible for handling data in accordance with its classification, ensuring compliance with applicable policies and regulations.

4. Cybersecurity

~~Appropriate steps will be taken~~UWG implements measures to protect information and information

systems from unauthorized access, compromise, or attack. Cybersecurity ~~requires an understanding of potential threats and utilizes strategies that~~efforts will include~~, for example,~~ identity management, risk management, and incident management strategies, as recommended in the USG IT Handbook.

5. Compliance

Data ~~stewards~~Stewards will ensure compliance with all applicable federal, state, and local regulations ~~and develop~~. This includes developing departmental ~~procedures~~guidelines, processes, handbooks as needed and ensuring all Data Users based on their role and responsibilities complete all mandatory and additional trainings as set forth by UWG, accordance with USG BPM Section 12.5. Compliance. ~~This includes training of all data users based on a position's role and responsibilities.~~

By adhering to this framework, UWG commits to the secure, documented, and accessible use of information by authorized and trained personnel.

Failure to adhere to UWG's data governance policies and procedures may result in disciplinary actions and other consequences, including:

- **Disciplinary Measures**: Employees found in violation may face corrective actions up to and including termination of employment, in accordance with UWG and USG policies.
- **Legal and Regulatory Penalties**: Non-compliance with federal and state laws, such as FERPA or HIPAA, may lead to legal action, fines, or other sanctions against the individual and/or the institution.
- **Reputational Damage**: Data breaches or mishandling of information can harm UWG's reputation, affecting trust among students, faculty, and the public.
- **Operational Impact**: Improper data management can disrupt institutional operations, leading to inefficiencies and potential loss of data integrity.

All members of the UWG Community are expected to understand and comply with data governance policies to protect the university's information assets and uphold its commitment to data security and integrity.

Definitions

Confidential Information - Information maintained by a USG organization that is subject to authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 USC Sec 3542) Confidential classified documents are exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

Data Owner- the chief executive office, or President of the institution ~~who is~~. Data Owners are responsible for ~~all~~the identification, appointment and accountability of data ~~read, created, collected, reported, updated or deleted by the offices of the organization~~trustees.

~~**Data steward**~~**Data Steward** - the individual identified by the data trustees ~~to be~~ responsible for the data ~~being read~~processed, and the technology used to do so if applicable, ~~created, collected, reported, updated or deleted and the technology used to do so,~~ in their data area(s).

~~Data trustee~~**Data Trustee** - the executives of the organizations who have overall responsibility for the data being ~~read, created, collected, reported, updated or deleted~~processed in their data area(s). These individuals are normally cabinet-level positions reporting directly to the Data Owner (i.e., University President ~~of the institution~~).

Data User - any faculty or staff, authorized by the appropriate institutional authority, to access enterprise data or data related to their institutions.

Personally Identifiable Information (~~PI~~/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 a USG organization that requires special precautions to protect from unauthorized use, access and disclosure guarding against improper information modification, loss or destruction. Sensitive information is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws but is not necessarily intended for public consumption.

Sensitive Personally Identifiable Information (Sensitive ~~PI~~/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 ~~PI~~/PII requires stricter handling guidelines because of the increased risk to the individual if compromised.

Unrestricted/Public Information - Information maintained by UWG that is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws. Some level of control is required to prevent unauthorized modification or destruction of public information.

UWG Community - For purposes of this procedure, (1) All persons enrolled at or employed by the University, including University students, faculty, staff, administrators, and employees, (2) recognized University-affiliated entities, including University departments, foundations, and registered University student organizations, and (3) Alumni and members of the public.

Related material

- University System of Georgia (USG) Information Technology (IT) Handbook
- USG Business Procedures Manual (BPM) Section 12. Data Governance and Management

Approval Signatures

Step Description	Approver	Date