

<b>Title:</b>	<b>Draft USG Data Handling and Storage Policy</b>		
<b>Policy Number:</b>	YYYY-Julian Date	<b>Topical Area:</b>	Security
<b>Document Type:</b>	Policy	<b>Pages:</b>	4
<b>Issue Date:</b>	DD-MMM-YY	<b>Effective Date:</b>	DD-MMM-YY
<b>POC for Changes:</b>	University System of Georgia (USG) - Office of Information Security		
<b>Synopsis:</b>	Establishes data handling and storage requirements.		

**PURPOSE**

Institutional data is information that supports the mission of an USG Institution. It is a vital asset and is owned by the Institution. Institutional data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This policy sets forth the institution’s standards with regard to the handling of sensitive institutional data.

**POLICY**

To establish policy for the safeguarding of restricted and sensitive data relating to students, faculty and staff that are created, received, maintained or transmitted by the institution. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all USG policies and applicable state and federal laws. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

**SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS:**

The Board of Regents Policy Manual, Section 700  
 USG Information Security Program Policy

**DEFINITIONS**

- I. Archiving/Storage: The act of physically or electronically moving inactive or other records to a storage location until the record retention requirements are met or until the records are needed again.
- II. Institutional Data: Institutional data is information that supports the mission of Institution. It is a vital asset and is owned by the Institution. Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Sensitive Data and sensitive personally identifiable information – S/PII as defined in this section is a subset of Institutional Data.

- III. Authorized User: Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to faculty and staff, trainees, students, vendors, volunteers, contractors, or other affiliates of the institution.
- IV. Electronic Media: All media on which electronic data can be stored, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices.
- V. Electronic Messaging: A set of communication processes used to relay information among the users of computers. Electronic Messages take many forms. Examples: Electronic Mail (E-Mail), FTP, cell phones, Instant Messaging and Internet chat.
- VI. Restricted Data: Data whose access is restricted by federal or state statute (i.e. HIPPA, FERPA, GLB, PCI-DSS). For purposes of this policy, restricted data is a subset of sensitive data.
- VII. Sensitive Data: Data, regardless of its physical form or characteristics, with the highest level of protection including, but not limited to, data protected by law, data protected by legal contracts, or security-related data. It also includes data that is not open to public examination because it contains information, which, if disclosed, could cause severe reputation, monetary or legal damage to individuals or the institution or compromise public activities. Examples include: passwords, intellectual property, on-going legal investigations, medical or grades information protected by FERPA or GLB or PCI or HIPAA, social security numbers, birth dates, professional research, graduate student work, bank or credit card account numbers, income and credit history.

#### DATA COLLECTION

- A. Users should collect only the minimum necessary institutional/sensitive information required to perform institution business.
- B. University System of Georgia (USO) and institution leadership must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with the USG and institution policy and procedure.

#### DATA ACCESS

- A. Only authorized users may access, or attempt to access, sensitive information.
- B. Authorization for access to sensitive data comes from the data owner or custodian, and is typically made in conjunction with an acknowledgement or authorization from the requestor, or other official authority.
- C. Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform institution business.
- D. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the

information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

- E. Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the office or individual granting/revocation department.

#### DATA HANDLING AND DATA TRANSFER

- A. Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.
- B. Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information, which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.
- C. Sensitive information must not be taken off-campus unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.
- D. Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.
- E. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive or laptop.

#### STORAGE OF SENSITIVE DATA

- A. Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.
- B. Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling or working away from the Institution.
- C. Servers and other computers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.
- D. Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.
- E. It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets and databases) that is created on a PC or similar system should be stored on a network drive hosted on a managed server.
- F. Electronic media storing restricted/sensitive data must be protected by

password security. To the extent possible, these devices must employ encryption methods.

## RESPONSIBILITY

- A. Supervisory Personnel: USO and Institution employees whom have supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisory personnel is responsible for the following:
1. Communicating this policy to personnel under their supervision.
  2. Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.
  3. Providing education and training in data management principles to employees under their supervision.
- B. User Responsibilities: Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:
1. Access institutional/sensitive data only in their conduct of institution business.
  2. Request only the minimum necessary confidential/sensitive information necessary to perform institution business
  3. Respect the confidentiality and privacy of individuals whose records they may access.
  4. Observe any ethical restrictions that apply to data to which they have access.
  5. Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

## COMPLIANCE

Compliance with this data protection policy is the responsibility of all members of the Institution community and the University System of Georgia. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to institutional information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by state and federal authorities.



<b>Title:</b>	<b>Draft USG Data Handling and Storage Standard</b>		
<b>Policy Number:</b>	YYYY-Julian Date	<b>Topical Area:</b>	Security
<b>Document Type:</b>	Standard	<b>Pages:</b>	4
<b>Issue Date:</b>	DD-MMM-YY	<b>Effective Date:</b>	DD-MMM-YY
<b>POC for Changes:</b>	University System of Georgia (USG) - Office of Information Security		
<b>Synopsis:</b>	Establishes data handling and storage standards.		

## Purpose

The USG Data Handling and Storage Policy requires controls to manage risks to the confidentiality, integrity and availability of University System of Georgia information. This handling standard defines the controls required for sensitive University System information in any form. These required controls represent a minimum standard for protection of sensitive and sensitive personally identifiable information (S/PII). Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, financial, student, credit cardholder data), may also apply.

Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys highly sensitive USG institutional information is responsible and accountable for complying with this standard.

## Data Creation

University System employees create records or handles records as part of the normal course of conducting the business of the institution. These records document the decisions and activities of our complex educational and business enterprise. It is essential that they be created and maintained appropriately throughout their entire life cycle.

*Sensitive information* contained in institution records constitutes an area of critical concern because of the severe risk to the institution and the System should records be mishandled or information inappropriately accessed or disclosed. As a consequence, records containing sensitive information should exist only in areas where there is a legitimate and justifiable business need, as authorized by the data steward, and maintained under strict controls as outlined in this document.

Institution departments should work to identify and track all institution records through their life cycle by way of records retention schedules (prepared in

collaboration with the institution and State Archive). A first priority in this effort should be the identification of sensitive information. Records schedules will document the existence of these materials, the rationale behind keeping them, and help ensure their availability during the period in which they are vital as either active administrative or historical records. Record retention schedules also will work to ensure the timely disposal of non-permanent, inactive records, thereby mitigating the risk of exposure of information when it no longer serves an active administrative or historical function.

## **Data Access**

Highly sensitive information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. In some cases, information is highly sensitive because of its aggregation into a single document, regardless of whether it contains highly sensitive data elements.

Only institution employees who have authorization from the relevant Data Steward(s), and have a signed confidentiality agreement on file, may have access to highly sensitive information. Any other disclosure of highly sensitive information requires the written approval of appropriate leadership, in consultation with the Office of Legal Affairs as necessary.

## **Data Use, Transmission and Storage**

The following controls are **required** when using, transmitting or storing sensitive information.

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying or faxing it, ensure that only authorized personnel will be able to see the output.
- Store paper documents in a locked drawer *and* in a locked room, or in another secure location approved by the Data Steward.
- Properly identify such information as highly sensitive to all recipients, by labeling it "Sensitive," providing training to personnel, explicitly mentioning the classification, or similar means.
- Encrypt electronic information using an encryption algorithm approved by the USG Office of Information Security when:
  - Placing it on removable media;
  - Placing it on a mobile computer (e.g., mobile devices, PDAs, smart phones, thumb drives); or
  - Sending it via e-mail to *non-institution.edu* addresses.
- Do not send this information via instant message or unsecured file transfer

- unless it is encrypted.
- Follow an established and documented software development lifecycle when building applications that process highly sensitive information.

## Data Transport

The following controls are **required** when transporting highly sensitive information:

- When sending such information by mail (including U.S. Postal Service, DHL, UPS, FedEx, etc.) in non-electric form, the sender must obtain tracking and signature confirmation services and use a tamper-evident sealed package.
- Do not send unencrypted sensitive information by campus mail.
- When carrying unencrypted sensitive information, or devices containing such information, ensure that it is physically secure at all times.
- Do not remove highly sensitive information from an approved secure location without prior approval of the Data Steward.

## Data Destruction

- Institution records should be destroyed only in accordance with the *Archives and Records Management Policy*.
- Destroy electronic instances of institution information using an USG OIS - approved method. **Reformatting a hard drive is not sufficient to securely remove all data.**
- Crosscut shred or pulp all sensitive information in paper form. This includes all transitory work products (e.g., unused copies, drafts, notes).

## Definitions

**Data Handling** Using, storing, processing, transferring, administering, aggregating, sharing, and/or maintaining Institution information

**Data Steward** An individual who is responsible for ensuring the confidentiality, integrity, and availability of Institution information. A Data Steward defines access to and restrictions on use of the information for which he or she is responsible.

**Encrypt(ion)** The process of encoding data so that it can only be read using the appropriate key.

**Information Security** The protection of the confidentiality, integrity, and availability of Institution information.

**Security Classifications** Categories of Institution information based upon

intended use and expected impact if disclosed.

**Public** Information intended for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

**Internal** Information not intended for parties outside the University that, if disclosed, would have minimal or no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

**Sensitive** Information intended for limited use within the Institution that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

**Highly Sensitive** Information intended for very limited use within the Institution that, if disclosed, could be expected to have a severe adverse effect on the operations, assets, or reputation of the Institution or University System, or the Institution's obligations concerning information privacy.