ITS Document Number: POL-XXXX

Document Category: Policy
Document Scope: IT Security

Review Frequency: Annual
Review Schedule: 2015

ADDITIONAL DETAILS
See IT Security Plan.

Effective: 2006
Last Updated: 2014

Responsible University Officer:
Chief Information Officer

Document Owner:
Information Security Officer

Document Contact:
Information Security Officer

Summary

Herein contained is the institutional IT security policy for the University of West Georgia.

Content

Institutional IT Security Policy .......................................................... 2
Institutional IT Security Policy

1.0 Introduction

1.1 Purpose
This document is intended to be a framework by which all University of West Georgia (UWG) groups develop standards and procedures to achieve the policies listed below.

1.2 Scope
This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use UWG information technology. All information technology and assets, as defined by the UWG IT Strategic Plan, whether owned, leased, rented or otherwise controlled or maintained by UWG, are subject to this policy.

Authorized users accessing UWG information technology resources and/or the UWG data network, whether on campus or off, are responsible for ensuring the security and integrity of the system(s) used to access the resources. Use of UWG information technology constitutes an acceptance of this policy.

1.3 Directions
Each unit is responsible for complying with security policies and standards contained within this security document.

2.0 Policy Development, Documentation, and Review

2.1 Security Policies Development
UWG will develop and maintain a security policy and security standards and procedures that are appropriate to UWG’s organization and mission in order to comply with Board of Regents Policy 1.3 and the University System IT Handbook. The following guidelines will be used to ensure that the security policy and security standards and procedures are in place.

2.1.1 Obtaining Support
It is the responsibility of the President of the University to “ensur(e) appropriate and audit(able) security controls are in place on his/her campus.” (BOR Policy 11.3.3) The President will obtain a commitment from senior management to enforce the security policy. Working relationships between entities will be established to foster communication and enforcement of the security policy, standards and procedures. An approval process will be established for all security policies, standards and procedures.
2.1.2 Conducting Research
UWG will conduct research that will identify successful practices, experiences, and ideas that will produce appropriate and effective security policies, standards and procedures.

2.1.3 Classifying Standards Policies and Plans
Each security standard will fall into one of three types:

A. Program Policies
Program standards address overall IT security goals and typically apply to all IT resources within the institution. Program standards shall comply with existing laws, regulations and state and federal policies, and support and enforce the institution’s mission statement and organizational structure.

B. System-specific Policies
System-specific standards address IT security issues and goals of a particular system.

C. Issue-specific Policies
Issue-specific standards address particular IT security issues. Examples of issue-specific standards include but are not limited to Internet access, installation of unauthorized software or equipment, and sending/receiving email attachments.

2.1.4 Establishing Periodic Review Process
UWG will perform periodic reviews of security standards to determine if current rules and practices are effective and adequate.

2.2 Security Policies Documentation
UWG will document all security policies, standards and procedures to ensure the integrity, confidentiality, accountability, and availability of information is not compromised. Each IT security standard’s documentation will adhere to the following guidelines:

2.2.1 Defining Standards
IT security standards will consider the following guidelines:
- Identify general areas of risk
- State generally how to address the risk
- Provide a basis for verifying compliance through audits
- Outline implementation and enforcement plans
- Balance protection with productivity

2.2.2 Classifying Standards Policies
Each IT security standard will be identified as program, system-specific, or issue-specific as outlined in section 2.1.3. Based upon the class of standard
the documentation of the standard will follow the appropriate outline identified by the OIIT Template.

2.2.3 Defining Additional Guidelines
Each IT security standard will consider each of the following items:
• Maintaining security guidelines
• Enforcing standards
• Identifying standard exceptions

2.3 Security Policies Implementation
UWG will implement security standards and procedures that are appropriate for the institution and its mission. Security standards and procedures will be disseminated appropriately to create and maintain awareness across the university community.

2.4 Policies Review and Evaluation
UWG will review IT security standards and procedures periodically and will submit IT security standards and procedures to the University System of Georgia office of Information Technology Services for review as necessary.

3.0 Organizational Security

3.1 Information Security Infrastructure
UWG will develop and maintain an internal information security infrastructure to ensure the confidentiality, availability, accountability and integrity of information assets.

The steps for securing the information infrastructure include but are not limited to:

3.1.1 Managing Information Security
UWG will define and create organizational roles for information security. These will include forming, reviewing, and approving campus information security, maintaining internal threat assessments, overseeing investigations of security related incidents, and overseeing business issues regarding new security initiatives.

3.1.2 Coordinating Information Security
The President of University shall be responsible for ensuring appropriate and auditable security controls are in place.

President’s Advisory Committee members will be responsible for:
• Informing personnel of UWG policies on acceptable use of information assets.
• Ensuring that application development IT personnel under their supervision comply with these policies and procedures.
• Ensuring that non-university contract personnel under their supervision comply with these policies and procedures.

Vice President for Student Affairs and Enrollment Management will be responsible for:
• Informing current and new students of UWG policies on acceptable use of information assets.
• Ensuring that students comply with UWG policies, standards and procedures.

System Administrators will be responsible for:
• Monitoring security integrity of information assets.
• Maintaining and ensuring data backups of critical electronic information.
• Promptly reporting suspicious activity or occurrence of any unauthorized activity to the Information Security Officer and Chief Information Officer.

The UWG Information Security Group will be responsible for:
• Retaining the UWG’s IT security policies, standards and procedures.
• Developing and disseminating awareness and training materials.
• Assuring compliance through auditing.
• Reporting compliance audit findings to UWG’s Chief Information Officer and the University’s Department of Internal Audits.

All faculty, staff, and students will be responsible for:
• Abiding by official UWG policies on acceptable use of information assets.
• Promptly reporting suspicion of or occurrence of any unauthorized activities to the Chief Information Officer.
• Any use made of their accounts, logon IDs, passwords, PINs and tokens.

The Chief Information Officer will be responsible for:
• Ensuring the availability, integrity and confidentiality of the UWG’s information assets.
• Assuring that violations are addressed according to this policy document.

3.1.3 Allocating Responsibilities
Each unit is responsible for creating and maintaining system-specific standards and procedures to supplement program level standards to ensure the security and availability of IT resources.

3.1.4 Authorizing information processing facilities
UWG will address the following issues when creating new information processing facilities:

- Assess the ability of the new facility to conform to existing security standards, including any state, federal, Board of Regents, or institutional requirements
- Evaluate hardware and software compatibility of the new facilities with existing facilities
- Evaluate the need for additional security measures and the impact of personal computing systems

3.1.5 Assessing Third-parties

UWG will address all relevant security issues when contracting with third-parties and will ensure third-parties comply with all IT security standards including disciplinary actions. All third party access to campus computer systems and networks should be reported to ITS.

3.2 Third-Party Access Risk Management

UWG will conduct risk assessments, identify risks, and develop security procedures to control third-party access. Controlling access will include creating user profiles, educating on-site, third-party users about institutional policies, standards and procedures, and implementing tight controls on third-party user accounts using remote access.

3.3 Third-Party Contracts

UWG will identify all IT security issues associated with contract work and develop security procedures specifically tailored to the contract work. The following criteria will be considered when developing security procedures.

- Access Control
- Asset Protection
- Services Management
- Liabilities Management
- Compliance Management
- Equipment Security
- Personnel Management

4.0 Asset Classification and Control

4.1 Asset Inventory

UWG will maintain documented inventories to account for all hardware and software purchased by the University. Assets will be inventoried in compliance with all applicable asset management policies, including Article 6 of Chapter 9: Georgia Computer Systems Protection Act, Title 16 from the Official Code of Georgia annotated. Inventory lists will be updated in accordance with institutional asset management procedures.
4.2 Asset Classification
UWG will classify its information assets to determine which assets constitute the critical information infrastructure of the institution. The classification of assets will be accomplished through the following steps:

• Organize assets
• Review relevant information
• Conduct interviews and surveys
• Identify interdependencies
• Classify assets

4.3 Risk Analysis
UWG will identify and document the vulnerabilities and risks associated with its critical assets. The guidelines for analyzing risk to critical IT assets are:

4.3.1 Defining Areas of Control
UWG will ensure operational objectives are achieved, undesired events are detected and prevented, and ensure no single individual controls all key aspects of IT operations.

4.3.2 Identifying Critical Asset Support Elements
UWG will identify support elements that will ensure critical assets continued, successful operation.

4.3.3 Defining Areas of Potential Compromise
UWG will review any factor(s) that pose a potential risk to critical IT assets and will compile a list of threats and vulnerabilities that can affect critical IT assets.

4.4 Risk Assessment
UWG will perform periodic risk assessments.

5.0 Personnel Security

5.1 Employment Hiring Practices
UWG will screen, educate, and train employees who will be granted access to UWG information systems.

5.1.1 Screening Potential Employees
UWG will implement screening procedures for potential employees who will be granted access to UWG information systems. Re-screening will be performed if there is cause for doubt or concern or in cases of job change, role change, or promotion.

5.1.2 Disseminating Employee Responsibilities
UWG will ensure that all newly hired employees will be informed of their responsibilities regarding accessing sensitive institutional information. All newly hired employees will be notified of the terms and conditions of their employment regarding information security issues and may be required to sign confidentiality and non-disclosure statements.

5.1.3 Evaluating the Duties of New Employees
UWG managers and supervisors will implement procedures to evaluate the duties of provisional personnel who access sensitive information. These procedures should be reviewed and updated as necessary.

5.2 Acceptable Use of Technology
UWG will insure the appropriate use of its information assets as outlined in the Acceptable Use Policy (AUP). The AUP will define appropriate and inappropriate use of technology and enforcement of the policy.

5.3 User Training
UWG will provide information security training to its faculty, staff, and students. Completed training will be documented.

5.4 Security Incidents
UWG will implement procedures for reporting and handling information security incidents.

5.4.1 Reporting Incidents
UWG will maintain and update procedures for faculty, staff, and students to report breaches of security incidents to the appropriate personnel.

5.4.2 Managing Security Incidents
UWG will utilize its current Incident Response process to:
- Log and track incidents
- Collect and analyze data
- Contain incident
- Utilize escalation procedures
- Resolve incident
- Recover and restore systems
- Report incidents to management and outside agencies as necessary
- Analyze logs periodically

5.5 User Awareness and Responsibilities
UWG will enhance user awareness of security vulnerabilities or threats to UWG information and communication systems through user education.

5.6 Disciplinary Process
UWG will use existing disciplinary bodies to ensure fair and equitable treatment of persons suspected or found to be in violation of UWG policy or standards. This process applies to all UWG faculty, staff and students, in addition to any authorized guests as identified by the AUP.

6.0 Physical and Environmental Security

6.1 Physical Perimeter and Facilities
UWG will prevent and detect unauthorized access or damage to facilities that contain UWG information assets. UWG will ensure that the documentation of the physical infrastructure remains confidential and that all critical areas are equipped with fire, water, and physical intrusion alarm systems.

6.2 Physical Entry to Restricted Areas
UWG will restrict access to areas that house sensitive or critical UWG information assets.

6.2.1 Issuing Institution Identification Badges
UWG will implement a badge system where appropriate, maintain entry logs, and review and update access rights in restricted areas periodically.

6.2.2 Restricting Physical Access
UWG will review and update access rights to restricted areas periodically and will allow only authorized personnel access to UWG work areas containing sensitive information.

6.2.3 Securing Sensitive Information
UWG will secure sensitive information, either in print or electronically stored, from unauthorized access and disclosure.

6.2.4 Inspecting Luggage and Packages
UWG reserves the right to inspect user’s luggage and packages as necessary to safeguard and deter theft of sensitive equipment and information.

6.3 Equipment Sites
UWG will secure production systems and assure continuity by training users about their responsibility to protect equipment and by providing security controls that alert, monitor, and log threats.
6.4 Power Supplies
UWG will ensure that critical equipment and information systems shall have an appropriate, protected, consistent, and continuous supply of power to ensure continued, successful operation.

6.5 Equipment Re-Use or Disposal
UWG will ensure equipment or media containing institutional information will be rendered unrecoverable prior to re-use or disposal. UWG will ensure that disposal of equipment or media will be done in accordance with all applicable surplus property and environmental disposal laws, regulation, or policies.

7.0 Operations Management

7.1 Operational Change
UWG will develop and implement change management procedures for information processing facilities, systems, software, and operational procedures.

7.2 Network Controls
UWG will institute controls to ensure the security of the network in order to protect information and all services from unauthorized access.

7.3 Development and Operation Facilities
UWG will separate production computing environments from development and test computing environments to reduce the risk of one environment adversely affecting the other.

7.4 External Facilities Management
UWG will establish contractual controls to reduce security risks from external contractors that manage information processing facilities.

8.0 System and Software Management

8.1 Information and Software Exchange Agreements
UWG will have written agreements with external organizations prior to the exchange of institutional information. The agreement will exist whether the information is in electronic or physical form and shall comply with any state, federal, Board of Regents, or institutional law or policy. The content of the agreement(s) will vary depending on the reason for the exchange. Institutional procedures for exchanging information or software shall consider: Assigning responsibilities for transmission, dispatch, and receipt Implementing minimum technical standards for packaging and transmission
Assigning responsibilities for software data protection, copyright compliance, and similar considerations
Implementing extra controls for sensitive items as necessary

8.2 Electronic Mail Security
UWG will implement standards and procedures that will comply with state, federal, Board of Regents, and institutional electronic mail security regulations.

8.3 Publicly Available Systems
UWG will provide access to its publicly classified institutional information in accordance with the safeguards used to protect UWG resources.

8.4 Electronic Commerce
UWG will implement safeguards to ensure the security of electronic commerce.

8.5 System Capacity
UWG will monitor current and anticipate future system capacity requirements to ensure systems meet institutional mission and goals. Capacity considerations shall include:
- Processing power
- Bandwidth
- Storage
- Communication systems
- Updates/Upgrades/Patches

8.6 System Acceptance
UWG will define and document necessary system acceptance criteria for information systems. UWG will test and document all new or upgraded information systems according to the system acceptance criteria in order to avoid system failures.

8.7 Malicious Software
UWG will use prevention and detection controls and create security awareness to protect information systems and services against malicious software.

9.0 Information Management

9.1 Information Handling
UWG will ensure appropriate handling, storage, and security of media that contain sensitive, confidential, or vital information to provide security, confidentiality, integrity, and availability of information.

9.2 Media Disposal
UWG will render information unrecoverable before disposing of media. Procedures shall include identifying sensitive media, disposing of paper media, cleansing magnetic or optical media, and developing disposal procedures.

10.0 Back-Up Procedures

10.1 Back-Up Procedures Development
UWG will back-up all critical, electronically-stored data. The back-up system, media, and restoration procedures will be tested regularly to ensure that data can be recovered following a system failure or disaster.

10.2 Activity Logs
UWG will maintain appropriate activity logs for critical information systems and develop procedures to review the logs regularly.

10.3 Fault Logs
UWG will maintain fault logs to trace system activity and errors and implement automated logging whenever possible.

10.4 Disaster Recovery and Operational Continuity
UWG will ensure that it can continue to deliver essential functions of information systems in the event of an emergency or disaster.

10.4.1 Assessing the Risks and Impacts of an Emergency or Disaster
UWG will assess the risks and determine the priority of the restoration of information assets based on the importance and sensitivity of the asset(s).

10.4.2 Developing Operational Continuity
UWG will utilize operational continuity plans to ensure the university’s objectives and priorities are met. The operational continuity plans shall be periodically reviewed.

11.0 Documentation

11.1 Security Policies, Procedures, Plans, Guidelines, and Standards
UWG will document all security policies, standards, and procedures and ensure that they are disseminated to appropriate managers and users.
11.2 Operating Procedures
UWG will document operating responsibilities and procedures for UWG information processing facilities. Operational procedures shall include operating functions and system maintenance.

11.3 Operations System Documentation Security
UWG will secure operational system documentation from unauthorized access or disclosure.

12.0 Access Control

12.1 Access Control Policy
UWG will control access to information systems. All sensitive UWG information will be protected from improper disclosure, modification, and deletion.

12.1.1 Managing Privileges
UWG will identify the authorities responsible for critical and sensitive systems. These authorities in turn are responsible for the management of the privileges of the users and the administrators of the systems.

12.1.2 Managing Access Authorization and Restrictions
UWG will ensure only authorized users gain access to institutional information systems based on their level of authorization. Access controls will include remote access users and third parties. UWG will audit its systems to monitor the activity of system users.

12.2 Password Management
UWG will maintain password management procedures pursuant with its Acceptable Use Policy.

12.3 Networks and Systems
UWG will control access to its networks, systems, and resources to ensure only authorized users gain access based on their level of authorization.

12.4 System Utilities
UWG will maintain procedures to ensure that system level utilities are secure, segregated, and limited to authorized system administrators.

12.5 Network Connection Times
UWG will maintain controls to manage network resources. These controls include but are not limited to bandwidth usage, time and date limitations, connection control, etc.
12.6 System Access Monitoring
UWG will monitor connectivity to institutional systems. The monitoring process will include:
• Assessing the risk of unauthorized use
• Monitoring system use
• Maintaining and reviewing system events

12.7 Remote Access Management
UWG will manage remote access to its network, systems and their resources. Management of remote access will consider:
• The risk of remote access
• The Benefits of telecommuting
• User training

13.0 Systems Development and Maintenance

13.1 Security Requirements
UWG will ensure that all system development and maintenance adhere to existing security requirements. Business requirements for system development will specify and define the necessary system controls based on existing policy.

13.2 Cryptographic Techniques
UWG will implement cryptographic techniques for sensitive systems as needed.

13.3 Change Control Procedures
UWG will develop change control procedures before upgrading or changing operating systems and software to avoid security risks and service disruptions.

14.0 Compliance

14.1 Legal Requirements
UWG will comply with federal, state, Board of Regents, and institutional information security regulations, develop acceptable usage policies, and conduct security awareness training for all users.

14.2 Security Policies and Technical Compliance Review
UWG will periodically review documented policies, procedures and operations to ensure compliance with state, federal, Board of Regents and institutional
security requirements. The review process shall include security and technical compliance.