Information Security Program

July 2019
Table of Contents

Introduction and Purpose ........................................................................................................ 5
Scope ...................................................................................................................................... 5
Information Security Policy and Procedure Development ....................................................... 6
  Responsible Units ................................................................................................................. 6
USG and UWG Associated Policies and Procedures ............................................................... 7
Information Security Organization and Governance .............................................................. 7
  Roles and Responsibilities ................................................................................................. 7
  University President ........................................................................................................ 7
  VP IT/Chief Information Officer ......................................................................................... 7
  Information Security Officer (ISO) .................................................................................... 8
Data Owner ........................................................................................................................... 8
Data Trustees ....................................................................................................................... 8
Data Stewards .................................................................................................................... 8
Data Users ........................................................................................................................... 9
Information System Owners ................................................................................................ 9
  Responsible Units ........................................................................................................ 9
  USG and UWG Associated Policies and Procedures ......................................................... 9
Risk Management, Assessment and Planning ..................................................................... 9
  Risk Assessment ............................................................................................................. 10
  Risk Planning ................................................................................................................ 10
  Responsible Units ........................................................................................................ 10
  USG and UWG Associated Policies and Procedures ....................................................... 10
Information System Categorization – Security Categories, Data Classification, and Information Classification ........................................................... 10
  Security Categories ....................................................................................................... 11
  Data Classification ......................................................................................................... 11
  Information Classification ............................................................................................. 12
  Responsible Units ........................................................................................................ 13
  USG and UWG Associated Policies and Procedures ....................................................... 13
Privacy of Personal Information ......................................................................................... 14
  Collection of Personal Information ............................................................................... 14
  Access to Personal Information ................................................................................... 14
  Access to Electronic Data Containing Personal Information ........................................ 15
  Responsible Units ........................................................................................................ 15
  USG and UWG Associated Policies and Procedures ....................................................... 15
Personnel Information Security – User Account Management ........................................... 15

Information Security Program  Page 2
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>23</td>
</tr>
<tr>
<td>Separation of Duties</td>
<td>24</td>
</tr>
<tr>
<td>Emergency Changes</td>
<td>23</td>
</tr>
<tr>
<td>Access Review</td>
<td>24</td>
</tr>
<tr>
<td>Modifying Access</td>
<td>24</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>24</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>24</td>
</tr>
<tr>
<td>Information Asset Management</td>
<td>24</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>25</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>25</td>
</tr>
<tr>
<td>Information Systems Acquisition</td>
<td>25</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>25</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>25</td>
</tr>
<tr>
<td>Information Security Incident Management and Response</td>
<td>25</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>26</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>26</td>
</tr>
<tr>
<td>Physical Access Control</td>
<td>26</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>26</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>26</td>
</tr>
<tr>
<td>Business Continuity Planning</td>
<td>26</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>27</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>27</td>
</tr>
<tr>
<td>Disaster Recovery Planning</td>
<td>27</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>27</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>27</td>
</tr>
<tr>
<td>Periodic Security Assessments and Audits</td>
<td>27</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>27</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>27</td>
</tr>
<tr>
<td>Laws and Compliance</td>
<td>27</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>30</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>30</td>
</tr>
<tr>
<td>Policy Enforcement</td>
<td>30</td>
</tr>
<tr>
<td>Responsible Units</td>
<td>31</td>
</tr>
<tr>
<td>USG and UWG Associated Policies and Procedures</td>
<td>31</td>
</tr>
</tbody>
</table>
Introduction and Purpose

The University of West Georgia’s (UWG) Information Security Program provides direction for managing and protecting the confidentiality, integrity and availability of UWG information assets.

In accordance with the University System of Georgia’s (USG) IT Handbook and Board of Regents (BOR) Policy Manual, this Information Security Program contains administrative, technical and physical safeguards to protect campus information assets. Unauthorized modification, deletion or disclosure of information assets can compromise the mission of UWG, violate individual privacy rights and possibly constitute a criminal act.

The intent of the Information Security Program is to:

- Document roles and responsibilities of positions within the University as they relate to information security.
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g., paper or electronic).
- Document risk management strategies to identify and mitigate threats and vulnerabilities.
- Document incident response strategies.
- Document strategies for ongoing security awareness and training.
- Comply with applicable laws, regulations, UWG and USG policies.

It is the collective responsibility of all users to ensure:

- Confidentiality of information under their care.
- Integrity and availability of information stored on or processed by UWG information systems.
- Compliance with applicable laws, regulations, USG policies and UWG policies governing information security and privacy protection.

The UWG Information Security Program and related documentation enhances institutional effectiveness and sustainability by setting forth standards and controls designed to protect information assets and the privacy of our constituents.

Scope

Consistent with the USG IT Handbook and BOR Policy, the UWG Information Security Program shall apply to the following:

- Centrally and departmentally managed campus information assets.
- All users employed by UWG, its auxiliaries, contractors, vendors or any other person with access to UWG’s network resources or information assets. This includes non-UWG-owned computing devices that may store protected information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by UWG. This includes third party service providers’ systems that access or store...
Auxiliary organizations, external businesses and organizations that use campus information assets must operate those assets in conformity with the UWG Information Security Program.

UWG retains ownership or stewardship of information assets owned or managed by, or entrusted to the University. UWG reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or restricting data to/from campus information systems and across network resources. These activities are intended to protect the confidentiality, integrity and availability of information and are not intended to restrict, monitor or utilize the content of legitimate academic and organizational communications.

**Information Security Policy and Procedure Development**

UWG’s Information Security Program, combined with UWG Policy 8.1 Technology and Use, and UWG Procedure 8.1.1 Acceptable use for Computers and Network, establishes expectations for protecting university information assets. These are supported by related policies, standards, guidelines and practices to facilitate campus compliance:

- **Policies** are high-level statements of principle that provide technology agnostic scope and direction to the campus community. Campus-level policy must follow the UWG policy approval process.

- **Standards** establish specific criteria and minimum baseline requirements or levels that must be met to comply with policy. They are typically technology agnostic and they provide a basis for verifying compliance through audits and assessments.

- **Guidelines** are recommended or suggested actions that can supplement an existing standard or provide guidance where no standard exists. They may or may not be technology agnostic.

- **Procedures** consist of one or more interrelated steps taken to achieve a specific goal or task designed to implement a policy, standard or guideline. They are detailed descriptions that may use specific technologies, instructions and forms to facilitate completing the process. Campus-level procedures must follow the UWG procedure approval process.

The Vice President of Information Technology Services/Chief Information Officer (VP IT/CIO) or designee is responsible for coordinating the development of information security and technology policy, procedures, standards, and guidelines. Using a standard format, a draft policy or procedure is developed and submitted to the Campus Policy Taskforce. The documents are shared broadly with campus constituents for review and comment. All input is considered before a final document is produced. Policies require Presidential approval, but procedures, standards, and guidelines only require VPIT/CIO approval and Presidential review.

Information Technology Services division level Document Development Procedure sets document standard as well as a review cycle for all technology and security policy, procedures, standards and guidelines.

**Responsible Units**

All departments within the division of Information Technology Services are responsible for following the document development guidelines.
USG and UWG Associated Policies and Procedures

1. UWG ITS Document Development Procedure
2. UWG Policy 1.1 Institutional Policy
3. UWG Policy 1.2 Policy and Procedures
4. UWG Policy 1.3 Policy Authority
5. USG IT Handbook Section 1

Information Security Organization and Governance

In accordance with USG policy, a position is designated to coordinate and oversee campus compliance with an information security program and related laws, policies, standards and practices. The UWG Information Security Officer (ISO) reports to the Deputy CIO and works to develop, implement and ensure compliance with policies, standards and practices related to the security of information technology resources.

The VP IT/CIO reports directly to the President and is a member of the cabinet that provides advice and counsel to the President. The VP IT/CIO regularly briefs the Faculty Senate, Administrative Council, the President’s Advisory Counsel, and other campus constituents on information security issues.

The IT Steering Board reviews and recommends prioritization of information technology projects. A security review by the ISO is included in the project development cycle. Technology procurement is governed by USG IT Handbook Section 4. The IT Steering Board reviews and recommends for approval large or complex IT acquisitions, and routine approvals are granted via Peoplesoft workflow.

Administrators across the university are responsible for ensuring information security policies, standards and practices are followed by employees in their respective areas.

Technical support staff and individual users are expected to follow established standards and practices and to report potential security violations.

Roles and Responsibilities

The USG IT Handbook, along with BOR Policy defines the following roles and responsibilities as they relate to technology and information security:

University President

The President shall be responsible for ensuring that appropriate and auditable security controls are in place and acts as the university data owner.

VP IT/Chief Information Officer

The Chief Information Officer (CIO) is responsible for the overall leadership and general administrative responsibilities for the University of West Georgia's IT organization including academic and administrative computing, telecommunications, data administration, network infrastructure, web development, software and classroom instructional technology support, and system support services. The CIO provides leadership in the development and monitoring of an IT plan and fosters a culture that is collaborative and service oriented.
The CIO along with the Information Security Officer (ISO), whether or not designated as data trustees, have the responsibility for ensuring that a technical infrastructure is in place to support the data needs and assets, including availability, delivery, access, and security across the entirety of their operational scope.

**Information Security Officer (ISO)**

The ISO is designated by the VP IT/Chief Information Officer. The individual must stay abreast of security related news, policies and best practices in government, at other organizations and in higher education so that the policies of this University may be revised to address policy weaknesses.

This person's responsibilities include but are not limited to working with managers to train users; overseeing University network security; investigating policy violations; recovering from incidents; and coordinating responses and disciplinary actions with appropriate University members, offices and departments.

**Data Owner**

As chief executive officer, the president is identified as the data owner of the institutional data. The Data owner has the responsibility for the identification, appointment and accountability of Data Trustees. The Data Owner will inform the USG Data Governance Committee of their data trustee appointments including office, name, and contact information of the incumbent.

**Data Trustees**

Data trustees, designated by the data owner, are senior leaders (VPs) who have overall responsibility for the data being read, created, collected, reported, updated or deleted by the units reporting to them. These positions/offices would normally be cabinet-level positions reporting directly to the data owner.

Responsibilities of the data trustees include, but are not necessarily limited to:

1. Ensuring that data accessed and used by units reporting to them is done so in ways consistent with the mission of the office and participant organization;

2. The identification, appointment and accountability of data stewards within the functional area(s) for which they are responsible. The data trustees will inform the UWG Data Governance Committee of their data trustees appointments, including office, name, and contact information of the incumbent;

3. Participating as a member of the strategic data governance and management committee; and,

4. Communicating concerns about data quality to the data owner.

**Data Stewards**

Data stewards, designated by the data trustees, are offices/positions responsible for the data being read, used, created, collected, reported, updated or deleted, and the technology used to do so, in their functional areas. Positions held by the data stewards normally would report directly to the data trustee. Data stewards recommend policies to the data trustees, and establish procedures and guidelines concerning the access to, completeness, accuracy, privacy, and integrity of the data for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas. Depending on the size and complexity of a functional unit, it may be necessary, and beneficial, for a
designated data steward to identify associate data stewards to manage and implement the stewardship process

Data Users

Any individual with access to the University’s systems, information, or networks is considered a data user and is responsible for following all policies and procedures associated with that access.

Information System Owners

The information system owner is the senior person in the organization responsible for the application or service, and ensures that the application or services renders value to the organization. For most infrastructure services such as the local area network, the CIO is that information system owner. For most business and educational support systems, the Vice President to whom the function reports is normally the information system owner. Information system owners may appoint a functionally responsible designee as the primary liaison between the IT service unit and the customers served by the system or services provided by IT. For example, the VP of Enrollment Management, who is the information system owner for the student information system, might appoint the Registrar as the day-to-day liaison between the customers of the enrollment management system and IT for support and service provisioning.

Responsible Units

All individuals within the division of Information Technology Services are responsible for understanding their security roles and responsibilities.

All Data Trustees are responsible for understanding this section and identifying the data stewards and information systems owners.

USG and UWG Associated Policies and Procedures

1. UWG ITS IT Steering Board Procedures
2. UWG Procedure 8.2.2 Data Storage and Use
3. UWG Procedure 8.2.4 Data Governance and Classification
4. USG IT Handbook Section 1
5. USG BPM Section 12

Risk Management, Assessment and Planning

Risk management allows an organization to identify the threats in their environment that can act as impediments to achieving the University’s mission. By systematically assessing potential risks involved in providing and maintaining information systems and information access the University can better plan for secure information systems, implement effective controls, determine resource requirements, and identify budgetary needs.

Once UWG identifies and assesses an information security risk, a determination can be made to either avoid the risk altogether (often not an option), reduce the risk to acceptable levels, transfer the risk to another party or assume the identified risk.
Risk Assessment

UWG performs periodic assessments of its information security risks and vulnerabilities. Risk assessments may be aimed at particular types of information, areas of the organization or technologies. Risk assessments are part of an ongoing risk management process. They provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. The UWG ITS Risk Assessment Guide contains processes to perform annual self-assessments and report on the risks identified and the associated mitigation efforts.

Risk Planning

Security must be a consideration from the very beginning of every project involving technology or information systems. When implementing information systems and solutions a formal project plan will guide project execution and include a well-planned evaluation of the risk(s) associated with the project. In addition, a risk review should be performed before any system is placed into production that includes:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.
- A risk assessment, including a review for regulatory, legal and policy compliance.
- A contingency plan, including the data recovery strategy.
- A review of on-going production procedures, including change controls and integrity checks.

Responsible Units

All directors within the division of Information Technology Services are responsible for carrying out annual risk assessments and ensuring risk review is included in every technology implementation.

Information System Owners and/or Data Stewards are responsible for working with ITS to ensure functional risks are assessed and remediated.

USG and UWG Associated Policies and Procedures

1. UWG ITS Risk Assessment Guide
2. UWG Project Management Development Documents
3. USG IT Handbook Section 2
4. USG IT Handbook Section 6

Information System Categorization – Security Categories, Data Classification, and Information Classification

Data, information, and information systems are critical assets of the University, and as such, every member of the campus community has a responsibility to protect the confidentiality, integrity, and availability of the data and the information system accessed or managed as part of their job function.

Adequate protection of data and information requires an understanding of what is being protected and why it is being protected. This understanding begins by defining the following:
1) Security Categories

2) Data Classification

3) Information Classification

Security Categories
The security categorization of information systems and data is based on the potential impact that a loss of that data or information system would have on the organization. The Security Categories are Confidentiality, Integrity, and Availability which are defined as:

1. Confidentiality - “Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…” [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.

2. Integrity - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…” [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

3. Availability - “Ensuring timely and reliable access to and use of information…” [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to, or use of, information or an information system

Data Classification
By default and in accordance with the USG IT Handbook, all institutional data is designated as internal data for use within the organization or to satisfy external reporting requirements to the USG BOR, and to state, federal, or other external agencies. Employees have access to these data for use in the conduct of University business. These data, while available within the organization, are not designated as open to the general public unless otherwise required by law. The permission to view or query institutional data should be granted to all data users for all legitimate purposes. As part of the data definition process, data stewards will assign each data element and each data view in institutional data to one of three categories: unrestricted, sensitive, and confidential. Note: In some circumstances, as long as specific identifying data elements are removed, a data view may include elements of institutional data that would otherwise be sensitive or confidential.

Unrestricted Data
Where appropriate, data stewards may identify institutional data elements that have no access restrictions as available to the general public. These data will be designated as unrestricted or public data.

Sensitive Data
Where necessary, data stewards may specify institutional data elements as sensitive data for which users must obtain specific authorization to access since the data’s unauthorized disclosure, alteration, or destruction will cause perceivable damage to the participant organization. The specification of data as sensitive should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or limitations access is typically given.

Confidential Data
Where required, data stewards may identify institutional data elements as confidential, for which the highest levels of restriction should apply due to the risk or harm that may result from disclosure or inappropriate use. This includes information whose improper use or disclosure could adversely affect the ability of the participant organization to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

Information Classification

The University’s records (paper or electronic, including automated files and databases) are essential public resources that must be given appropriate protection from unauthorized use, access, disclosure, modification, loss, or deletion. Each record must be classified using the following classification structure:

1. Unrestricted/Public Information is information maintained by the organization that is not exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

2. Sensitive Information is information maintained by the organization that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of UWG financial transactions and regulatory actions.

3. Confidential Information is information maintained by the organization that is exempt from disclosure under the provisions of the Open Records Act or other applicable state or federal laws.

In addition, Personal Information may occur in unrestricted/public, sensitive, and/or confidential information. Personal information is information that identifies or describes an individual as defined in, but not limited by, the statutes listed below. This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal information includes, but is not limited to:

1. Notice-triggering personal information - specific items or personal information (name plus Social Security Number, driver’s license/Georgia identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person.

2. Protected Health Information - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. Laws require special precautions to protect from unauthorized use, access, or disclosure.

3. Electronic Health Information - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers conducting electronic transactions ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure.

4. Personal Information for Research Purposes - personal information requested by researchers specifically for research purposes. Releases may only be made to the USG or other non-profit educational institutions in accordance with the provisions set forth in the law.

5. 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.

6. 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 an individual if compromised. The designated owner of a record is responsible for
making the determination as to whether that record should be classified as public or confidential,
and whether it contains personal and/or sensitive information. The owner of the record is
responsible for defining special security precautions that must be followed to ensure the integrity,
security, and appropriate level of confidentiality of the information. Records containing sensitive
and/or personal information require special precautions to prevent inappropriate disclosure. When
confidential, sensitive, or personal information is contained in public records, procedures must be
used to protect it from inappropriate disclosure. Such procedures include the removal, redaction, or
otherwise masking of the confidential, sensitive, or personal portions of the information before a
public record is released or disclosed.

Records Retention

Almost all data and information stored or used by the University is subject to the BOR Policy on
Records Retention and the USG Records Retention Schedule. Data Trustees and Data Stewards
are responsible for ensuring that the data under their purview follows the appropriate Records
Retention Schedule.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring the
information assets under their span of control are properly categorized and security measures are
in place to maintain data and information security.

Data Trustees and Data Stewards are responsible for ensuring the data assets under their span of
control are properly categorized and functional security measures are in place to maintain data and
information security.

USG and UWG Associated Policies and Procedures

1. UWG ITS Server Standard
2. UWG ITS Server Classification Procedure
3. UWG Procedure 8.2.2 Data Storage and Use
4. USG IT Handbook Section 5
5. USG IT Handbook Section 6
6. BOR Policy on Records Retention
7. USG Records Retention Schedule
8. UWG Records Retention Policy
Privacy of Personal Information

UWG is a public university and information stored on campus information systems may be subject to disclosure under state law and the Georgia Open Records Act. No campus information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, UWG acknowledges its obligation to respect and protect private information about individuals stored on campus information systems and network resources. All users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or protection of information they create or store on campus systems.

Collection of Personal Information

To comply with state and federal laws and regulations, individuals and processes may not collect personally identifiable information unless the need for it has been clearly established.

When such information is collected:

- The Data Steward and individual user collecting the information will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The Data Steward and individual user collecting the information shall store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

Access to Personal Information

Except as noted elsewhere in USG or UWG policy, information about individuals stored on campus information systems may only be accessed by:

- The individual to whom the stored information applies or the individual's designated representative(s).
- Authorized UWG employees with a valid UWG-related business need to access, modify or disclose that information.
- Appropriate legal authorities.

When appropriate, authorized UWG personnel following established campus procedures may access, modify and/or disclose information about individuals stored on campus information systems, or a user's activities on campus information systems, or network resources without consent from the individual. For example, UWG may take such actions for any of the following reasons:

- To comply with applicable laws or regulations.
- To comply with or enforce applicable USG or UWG policy.
- To ensure the confidentiality, integrity or availability of campus information.
- To respond to valid legal requests or demands for access to campus information.

If UWG personnel accesses, modifies and/or discloses information about an individual and/or the individual's activities on campus information systems or network resources, that individual will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by UWG policy or applicable laws.

Data Stewards are advised to consult the UWG Records Retention Manager to determine which records must be made available for public inspection under the Georgia Open Records Act.
Access to Electronic Data Containing Personal Information

Individuals who access or store sensitive or confidential data must use due diligence to prevent unauthorized access and disclosure of such information.

Browsing, altering or accessing electronic messages or stored files in another user's account, computer or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for UWG business reasons. This prohibition does not affect:

- Authorized access to shared files and/or resources based on assigned roles and responsibilities.
- Authorized access by a network or system administrator, support technician or departmental manager where such access is within the scope of that individual's job duties.
- Access to implicitly publicly accessible resources such as university websites.
- Campus response to subpoenas or other court orders.
- Campus response to a request pursuant to public record disclosure laws.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring compliance with this section.

Data Stewards are responsible for ensuring compliance with this section.

USG and UWG Associated Policies and Procedures

1. UWG ITS Work Expectations Document
2. UWG Procedure 8.1.1 Acceptable Use for Computers and Network
3. USG IT Handbook Section 5
4. USG IT Handbook Section 6

Personnel Information Security – User Account Management

User account access is a critical component of ensuring overall data privacy and protection. It is the shared responsibility of Human Resources and Information Technology Services to ensure that employees have only the access required to complete their job functions, and that accounts are removed from systems promptly upon termination or change in employment.

Termination or Change of Employment

Access rights must be promptly revoked from information resources upon termination of employment, or when job duties no longer provide a legitimate business reason for access, except where specifically permitted by campus policy or by the Data Steward. Unless otherwise authorized in writing, when an employee voluntarily or involuntarily separates from the University, information system privileges, including all internal, physical and remote access, must be revoked within five business days. Changes in employment that result in a change in job duties and access rights must be reported within 30 days.
Procedures must be implemented to ensure proper disposition of information assets upon termination. Electronic and paper files must be promptly reviewed by an appropriate manager to determine who will become the data steward of such files, and identify appropriate methods to be used for handling the files. If the separating employee is holding resources subject to a litigation hold, the Data Trustee must ensure preservation of relevant information until the litigation hold has been revoked, at which point the resource is subject to the normal record retention schedule.

Procedures must be implemented to verify that items granting physical access, such as keys and access cards, are collected from the exiting employee. Any access list that grants the exiting employee physical access to a limited-access area on the campus must be updated appropriately to reflect the change in employment status.

Procedures must be established to allow for separated employees to obtain such incidental personal electronic information, as appropriate.

Information system privileges retained after separation from the campus must be documented and authorized by an appropriate Data Steward. Under no circumstances will access to campus technology resources continue beyond 6 months from date of separation unless approval from the President is obtained.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring compliance with this section.

The Chief Human Resource Officer is responsible for procedures that properly notify the appropriate parties on campus of employment changes.

USG and UWG Associated Policies and Procedures

1. UWG ITS Account Management Procedures
2. UWG Human Resources Procedure
3. USG IT Handbook Section 5
4. USG IT Handbook Section 6
5. UWG Physical Access Control

Information Security Awareness Training, and Education

The key to maintaining information security is a well-trained and educated University community. Information security training is required of all new employees, and must be refreshed annually. In addition to this high-level training, supervisors are responsible for training employees on the specific requirements of the data and information they handle as part of the job duties. This includes any privacy regulations, state and federal laws, and UWG or USG policies that govern the use of that data or system.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring that their staff is properly trained on information security appropriate to their job role as well as any relevant regulations and laws.
Information System Owners and/or Data Stewards are responsible for ensuring users who access their systems are properly trained and understand the rules and regulations that impact the use of those systems.

The President is responsible for ensuring annual information security training is completed.

**USG and UWG Associated Policies and Procedures**

1. UWG Annual Training Procedures
2. UWG Procedure 8.2.3 Security Awareness Training
3. Department level training procedures
4. USG IT Handbook Section 1
5. USG IT Handbook Section 5

**Managing Third Parties**

Third parties, i.e, contractors, vendors, consultants, cloud service providers who access UWG information assets must adhere to appropriate USG and UWG information security policies and standards. If appropriate, a risk assessment must be conducted to determine the specific implications and control requirements for the service provided and/or the information accessed.

**Granting Access to Third Parties**

Third party service providers may be granted access to campus information assets containing confidential or sensitive data only when they have a need for specific access in order to accomplish an authorized task. This access must be requested and approved by the Information System Owner or Data Steward and based on the principles of business need and least privilege.

Third party service providers will not be granted access to any UWG network or system until a Third Party Agreement has been signed which defines the method of access, appropriate security controls and confidentiality terms.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that third party access is properly vetted before access is granted. This includes validating that a Third Party Agreement exists and that a Third Party Remote Access form has been completed.

Information System Owners and/or Data Stewards are responsible for ensuring third parties who access their systems have a Third Party Agreement in place.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS Third Party Agreement Policy and Procedure
2. UWG ITS Remote Access Policy and Procedure
3. USG IT Handbook, all sections that mention vendor requirements

**Information Technology Security**
The USG IT Handbook and UWG policies and procedures require the University to appropriately secure its information technology resources to protect the confidentiality, integrity and availability of university information. This includes, but is not limited to computer systems, network resources and software applications.

Each member of the campus community and third party providers are responsible for the security and protection of information technology resources over which they have control. The physical and logical integrity of these resources must be protected against potential threats such as unauthorized access, malicious or criminal action, inadvertent compromise and inappropriate use.

Protection of information technology assets must be commensurate with the criticality of the function performed, the nature and level of access provided, information classification associated with the asset, exposure of the asset to potential risks, and the liability to the university if the asset is compromised. In general, a combination of administrative, operational and technical security safeguards will be required.

Combined with UWG’s Acceptable Use Policy, said policies and related standards and practices set expectations and define minimum requirements for securing UWG’s information technology infrastructure and resources.

End Point Security

Any device that connects to the network or stores data must have device-appropriate controls in place to detect, prevent and report malicious software effectively. Electronic data received from untrusted sources must be checked for malicious software prior to being placed on a non-quarantined location of a campus network or information system. In addition, desktop and mobile devices must be managed by the campus standard end point management application and participate in application and operating system patching.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring appropriate controls are in place to maintain network and application security.

USG and UWG Associated Policies and Procedures

1. ITS End Point Security Procedure
2. USG IT Handbook Section 5

Network Management

The network infrastructure is provided as a central utility for all users of UWG information resources. It is important that the infrastructure, which includes cabling and the associated ‘active equipment,’ continues to develop with sufficient flexibility to meet demands while at the same time remaining capable of utilizing anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Procedures must be in place that allow the identification and control of devices and users of the network, and if necessary, removal of devices and/or users from the network.

All connections between the UWG networks and the Internet (or any other publicly accessible computer network) must be managed by an approved firewall and related access controls.
device (switch and router) and firewall configuration standards and procedures must be documented to ensure reliable and reproducible device deployment.

Firewall configuration rules and permissible service rules should be reached after an evaluation of risks and benefits has been conducted by the ISO, firewall administrator, and information system owner. These rules will be changed using the Change Management Procedure.

Because firewalls provide such an important barrier to unauthorized access to UWG’s networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.

**Responsible Units**

The Director of Infrastructure and Operations in Information Technology Services is responsible for ensuring appropriate controls are in place to maintain network security.

**USG and UWG Associated Policies and Procedures**

1. ITS Network Management and Security Procedure
2. ITS Change Management Policy and Procedure
3. ITS Firewall Management Documentation
4. USG IT Handbook Section 5

**Encryption**

Confidential and sensitive data and information, including account credentials, must not be stored or transmitted unless effective security controls have been implemented to protect the data. Individuals must use encryption, or equally effective measures, when handling confidential and sensitive information. This includes portable electronic media, such as thumb drives, CDs, DVDs, laptops, and mobile devices. Applications must use encryption to protect credentials while at rest and while in use or in transit. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by the UWG Information Security Officer in conjunction with the appropriate Data Steward.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that encryption is in use where required by policy or law.

**USG and UWG Associated Policies and Procedures**

1. UWG Procedure 8.2.2 Data Storage and Use
2. USG IT Handbook Section 5

**BYOD**

All UWG employees, including full- and part-time staff, consultants and other agents who use a personally-owned device to access, store, back up or relocate any UWG or client-specific data must take steps to protect that data and information. Such access to data and information is a privilege, not a right, and UWG employment does not automatically guarantee the use of...
personally-owned devices on the UWG network or with UWG systems. When a personally-owned device is used, the end user agrees to abide by all UWG, and USG policies and procedures, as well as all applicable state and federal laws.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that the UWG BYOD Procedure is followed.

All supervisory staff at UWG are responsible for ensuring that the UWG BYOD Procedure is followed in their unit.

**USG and UWG Associated Policies and Procedures**

1. UWG Procedure 8.2.6 BYOD
2. USG IT Handbook Section 8

**Media Disposal and Protection**

All UWG employees and agents are responsible for ensuring that all devices that store UWG information are protected while in use, and disposed of in such a way to render the information unreadable and unrecoverable. This includes using encryption on portable devices and mobile media to secure confidential or sensitive data. Portable media should be labeled in such a way to ensure proper storage and destruction.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that the UWG Media Hardware Disposal and Data Storage and Use Procedures are followed.

All supervisory staff at UWG are responsible for ensuring that the UWG Media Hardware Disposal and Data Storage and Use Procedures are followed.

**USG and UWG Associated Policies and Procedures**

1. UWG Procedure 8.2.7 Media Hardware Disposal
2. UWG Procedure 8.2.2 Data Storage and Use
3. USG IT Handbook, multiple sections

**Information Asset Event Logging and Monitoring**

In order to effectively manage information systems and maintain confidentiality, availability and integrity, computer and network hardware, operating system and applications must be configured to log events that impact the health of the system as well as the security of the system. Logs serve functions such as optimizing system and network performance, recording the actions of users and providing data useful for investigating security events. Logs containing records related to computer security may include audit logs that track user authentication attempts and security device logs that record possible attacks.

Data generated by event monitoring must be retained for a period of time that is consistent with effective use, UWG records retention schedules, regulatory and legal requirements such as
compliance with litigation holds, and USG Policy.

At a minimum, network, server and application administrators are required to regularly review, remediate and report events that occur using the IT Handbook Section 3.2 as a guide. Any compliance or regulatory requirement supersedes the USG IT Handbook.

<table>
<thead>
<tr>
<th>Category</th>
<th>No Confidential, Sensitive or PII</th>
<th>Departmental Level System with limited C,S and PII</th>
<th>Enterprise Information System with C,S and PII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Retention</td>
<td>1 to 2 weeks</td>
<td>1 to 3 months</td>
<td>3 to 12 months</td>
</tr>
<tr>
<td>How often logs must be analyzed</td>
<td>Every 1 to 7 days</td>
<td>Every 1 to 3 days</td>
<td>Once a day</td>
</tr>
</tbody>
</table>

Network monitoring, or event monitoring must not be conducted for the purpose of gaining unauthorized access, ‘snooping,’ or for other activities that violate USG and UWG Acceptable Use Policies. Records created by monitoring controls (e.g., event logging) must be protected from unauthorized access and reviewed regularly. Access to the data generated by the monitoring controls (e.g., logging) must be restricted to those who have a business need.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that appropriate logging and monitoring is taking place, and all USG and UWG policies and procedures are being followed.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS Logging and Monitoring Procedure
2. UWG Procedure 8.1.1 Acceptable Use for Computers and Network
3. USG Handbook Section 3

**Configuration Management**

Configuration standards are necessary to ensure that information technology systems, network resources, and applications are appropriately secured to protect confidentiality, integrity and availability. Network, system, desktop and application administrators are responsible for defining and maintaining configuration standards that meet all UWG and USG policies along with applicable state and federal laws. System configuration documentation must include data and process flow diagrams.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that
the configuration management is taking place on the systems and networks within their span of control.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS Configuration Management Procedure
2. UWG ITS Data and Process Flow Standard

**Information System Patching, Vulnerability Assessment and Maintenance**

A robust application, firmware, BIOS and operating system patch management routine provides a strong foundation for overall security. Patch management must include periodic review of available patches, testing of patches, and timely installation of patches. In addition, vulnerability scanning and remediation must be done to detect weaknesses in installed applications or system configurations.

Vulnerability notices come from a variety of sources, such as REN-ISAC, MS-ISAC, and operating systems and application vendors. Each notice must be reviewed to determine if any UWG systems are impacted. If a system is deemed vulnerable, research must be done to determine if a patch can be safely applied, or if other remediation steps are necessary. All actions should be documented in maintained in the ITS ticketing system.

In addition to external vulnerability notices, UWG will actively perform vulnerability scans to detect operating system and application vulnerabilities. The results of these scans must be reviewed and appropriate actions taken to address the vulnerability. All actions should be documented in maintained in the ITS ticketing system.

Security related service packs, patches, and/or hot fixes, including those for firmware and BIOS, must be applied periodically to all operating systems and applications. Whenever possible, the systems should be configured to automatically notify the system/network/application administrator when a patch is available. After release of a patch, appropriate testing must be done before the patch is put into production. Patches that address critical vulnerabilities must be applied as quickly as possible. Normal patches must be applied no later than 30 days after announced. Patches should only be acquired from the operating system vendor or a well-known, reputable, and trusted authority on the system.

Patches must be thoroughly tested before implementation into the production environment. In addition, controls should be taken to ensure the production systems can be effectively and properly “rolled back” to the state before patches were applied.

In accordance with change management, all patch installs should be documented and maintained.

System maintenance windows will be defined based on the business need of the University, and in conjunction with the information system owner.

In addition to vulnerability scanning, certain systems require that penetration testing be performed to meet various regulatory requirements. System that fall under PCI or the GLBA are two such examples. The directors of IS and IO should work with the information system owners to ensure pen testing is completed as required.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that all devices are patched and have vulnerability management procedures defined and followed.
USG and UWG Associated Policies and Procedures

1. UWG ITS Vulnerability Management Procedure
2. UWG ITS Patch Management Procedure
3. UWG Vulnerability Scanning Procedure
4. UWG Maintenance Windows Document
5. USG IT Handbook Section 5

Change Management

The introduction of change into an information system or network carries inherent risk to both resource availability as well as security. A well-defined change control, or change management, process helps to reduce the risk and ensure that needed changes are well planned and successful. UWG ITS maintains a change control policy and procedure to manage change in the University’s systems and networks. Changes which are well documented and routinely performed can be classified as pre-approved. Other changes will require review and approval by a change control board.

Emergency Changes

Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the campus’ formal change management process. Such emergency changes must be appropriately documented and promptly submitted to the campus normal change management process.

Responsible Units

All directors within the division of Information Technology Services are responsible for ensuring that the Change Management Policy and Procedure is followed.

USG and UWG Associated Policies and Procedures

1. UWG ITS Change Management Policy and Procedure

Access Control

Access to UWG information systems must be controlled in order to reduce risk and the potential for data exposure. Granting access to UWG information systems, separating duties of individuals who have access to an UWG information asset, and conducting reviews of access rights to UWG information systems are all integral to overall information security.

Appropriate controls must be in place to prevent unauthorized access to protected information. This includes not only the primary information system, but also all data extracts and backup copies. Access to campus protected information systems must be denied until specifically authorized by the Information System Owner or Data Steward. When access is granted, it must be based on the principles of business need and least privilege.

Authentication controls, such as login and password, must be implemented for access to campus
information assets that access or store protected data, must be unique to each individual, and may not be shared. Shared Authentication: when approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved in writing at least annually.

Access to public and shared resources may be excluded from access control requirements.

**Separation of Duties (SOD)**

The separation of duties principle must be followed when assigning job responsibilities relating to restricted or essential resources. Information System Owners and Data Stewards must maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data, and must avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee’s job duties. A specific periodic review of access rights must be completed to ensure SOD is maintained on enterprise applications such as Banner and Peoplesoft.

**Access Review**

In conjunction with ITS, Information System Owners and Data Stewards must review user access rights to information systems containing protected data every six months. The results of the review must be documented.

**Modifying Access**

Modifications to user access privileges must be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) must have their logical access rights reviewed, and if necessary, modified or revoked within one month after changing positions.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for ensuring that access control is applied to the systems under their authority.

Information System Owners and/or Data Stewards are responsible approving and reviewing all user accounts and access permissions. They also are responsible for maintaining and reviewing permissions to ensure separation of duties.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS User Account Policy and Procedure
2. UWG Controller SOD Review Procedure
3. UWG Bursar SOD Review Procedure
4. UWG Financial Aid Office SOD Review Procedure
5. USG IT Handbook Section 1
6. USG IT Handbook Section 3

**Information Asset Management**
Along with the requirement to maintain an inventory of physical assets as required by the BOR Policy Manual, a list of major software applications and associated hardware assets must include the following:

1. The Information System Owner
2. The Data Trustee
3. The Data Steward(s)
4. The Data Users (user account list)
5. The classification of the system

**Responsible Units**

All directors within the division of Information Technology Services are responsible for maintaining an inventory list of equipment and related information.

The Director of IO and the Director of IS are responsible for maintaining system classification documentation that meets the requirements set out by the IT Handbook.

Information System Owners are responsible for providing a list of Data Stewards and approving and reviewing Data Users

**USG and UWG Associated Policies and Procedures**

1. UWG ITS User Account Policy and Procedure
2. USG IT Handbook Section 5

**Information Systems Acquisition**

Procurement of information technology is governed by state policy, the Department of Administrative Services (DOAS), USG policy, and UWG policy. Approval for desktop systems, tablets, peripherals and certain software application purchases may be granted via the ePro purchasing workflow. Larger systems and software purchases are required to go through the IT Governance process, and may also require USG approval.

**Responsible Units**

All units are responsible for following this section.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS IT Governance
2. UWG Purchasing Guidelines
3. USG IT Handbook Section 4

**Information Security Incident Management and Response**

In order to react quickly and appropriately when an information security event occurs, the organization must have an information security incident response plan. The plan will cover the NIST recommended step of 1. preparation, 2. Detection and analysis 3. containment, eradication, and
recovery and 4. post –action review. Because incident response is a complex activity, the incident response plan must be tested at least once per year and must involve information system owners, as well as the senior campus administration.

**Responsible Units**

All directors within the division of Information Technology Services are responsible for understanding the UWG ITS Incident Response Policy and Plan, and conducting annual tests within their units.

The VP IT/CIO is responsible for ensuring UWG senior management is aware of their role in incident response.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS Incident Response Policy and Procedure
2. USG IT Handbook Section 5

**Physical Access Control**

The physical areas where information assets containing confidential and sensitive data, or PII, must be protected from unauthorized physical access. These physical areas include data centers, office areas and other locations. Information assets which access protected data that are located in public and non-public access areas must be physically secured to prevent theft, tampering or damage.

**Responsible Units**

All directors and staff within the division of Information Technology Services are responsible for maintaining the physical security of their areas.

The Director of Infrastructure and Operations is responsible for maintaining the physical security of the data closets and data centers. A monthly review of access to data closets and data centers must be completed and maintained for audit review.

**USG and UWG Associated Policies and Procedures**

1. UWG ITS Physical Access Policy and Procedure
2. UWG Data Center and Data Closet Access Review Procedure
3. USG IT Handbook Section 5

**Business Continuity Planning**

All units within the university must ensure that they can continue to operate in the event of a disaster that renders their information systems and assets unavailable for an extended period of time.

Business continuity planning is a methodology for restarting the university after a hypothetical severe disaster, assuming that a large percentage of resources have been lost. The end-product of business continuity planning is a roadmap or plan for all identified essential units or functions addressing the issue of how to bring back their operations. A business continuity plan is designed to cover all campus activities that are identified as essential to the restarting of all key university businesses on campus.
Responsible Units
All departments within UWG are responsible for developing business continuity plans.

USG and UWG Associated Policies and Procedures
1. USG IT Handbook Section 3

Disaster Recovery Planning
All departments within the division of Information Technology Services are responsible for developing and maintaining a plan for the restoration of services in the event of a disaster, and in accordance with the campus business continuity plans. The IT DR Plan should outline priorities, recovery time estimates, objectives and procedures for all IT functions. In the case of a catastrophic event that disrupts campus IT services, the plan should provide priorities and strategies for the restoration of hardware, applications and data. The campus business continuity plans should be developed in conjunction with information system owners so that recovery times are clearly understood by all parties.

Responsible Units
All directors within the division of Information Technology Services are responsible for supporting the ITS DR Plan.

USG and UWG Associated Policies and Procedures
1. UWG ITS Disaster Recovery Plan
2. USG IT Handbook Section 3

Periodic Security Assessments and Audits
In addition to audit activities that may be conducted by UWG Internal Audit, USG Department of Audit and the State of Georgia auditors, the ISO will conduct periodic system security audits to determine if the controls in place are effective (NIST 800-171 Security Assessment).

Responsible Units
The UWG ISO is responsible for conducting system security audits every year.
The directors within ITS are responsible for making systems and personnel available to assist with audit activities as well as remediating audit findings.

USG and UWG Associated Policies and Procedures
1. UWG ITS Disaster Recovery Plan
2. USG IT Handbook Section 3
3. NIST 800 - 171

Laws and Compliance
All campus information security practices must comply with a variety of federal and state laws as well as BOR, USG and UWG policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information, including personally identifiable information (e.g., social security number, driver’s license number), personal financial information (e.g., credit card numbers), medical information and confidential student information.

There are many individual laws, regulations and policies that establish our information security requirements. Some of the most notable include:

**Family Education Rights and Privacy Act (FERPA)**

The primary law that governs the privacy of educational information is the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(b).

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing “personally identifiable education information,” such as grades or financial aid information, without the student’s written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers.

Generally, institutions must have written permission from the student in order to release any information from a student’s education record. However, FERPA does allow institutions to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31): 1. School officials with legitimate educational interest; 2. Other schools to which a student is transferring; 3. Specified officials for audit or evaluation purposes; 4. Appropriate parties in connection with financial aid to a student; 5. Organizations conducting certain studies for or on behalf of the school; 6. Accrediting organizations; 7. To comply with a judicial order or lawfully issued subpoena; 8. Appropriate officials in cases of health and safety emergencies; or, 9. State and local authorities, within a juvenile justice system, pursuant to specific State law.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA) 9.5.2**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the rights of patients and participants in certain health plans. In 2000, the federal Department of Health and Human Services adopted copious regulations granting consumers the right to receive written notice of the information practices of entities subject to HIPAA.

Colleges and universities that are affiliated with health care providers are considered covered entities, and participant organizations must provide written notice of their affiliated health care provider’s electronic information practices. Most employer-sponsored health plans also are considered to be “entities” subject to HIPAA. As a result, various compliance obligations are imposed on colleges and universities that sponsor and administer such plans.

HIPAA generally requires covered entities to:

1. Adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed;
2. Require their business associates to protect the privacy of health information; 3. Train their employees in their privacy policies and procedures; 4. Take steps to protect against unauthorized disclosure of personal health records; and, 5. Designate an individual to be responsible for ensuring the procedures are followed.

**Electronic Communications Privacy Act (ECPA) 9.5.3**
The Electronic Communications Privacy Act (ECPA) broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the “contents” of such communications, however, extends only to information concerning the “substance, purport, or meaning” of the communications.

In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students’ network use or of network usage patterns, generally, would not be prohibited by the ECPA, as long as the substance of the communication was not made public.

The ECPA will come into play when an institution is forced to monitor or intercept student, faculty, or employee electronic communications such as e-mail. The effect of the law may depend on the type of person being monitored and the person’s association with the institution, as a student, faculty member, or employee, and whether the communication system is considered a public or private system.

The ECPA also contains specific exceptions allowing disclosures to law enforcement agencies under certain circumstances.

USA Patriot Act 9.5.4

The USA Patriot Act can effect educational institutions in many ways. Probably the most significant effect is that it potentially prohibits institutions from revealing the very existence of a law enforcement investigation. All institutions should ensure that they have worked with their legal staff to produce written procedures on how to deal with law enforcement information requests. Any institution employee faced with a request from law enforcement should follow these procedures.

TEACH Act 9.5.5

The TEACH Act relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use technology materials in educational settings. Institutions that want to take advantage of the relaxed copyright restrictions must limit “to the extent technologically feasible” the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information.

In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

Gramm - Leach - Bliley Act (GLBA) 9.5.6

The Gramm – Leach – Bliley Act (GLBA), enacted in 1999, was largely directed at financial institutions and creates obligations to protect customer financial information. However, it has been determined that colleges and universities are also covered by the act.

The GLBA has two major sections: privacy and security. The Federal Trade Commission’s (FTC) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Therefore, GLBA privacy requirements should not affect educational institutions. They should therefore focus mainly on the security sections of the GLBA.

The information security, or Safeguard, section has five major requirements that a USG participant organization must follow:

1. Designate one or more employees to coordinate the security safeguards; 2. Identify and assess the risks to customer information in each relevant area and evaluate the effectiveness of the current safeguards; 3. Design and implement a safeguards program and regularly monitor and test it; 4.
Select appropriate service providers and contract with them to implement safeguards; and, 5. Evaluate and adjust the program in light of relevant circumstances or the results of testing.

Computer Fraud and Abuse Act (CFAA) 9.5.7

The Computer Fraud and Abuse Act (CFAA) criminalizes unauthorized access to a “protected computer” with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. A participant organization may use this law when there has been a break-in of their computer systems.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. It applies to American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc. International.

Red Flag Rule

Identity theft is defined as a fraud committed or attempted using the identifying information of another person without authority. The risk to the institution and our faculty, staff, students, and other applicable constituents from identity theft and accompanying data loss is of significant concern.

UWG adopts the USG Identity Theft Prevention Standard and Program in an effort to detect, prevent and mitigate identity theft, and to help protect the organization and our faculty, staff, students, and other applicable constituents from damages related to the loss or misuse of identifying information due to identity theft. See the USG IT Handbook Section 5 for complete details.

Responsible Units

All directors within ITS are responsible for understanding the laws, policies and procedures that impact their areas.

All UWG units are responsible for understanding the laws, policies and procedures that impact their areas.

USG and UWG Associated Policies and Procedures

1. UWG Policy 5.3 Payment Card Industry Data Security
2. UWG Procedure 5.3.1 PCI DSS Incident Response Team
3. UWG Procedure 8.3.1 FERPA
4. UWG ITS Compliance Procedure
5. USG IT Handbook Section 5

Policy Enforcement

Consistent with USG policies, the ISO is authorized by the President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the university community.
Division and department leadership must ensure that measures are taken within their areas to comply with this program and its related policies and procedures. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the VP IT. Approved requests will be reviewed annually to determine if an exception is still warranted.

UWG reserves the right to temporarily or permanently suspend, block or restrict access to campus information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of UWG information assets; to protect UWG from liability; or to enforce this policy and its related standards and practices.

Potential violations will be investigated in a manner consistent with applicable laws and regulations, UWG and campus policies, standards, guidelines and practices.

**Responsible Units**

All UWG units are responsible for understanding the policies and procedures that impact their areas.

**USG and UWG Associated Policies and Procedures**

1. USG IT Handbook Section 3

Document Revision History

Creation Jan. 2018

Minor review: July 2019

Next Review: Jan. 2020