University of West Georgia Information Technology Security Plan

TABLE OF CONTENTS

Section I
Executive Summary

Executive Summary

The University of West Georgia's information technology resources are valuable assets that the University has the right and the obligation to manage, protect, secure, and control. University employees, students, sponsors, suppliers, and other affiliates must use these resources for appropriate purposes only, protect access to them, and control them appropriately. Access to networks, computing systems, and electronic data owned or operated by UWG is a privilege that entails responsibilities.

This information security policy follows guidelines provided by the University System of Georgia's Office of Information Technology. It describes how the University will protect its information technology resources and preserve the privacy of the members of the University community, and is binding on all those who use those resources. It is adopted and promoted so that the University can:

1. Fulfill its technology vision "to integrate information technology into West Georgia's academic and administrative mission to ensure that students, faculty, staff, and the community are well prepared for life in a knowledge-based and technologically dynamic society."
2. Identify, assess, and mitigate vulnerabilities and threats that can adversely impact the information assets of the University.
3. Meet its record-keeping and reporting responsibilities as required by state and federal law, the University System of Georgia, and the University administration.
4. Comply with the Family Educational Rights and Privacy Act of 1974 and other statutes and policies protecting the rights of individuals.
5. Maintain data integrity and accuracy.
6. Ensure that authorized individuals have timely, reliable access to IT resources.
7. Deny unauthorized access to IT resources.
8. Determine and maintain accountability for the management and use of IT resources.
9. Ensure the adoption of standards and procedures that implement this policy.
10. Make information about the applicable security laws, regulations, guidelines and policies readily available to all members of the University community.

This policy recognizes that all information technology resources require some degree of security, with the appropriate degree of protection determined by the nature of the resource and its intended use. While no policy can provide for absolute security, it aims to minimize risk while promoting the effective use of technology.

Responsibility for information security lies with the entire UWG community, but ultimate management responsibility rests with the President of the University. The President delegates operational security responsibilities to the Chief Information Officer and to the Vice Presidents of the University whose divisions operate IT units that report to them. The Faculty Senate recommends changes in IT policy to the President, while standards and procedures that implement the strategic policy are developed by ITS. Such standards and procedures, when approved by the President, become by reference part

of this policy, and are also binding on the University community. All such policies, standards, and procedures shall comply with federal and state laws and regulations and with state and University System policies, and shall support the University's mission.

Any sections or subsections in this plan found to be contrary to federal or state laws shall be severed with the remainder of the document remaining in full force and effect.

Section II
Institutional Profile

Institutional Profile

Description

The University of West Georgia is located in Carrollton Georgia and is identified as one of the four institutions that make up the robust tier of State Universities within the University System of Georgia. The University is a 4-year, coeducational, residential university that offers both undergraduate and graduate degrees to over ten thousand students.

The University of West Georgia is comprised of the Graduate School, the School of Nursing, the University Library, and four Colleges: the College of Arts and Science, the Richards College of Business, the College of Education and the Honors College. The College of Arts and Science is the largest academic unit followed by the College of Education, Richards College of Business and the School of Nursing. Approximate faculty for each unit is 269, 90, 47 and 23 respectively.

Information Technology and Information Systems

Like most universities, UWG depends on Information Technology and Information Systems in day-to-day operations.

Information Technology

Information technology is a broad term used to describe a multitude of uses for computing and communications technology in support of an institution's mission and activities. This typically includes computers, networking equipment, telephony, video distribution and transmission equipment, multimedia and similar computer-based audiovisual equipment, electronic or digital printing equipment, and other related hardware.

Additionally, the term information technology may be used to include both software that operates on this equipment and data retained by these hardware and software mechanisms. When considering data, software, hardware and their associated instructional, research or business processes, the term information systems is generally used.

Information Systems

1. A system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information.

2. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

Dependence and Commitment
The University depends on information technology and information systems in day-to-day operations. The University commits significant resources annually to incorporate technological advances into both its academic and operations areas.

The University provides network/Internet access to its faculty and staff via workstations/laptops connected to the campus network. Students are provided network/Internet access and access to various homework/research applications through hundreds of workstations located in multiple labs or freely accessible areas.

A switched network infrastructure provides network connectivity to over 55 academic, administrative, and residential buildings on the campus. The University has numerous servers that provide access for faculty, staff, and students to major IT services such as BANNER, PeopleSoft, Email, and the University web site.

Risks and Protection

Providing access to the network/Internet and to various applications pose a certain level of risk to the University.

The University of West Georgia recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized/malicious network access from “outside” the campus network
- Unauthorized installation of software
- Improperly licensed software
- Loss of data integrity
- Loss of data due to disaster
- Sabotage of data or systems
- Theft of hardware or data
- Unauthorized use of hardware or data
- Carelessness, negligence, or mismanagement
- Damage from environmental conditions

Protecting information technology is a dynamic and ongoing process. New risks develop at an alarming rate and continuously threaten the University’s information resources. To protect users and the University as a whole the University has adopted a Defense in Depth strategy of protection. This approach tries to achieve a balance between protection and cost, performance, and operational considerations of the University’s campus network, servers, and workstations.

Maps

The University maintains various maps to assist visitors and vendors as well as current students and employees in finding their way to and around the University and the University's information technology resources.

Campus Maps

To view the general layout of the Campus and obtain directions to the University of West Georgia please visit: http://www.westga.edu/maps/

Campus Network and Telecommunication Maps

Information Technology Services (ITS) maintains maps of the University's network and telecommunication system. Due to the sensitive nature of these maps they are only made available by ITS on a case-by-case basis and are not available through a public repository.

Roles and Responsibilities

Responsibility for protecting the University's information systems and data is shared by many entities and individuals throughout the University. The following section describes specific roles and responsibilities.

University President

The President shall be responsible for ensuring that appropriate and auditable security controls are in place.

Vice Presidents of the University

Each vice-president has specific outlined job responsibilities for his/her area. These responsibilities are outlined in UWG's policies and procedures.

Chief Information Officer

The Chief Information Officer 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 user oriented.

Technology Planning Committee (TPC)

The purpose of the TPC is to assess and recommend policy and procedures that contribute to the fulfillment of the University's technology vision. That vision is:

> "... to integrate information technology into West Georgia's academic and administrative mission to ensure that students, faculty, staff, and the

community are well prepared for life in a knowledge-based and technologically dynamic society."

Also, based on the charge of the TPC, the committee will:

"produce a Yearly Evaluation of Campus IT, which will include:
An assessment of campus annual reports, area assessments and other documents that provide evidence that the university is actively participating in the strategies articulated in the University Strategic Plan.

An evaluation of existing campus policies related to the allocation and use of technology to ensure that academic and administrative needs are adequately addressed.

A summary of the committee's findings and any recommendations for increased activity to fulfill participation in the IT Strategic Plan and/or recommendations for changes, additions or other improvements to the UWG IT Strategic Plan and accompanying processes."

The TPC consists of a total of 16 members with members representing the Senate and faculty serving for staggered three-year terms.

The membership specified by the Faculty Senate is:

Senate 2 (1 Arts and Sciences, 1 Business or Education); Faculty 6 (3 Arts and Sciences, 1 Business, 1 Education, 1 Library); 4 senior-level administrators (1 each from the divisions of Academic Affairs, Business and Finance, Student Affairs and Enrollment Management, and University Advancement); the Chief Information Officer); Students 3 (Appointed by the SGA).

Information Security Officer (ISO)
The ISO is designated by the Provost & Vice President of Academic Affairs and the 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.

UWG Information Security Group
The UWG Information Security Group (ISG) is made up of the ISO and appointed ITS and non-ITS staff and is responsible for handling first responses to security

issues related to IT resources for UWG. The ISG will work together to provide quick, appropriate responses and remedies to all IT security events.

System Owners and Operators

System owners and operators play a critical role in protecting UWG information systems and data. Their ranks might include members of the University's professional staff, deans, department heads, faculty members, contracted employees, or students.

System owners' and operators' areas of responsibilities for systems and information security include the following:

- Compliance with UWG policies, standards and procedures and statutory and regulatory requirements. (UWG Policies)
- Compliance with UWG guidelines related to physical and environmental security.
- Maintain confidentiality of sensitive data, especially personally identifiable information and valuable intellectual property.
- Grant access to users based on the principle of least privilege.
- Grant access to users based on the principle of separation of duties.
- Submit documented reports to the appropriate authority involving incidents of security breaches.
- Perform incident response activities when incidents involve their system(s).

Data Custodians

Data custodians are individuals who have been officially designated as accountable for specific data that is transmitted, used, and/or stored on a system or systems within a department, college, school, or administrative unit of UWG. The role of data custodians is to provide direct authority and control over the management and use of specific information. These individuals might be deans, department heads, managers, supervisors, or designated staff and may serve in dual roles as a system owner or operator as well as a data custodian.

Data custodians must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability.

Data custodians' responsibilities include the following:

- Ensure compliance with all UWG policies and all statutory and regulatory requirements.
- Provide system owners and operators with requirements for access control measures to protect sensitive data.
- Ensure appropriate disposal of all media on which data is stored at the end of its use.
- Ensure appropriate security measures for transmission of data.

- Support access control of data by acting as a control point for all access requests.
- Submit documented reports to the appropriate authority if there is a possibility of compromise of personally identifiable information.
- Ensure that access is granted based on the principle of least privilege.
- Ensure that access is granted based on the principle of separation of duties.
- Support regular review and control procedures that ensure that all access privileges are current and appropriate.

Data custodians, in conjunction with the system owners and operators are responsible for documenting any requested exceptions to UWG privacy or security related policies. Documented exceptions must be approved in writing by the authorized University officials responsible for the electronic information to which the exception applies. Exceptions will be considered only when warranted and only to the degree necessary to achieve the mission and business needs of the University. Any and all exceptions made must be documented and registered with the appropriate Vice President.

Users

All users have a critical role in the effort to protect and maintain UWG information systems and data. Users of UWG computing resources and data have the following responsibilities:

- Support compliance with all federal and state statutes and regulations.
- Comply with all UWG security, privacy, and usage policies and guidelines.
- Protect against unauthorized access to accounts, privileges, and associated passwords.
- Maintain confidentiality of sensitive information to which they are given access privileges.
- Accept accountability for all activities associated with individual user accounts and related access privileges assigned to them.
- Restrict to authorized purposes the use of UWG computers, email, computer accounts, and networks and the information accessed, stored, or used on any of these systems.
- Report all suspected security and/or policy violations to an appropriate authority (e.g., manager, supervisor, system administrator, etc.).

Users are also required to follow all specific policies, standards, and procedures established by UWG departments, schools, colleges, or business units with which they are associated and from which access privileges have been given.

Organization and Staffing

Information technology support is primarily centralized, and provided by the department of Information Technology Services. Information technology assets are distributed across the University with equipment located within each College or School, within the

Business and Finance Division, under the Chief Information Officer (CIO) and within separate units such as the University Library and Division of Student Affairs and Enrollment Management. An organizational chart for Information Technology is located in the Appendix of this document.

Business & Finance Division
The Business & Finance Division of the University is comprised of the following departments: Budget & Asset Management Services, Business and Auxiliary Services, Campus Planning and Facilities, Human Resources, Internal Audits, Office of the Controller, and University Police. The division is comprised of almost 300 hourly/administrative staff.

The Business and Finance Division is dedicated to giving each customer (student, employee, vendor, community, and individual) assurance that their critical business needs are our main focus by providing the highest quality business processes and services delivered quickly and conveniently in a personal environment by friendly, professional staff employing integrity in every action.

Information Technology is a vital part of the operation of the Business and Finance Division. The Division maintains IT resources for its staff in various forms including desktop and portable computers, printers, other peripheral hardware, and software titles.

The Division relies on ITS for core networking and IT services

College of Arts and Sciences
The College of Arts and Sciences (A&S) is the largest of the three colleges on the campus of UWG and is made up of 16 academic departments, the Writing Center, the Townsend Center for Performing Arts, and the Office of the Dean. The College is comprised of over 269 full and part-time faculty members and over 30 hourly/administrative staff. The College services the core requirements for all undergraduate programs as well as offers 39 undergraduate and 11 graduate degree programs and courses in 13 pre-professional programs.

Information Technology is a vital part of the operation of the College of Arts and Sciences. The College maintains IT resources for the faculty, staff and students in various forms including desktop and portable computers, printers, scanners and other peripheral hardware, classroom and homework labs, departmental labs, and software titles.

The College relies on ITS for core networking and IT services.

Computer Science
To best serve the specialized computing needs of computer science instruction and research, the Department of Computer Science (CS) (an academic department within the College of Arts & Sciences charged with providing degree programs in computer science) operates its own semi-autonomous computing infrastructure. This infrastructure is independent of and separate from the general infrastructure provided by ITS. A collegial and supportive working relationship exists between ITS and CS technical staff, with both groups frequently consulting each other on specific areas of expertise and experiences.

While the infrastructure maintained by CS is essentially autonomous, CS does not act as an independent IT unit. The Department relies on the College and the University for funding of equipment, and utilizes the core campus network as well as various other administrative services provided by Information Technology Services. Additionally, CS faculty and students are not excluded from general-purpose services and facilities provided by ITS (for example, CS faculty routinely teach courses in shared facilities such as lecture halls that utilize technology supported by ITS). Overall, the computing infrastructure maintained by CS is focused on the Department's mission to provide degree programs in computer science and, as such, the Department does not provide or duplicate existing services unless there is a direct contribution to its mission.

College of Education
The College of Education (CoE) is the second largest of the three physical colleges on the UWG campus. It is comprised of seven academic departments, the Dean's Office, Child Development Center, Reading Clinic, Speech-Language Clinic, Teaching Materials Center, Georgia Youth Science and Technology Center, Advising Center and an off-campus program at the Georgia Highlands College. The College is comprised of over 120 full and part-time faculty and staff and offers bachelors, masters, educational specialist, and doctorate level degree programs, as well as post-bachelors certification and alternative preparation opportunities. The College of Education is accredited by the National Council for Accreditation of Teacher Education (NCATE). As well, all education programs are approved by the Georgia Professional Standards Commission (PSC) for recommendation for Georgia professional educator preparation programs. Approximately 2,755 students are currently enrolled in professional education programs provided by the College.

Information Technology is a vital part of the operation of the College of Education. The College maintains IT resources for the faculty, staff and students in various forms including desktop and portable computers, printers, scanners and other peripheral hardware, classroom and homework labs, departmental labs, and software titles.

The College relies on ITS for core networking and IT services.

Division of Student Affairs and Enrollment Management
The Division of Student Affairs and Enrollment Management, as a complement to the academic program of the university, offers a variety of educational services, developmental programs, and student activities designed to enrich the student's university life. The division consists of 16 departments and units.

Every department and unit uses Information Technology to perform their daily operations. Several departments have designated IT functional support positions to assist with daily operations.

Student Affairs Web and Technology's (SAWT) main function is to act as a liaison between Student Affairs and Enrollment Management and IT concerns around campus. In addition, SAWT provides limited technical support to all departments in Student Affairs and Enrollment Management and offers introductory training for Banner to both Student Affairs and Enrollment Management and academic users. On a daily basis SAWT satisfies one-time or unusual requests for student information.

The Assistant Director for Operations in Admissions supports technology as it relates to Banner and Admissions. Tape loads, data loads from GA411, data extracts, population selections, letter generation, data extracts for GoalQuest, and training are just a few of the functions supported. The Data Collection Specialist assists in these functions.

The Technical Assistant in Financial Aid provides technical support which relates to Banner as well as general user support. Some functions like data extracts and letter generation are similar to Admissions. Other functions like FAFSA and awards processing are unique to Financial Aid. This position also supports the department with end-user issues and concerns regarding technology as well as purchases new technology for the department and coordinates with ITS for installation.

Some of these positions do occasional web design and maintenance.

The Division relies on ITS for core networking and IT services.

Information Technology Services (ITS)
ITS is the main provider of IT services and support for the University including all core information technology functions and services. ITS is made up of two major units: User Services (web software development, service desk management, desktop support, classroom support and special events), and Infrastructure Services (Windows and Unix systems administration and hardware support, networking, enterprise application support and telecommunications). The Office of the CIO is responsible for the project management, budget over site and information security functions of ITS.

ITS Core Services

ITS provides core IT services for the entire University and is the primary provider of IT desktop hardware and software support for the University. The core services provided by ITS can be divided into two areas: networking infrastructure and IT services and support. Listed below is a brief list of the ITS's core services. Visit ITS's Service Catalog for a detailed list of ITS's services.

Networking Services

- DNS Administration
- DHCP Administration
- VLAN Administration
- Firewall Administration
- SPAM Filter
- Email Gateway Services
- Telephony Switching and PBX
- Cable Television Contract Management
- Residence Life Network (ResNet)
- Wireless Networking

IT Services and Support

- Active Directory Services
- File and Print Sharing services
- Backup services (server storage only)
- Web services
- Campus Email
- Service Desk (phone/email access)
- Desktop Support
  - Hardware support
  - Software support
- Software License Management
- Audio/Visual Support
- Enterprise Anti-Virus Solution
- Banner Student Information Services
- Student Information Technology Services (SITS)
- Microsoft Campus Agreement (MCA)
- LDAP Authentication
- Listserv

ITS Departmental Applications and Services

In addition to the general IT Services listed above, ITS also support the following departmental applications and services.

- Alumni BlackBaud Database
- Residence Life FileMaker Pro Server
- Alumni Vanity Email Addresses

- Excel Center Acutrack
- RISK Management Chemical Database
- Institutional Research SAS/SPSS
- Financial Aid EdConnect
- Townsend Center Choice Ticketing
- SGA Voting Application

ITS Labs and Public Access

ITS manages multiple open Windows and Macintosh based computer lab environments for students and departments. All computers in the lab environment are networked, protected by antivirus software, and support numerous homework/research related software applications. These lab systems are currently placed in the locations listed below.

- Art Department(3 labs)
- Athletics
- Biology Building
- Career Services
- Chemistry
- Commuter Lounge
- Computer Science (4 labs)
- Excel Center
- Financial Aid
- Foreign Languages
- Geosciences (4 labs)
- Gunn Hall
- Health Center
- Honors House
- Learning Support Testing Lab
- Library (3 Labs)
- Math
- MIS
- Music
- Radio
- Registrar's Office
- Richards College of Business (4 labs)
- School of Nursing
- Sociology
- The College of Education (5 labs)
- The Technology Enhanced Learning Center (8 Labs)
- Theatre
- UCC Surf Center
- University Community Center Lab (UCC)
- Wolves Den Surf Center

Newnan Campus
The University of West Georgia's off campus site in Newnan offers two undergraduate degree programs, six graduate degree programs, and a selection of the core courses required for most undergraduate degrees. When available, the Newnan campus also rents rooms to community groups and organizations for training purposes. The campus is supported by 8 staff members and over 50 faculty members each semester. Over 1,000 students pass through the campus every academic year.

Newnan ITS manages one open computer lab for student use and two classroom computer labs. All computers in the labs are Windows based, networked, protected by anti-virus software, and support Microsoft Office 2007 and other necessary homework/research related software applications. Newnan ITS also maintains desktop and laptop computers for staff and faculty (including instructor stations), printers, scanners, and other instructional technology. Newnan offers the following support services for faculty, staff, and students:

- Active Directory Services
- File Sharing and Print Services
- Backup Services (Server storage only)
- Web Services
- Hardware/Software Technical Support
- Audio/Visual Hardware Support
- Computer Lab Management
- SITS (student technical support)

Richards College of Business
The Richards College of Business (RCOB) at the University of West Georgia is composed of four academic departments, the Small Business Development Center and the Center for Economic Education. The RCOB employs 54 full and part-time faculty and 13 administrative and hourly staff. The RCOB is accredited by The Association to Advance Collegiate Schools of Business International (AACSBI) and offers twelve undergraduate degree programs and five graduate degrees.

Information technology plays a strategic role in the RCOB's mission. The Richards College of Business maintains resources for students, faculty and staff that includes desktop and laptop computers, printers, scanners and other peripheral hardware in classrooms, classroom and homework labs, and faculty and staff offices.

The College relies on ITS for core networking and IT services.

University Library
The library is the most important learning center on any campus. Library services provided at Irvine Sullivan Ingram Library are among the most advanced in the state of Georgia. The Library's participation in the University System of Georgia's

GIL (Georgia Interconnected Libraries) project provides automated services for its patrons. Circulation, reserves, interlibrary loans, Special Collections, government documents, and serials are available through the library's World Wide Web homepage and its online public access catalog (OPAC). The Library's homepage contains an electronic suggestion board, and all patrons are encouraged to provide input. The Library's catalog and home page are available throughout the world to anyone with Internet access. Library users - students, faculty, or the public - have access to GALILEO (Georgia Library Learning Online). GALILEO includes the catalogs of all system libraries and full-text, searchable electronic journals and encyclopedias.

The Library provides a wide range of additional electronic resources to its students and faculty, with web-based indexes to all electronic materials. All licensed, electronic materials are available to University students and faculty from any computer in the world with an Internet connection. Students and faculty have circulation privileges at the other thirty-four University System of Georgia Libraries; the Library also provides access to the research libraries of the Atlanta area through West Georgia's membership in ARCHE - the Atlanta Regional Consortium for Higher Education. For students or faculty who require additional materials, electronic generation and transmission of interlibrary loans expedites this process considerably. The Library pursues an aggressive instructional program. The Library offers a for-credit course in a computer enhanced classroom or over the web, and it provides orientation presentations to classes and customized instruction on library resources for upper-division courses. It maintains traditional library reference service with library faculty on duty. Off-campus Library Services ensure that students enrolled in courses at the University's remote class sites receive the same level of library support as those at the Carrollton campus. Fax and courier services provide timely delivery to these sites. Reserve reading materials can be transferred to a library near the class site and Joint Borrowers' Cards are routinely issued to off-campus students.

Irvine Sullivan Ingram Library does not neglect traditional library services to students, faculty, and community members that visit the library in person. The Library presently contains seminar and conference rooms, lockable faculty carrels, hundreds of individual study carrels, facilities and equipment for microform reading and copying, the Annie Belle Weaver Special Collections Room, large areas for reference, periodical materials, maps, and the circulating book collection. Audio and video cassette players and photocopiers are also available to assist students and faculty with their study and research needs. The four-story structure provides more than 85,000 square feet of usable research/storage area and over 1,000 seating spaces for students and faculty.

Irvine Sullivan Ingram Library presently houses approximately 397,169 bound volumes, 24,447 reels of microfilm, a limited audiovisual collection, more than 1,143,479 pieces of microforms, 20,697 maps and charts, and 29,882

volumes/pieces and 348 linear feet of manuscript materials in special collections. The Library currently subscribes to 1101 paper magazines and newspapers. It is the Sixth Congressional District selective depository for over 198,134 United States government publications.

Ingram Library Systems

Irvine Sullivan Ingram Library incorporates appropriate technology to automate most of the services it provides. The Library has purposely shifted its collection of research databases from earlier CD-ROM technology to Web-based access. The Library is a participating member of Georgia Libraries Learning Online (GALILEO) and Georgia Interconnected Libraries (GIL). GALILEO provides students with a wealth of research databases, full-text articles and books, and other resources crucial to conducting academic research. GIL is a statewide automation system that provides students with a means to search Ingram Library's catalog of local resources and to search the collections of all other GIL participants. As such, GIL constitutes a single search interface to the University System's union catalog. In addition, GIL is a means by which the Library's patrons can initiate requests for items held by any USG library. The current status of this project can be obtained from the GIL site at (http://gil.usg.edu). In addition to those resources provided by GALILEO, Ingram Library purchases research databases and products that support the University's curricula.

The Library is active in pursuing cost-effective technologies to manage and provide access to its services. In close coordination with UWG Information Technology Services, the library implements state-of-the-art automation making virtually all Library interactions available to its patrons through online tools. Ingram Library provides access to its online resources whether the user is on-campus or off-campus.

The Library Systems Committee (LSC) participates in the planning and implementation of all automated systems in the Library. The committee serves as an advisory group to the Library's administration and the Systems Librarian, recommending policies and procedures related to automation. LSC serves primarily as a forum for discussing and solving problems as they affect the whole Library. To that end it may review proposals and make recommendations for automation; review budget proposals for hardware and software; advise division and department heads, as needed, in the implementation of and training for automated systems; and develop and update long-range automation plans. In the process of its activities, LSC makes planning decisions that affect the technology-supported research resources in use by the entire campus community.

The Library currently makes use of the following systems:

- Library Campus Website
- GALILEO: Research Resources
- GIL: Integrated Library System

- EZproxy Remote Access Proxy
- ILLiad and Ariel Interlibrary Loan Systems
- Docutek Course Reserves
- SFX Resource Link Server
- LibGuides CMS for Libraries
- Libraryh3lp Chat Service
- Windows Domain

Section III
Relevant Laws and Institutional Security Policies and Standards

Relevant Laws and Institutional Security Policies and Standards

Introduction

There is no single, comprehensive set of federal laws mandating either specific privacy practices or information security measures of colleges and universities. Depending on the particular institution and the nature of the activity at issue, institutions may be required to comply with any number of potentially applicable federal laws and regulations. The list of relevant acronyms is daunting: FERPA, HIPPA, ECPA, and CFAA are just a few of the federal laws that include obligations applicable to educational institutions. Both the USA PATRIOT Act and the recent TEACH Act also have electronic privacy and security implications.

Federal Laws

Family Education Rights and Privacy Act (FERPA)
One of the most significant, current risks under FERPA is that the number of electronic records created by or relating to students that are stored in college and university databases on servers has increased exponentially, increasing in turn the number of potential "educational records" that must be protected. Deciding what constitutes an educational record subject to FERPA, therefore, is increasingly complex in the current technological environment. This ambiguity, combined with the proliferation of electronic records and the need to protect against unauthorized disclosure, threatens to significantly increase the costs and risks of exposure for security breaches.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Colleges and universities that are affiliated with health care providers are considered covered entities and 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, educational institutions may be obligated to comply with HIPAA in connection with a broad range of activities.

Electronic Communications Privacy Act (ECPA)
Unlike FERPA and HIPAA, which are specific to certain types of entities, the 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 such communications. As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA. Thus, an institution's right to monitor electronic communications, or its obligation or ability to comply with a law enforcement request, may vary depending on whether the user in question is a student, an employee, or a member of the public.

Computer Fraud and Abuse Act (CFAA)
The 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.

USA PATRIOT Act
The USA PATRIOT Act also amends the portion of the national Education Statistics Act of 1994 (NESA) that specified that data collected by the National Center for Education Statistics (NCES) may only be used for statistical purposes. The amended NESA now permits the attorney general to petition a judge for an ex parte order requiring the Secretary of the Department of Education to provide data from the NCES that are identified as relevant to an authorized investigation or prosecution concerning national or international terrorism.

Another significant impact of the USA PATRIOT Act is its mandate to the INS requiring the INS to develop and implement the Student and Exchange Visitor Information System or "SEVIS". SEVIS is an Internet-based system that will allow schools to transmit information on foreign students to the INS for purposes of tracking and monitoring. The system will compile students' personally identifiable information including the admission at port of entry, academic information and disciplinary information, which must be maintained and updated for the duration of a student's stay in the United States.

TEACH Act
The TEACH relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings. But the new law carries with it obligations that have privacy and security implications: 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.

Among other things, institutions may be confronted with claims under the Digital Millennium Copyright Act (DMCA) if their users attempt to defeat the technological restrictions employed by digital rights management tools. The DMCA makes it unlawful to circumvent technological measures that effectively control access to protected works.

Gramm-Leach-Bliley Act (GLBA)
The GLBA is applicable to financial institutions, including colleges and universities, and creates obligations to protect customer financial information. The GLBA includes requirements to take steps to ensure the security of

personally identifying information of financial institution customers, such as names, addresses, account and credit information, and Social Security numbers. The Federal Trade Commission's (FTC's) 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. Nevertheless, educational institutions likely remain subject to the security provisions under the GLBA and the FTC's implementing rules.

State Law

Georgia Computer System Protection Act

The "Georgia Computer Systems Protection Act" is an act enacted by the 1991 Georgia General Assembly and signed into law by the Governor effective July 1, 1991 which repealed and replaced an act having the same name enacted by the 1981 Georgia General Assembly and signed into law by the Governor effective July 1, 1981. This act establishes certain events involving computer fraud or abuse as crimes punishable by defined fines or imprisonment or both. A modification to this act, HB 1630, was passed by the 1996 session of the Georgia General Assembly.

HB 1630 amends the Georgia Computer Systems Protection Act, thus making it unlawful for any person or organization knowingly to transmit certain misleading data through a computer or telephone network for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank; and for other purposes.

For further information regarding these acts, please visit:
http://www.usg.edu/oiit/policies/proact.phtml
http://www.usg.edu/oiit/policies/hb1630.phtml

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) IT 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 IT unit is responsible for complying with security policies and standards contained within this security document.

1.4 OIIT Template

This document was created based upon the Office of Information and Instructional Technology (OIIT) Information Technology Security Guidelines approved by the Board of Regents in April 2004 referred hereafter as the OIIT Template. This document does not include the detail that the original OIIT Template includes. The OIIT Template should be referenced for further detail regarding the intent or type of information needed to fulfill a policy.

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 712.03b. 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 auditable security controls are in place on his/her campus." (BOR Policy 712.03a) 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 OIIT 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 and Data Custodians 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 IT 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.

Acceptable Use Policy

1.0 Purpose
The purpose of this policy is to outline the acceptable use of computer and network equipment at the University of West Georgia. This policy is in place to protect the employees and students of the University of West Georgia. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 Scope
This policy applies to all University of West Georgia faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that is capable of being connected to or transmitting data on the campus data network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by university employees and students, and other authorized users. Authorized users accessing university computing resources and the university data network from off campus sites through dial- up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.
Use of the University's computing and network resources constitute an acceptance of this policy.

3.0 Availability
These policies are freely available to everyone. Printed copies are available from Information Technology Services. Copies may also be obtained in both PDF and HTML formats, from the web at http://policy.westga.edu. Adobe Acrobat reader is required to use the PDF format, and is freely available at http://www.adobe.com.

4.0 Access and Use
Access and use of University of West Georgia computing and networking resources is regulated by this policy, the University of West Georgia policies, and other applicable local, state, and federal policies.

4.1 Authorized Users
Individuals who have been granted and hold an active and authorized account on a University of West Georgia computer or network or who access and use a University of West Georgia computer or network and abide by this policy are considered authorized users. Any currently enrolled student or employee may be an authorized user of University West Georgia computer or network resources. Accounts and the files associated with that account are deleted upon termination of employment or when a student is no longer enrolled. Student accounts are deleted after the drop/add period for the current term. Graduating students may continue to use their account for six months after graduation.

4.1.1 Authorized Use

Authorized use is that which is consistent with the academic, research and service goals of this institution and falls within the guidelines of this policy and the policy of the Board of Regents which states that property owned by the institution shall be used only for institutional purposes. According to Section 712.01 of the Board of Regents of the University System of Georgia Policy Manual all computer and computer related resources are recognized as "valuable state assets" and therefore, property of the State of Georgia. Only people who have permission shall use such state assets. Furthermore, Georgia Code 16-9-93 G makes using a computer without permission an act of theft:

(a) Computer Theft. Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

(2) Obtaining property by any deceitful means or artful practice;

or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property

shall be guilty of the crime of computer theft.

4.2 Privileged Users

Privileged users are authorized users that have administrative, special, or trusted access to the campus data network and campus computing resources including network devices, servers, student, faculty, and staff information systems and other systems that may contain sensitive data or information. Privileged users will maintain due diligence in carrying out day-to-day duties to prevent the loss of confidentiality and integrity of sensitive information and data.

4.3 Inappropriate Use

The following behaviors are considered a direct violation of this policy: harass, threaten or otherwise cause harm to a specific individual(s), whether by direct or indirect reference; impede, interfere with, impair or otherwise cause harm to the activities of others, to include the introduction of virus(s) onto the network or a computer; download or post to university computers, or transport across university networks, material that is illegal, proprietary, in

violation of university contractual agreements or is otherwise damaging to the institution or individuals.

4.4 Unauthorized access

Users shall not attempt to guess or break another user's password. Attempting to gain access to University of West Georgia computers and networks to which you are not authorized is prohibited. A user may not use University of West Georgia computers to login or attempt to login to computers external to the University of West Georgia to which they are not authorized. It is a violation of this policy to read, alter, delete, or to change ownership or permissions of any other person's computer files, directories, or folders without proper authorization. This policy is applicable even if the system's operating system and/or security measures permit these acts. This also constitutes an act of "computer trespass" and is a violation of Georgia Code 16-9-93 G which states:

"Computer Trespass: Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data;

or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists

shall be guilty of the crime of computer trespass."

If you suspect that your computer or system account has been compromised, and that your files have been tampered with you should contact Information Technology Services.

4.4.1 Unauthorized monitoring

Unauthorized monitoring of data or traffic on any network or system is expressly forbidden. Users shall not attempt to probe, scan, sniff, or test the vulnerability of a system or network without the express written permission from the university's Chief Information Officer.

4.5 Providing services

Users are not permitted to provide network or computer-based services using the University of West Georgia computers or networks without prior

permission from the department responsible for the computers or networks in question. Examples of such services include, but are not limited to, FTP, WEB, IRC and peer-to-peer file sharing.

4.6 Sharing Passwords and Access
It is a violation of this policy for authorized users to share passwords, PINs, or any other means of access to the campus data network or campus computing resources.

Unauthorized disclosure of passwords is a violation of Georgia Code 16-9-93 G which states:

> Computer Password Disclosure: Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

4.7 Disruption of service
It shall be a violation of this policy to deliberately use a computer, laptop, or other device to disrupt or damage the academic, research, administrative, or related pursuits of another. Furthermore, such actions constitute an act of "computer trespass" according to Georgia Code 16-9-93 G:

> (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data;
>
> or
>
> (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists

shall be guilty of the crime of computer trespass."

5.0 Harassment
The following acts constitute computer harassment if the actions are sufficiently severe, pervasive, or persistent so as to interfere with or limit the recipient's ability to work or to participate in or benefit from the services, activities, or opportunities offered by UWG: (1) Deliberately using a computer to harass, annoy, terrify, intimidate, threaten, or offend another person by transmitting obscene language, photographs, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) Repeatedly attempting to communicate with a recipient after the recipient has given

reasonable notice that he or she does not desire such communication.

6.0 Privacy Issues

The University of West Georgia cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made. Users should not place confidential files or information on computers or transmit confidential files or information through the University of West Georgia network system.

6.1 Invasion of Privacy

Use of a computer to invade or threaten the invasion of the privacy of anyone is prohibited.

Georgia Code 16-9-93 G states:

> Computer Invasion of Privacy: Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

7.0 Legal Requirements and Institution Polices

Users of University of West Georgia computers and network systems are expected to abide by State and Federal laws that apply to the use of computers and computer resources. Users are also expected to abide by any institutional policies that apply to appropriate and ethical use of University of West Georgia computers or computer resources. This policy has been written and published in an attempt to make users aware of certain laws that apply to the usage of computers and computer resources. The Georgia Computer Systems Protection Act establishes certain acts involving computers as criminal and punishable by fines and/or imprisonment.

7.1 Individual Responsibilities and Expected Behaviors

Users of the University of West Georgia computer equipment and network systems are expected to understand this policy and abide by it. This policy is widely distributed and easily accessible, so lack of knowledge of this policy is not an excuse for failure to observe it. Questions regarding this policy can be directed to the Information Technology Services. Disregard for this policy may result in disciplinary actions as set forth in Section 8 of this document. In addition to local policy, users are expected to abide by the policies of the resources they may connect to over the Internet.

University of West Georgia computer and network users are expected to read sign on messages and system news for specific information such as system changes, policies and scheduled downtime. Additionally, valuable information is available at the University of West Georgia web site. System and network administrators may find it necessary to contact users regarding policy issues. If repeated attempts to contact an individual concerning a policy violation are

unsuccessful, the system or network administrator may be forced to temporarily deactivate the account simply to compel the owner to make return contact.

The following behaviors are considered a direct violation of this policy: harass, threaten or otherwise cause harm to a specific individual(s), whether by direct or indirect reference; impede, interfere with, impair or otherwise cause harm to the activities of others, to include the introduction of virus(s) onto the network or workstation; download or post to university computers, or transport across university networks, material that is illegal, proprietary, in violation of university contractual agreements or is otherwise damaging to the institution; harass or threaten classes of individuals. Further explanations of these behaviors can be found at http://policy.westga.edu/behavior.html.

7.2 Personal Business Use and Advertising

The use of University of West Georgia computers and networking services for personal business is prohibited. The campus email system, web server, or any other University of West Georgia computer shall not be used to advertise, promote, or solicit private business.

The Board of Regents of the University System of Georgia states in Section 711.02 Business Enterprises that:

> "Institutions of the University System shall not permit the operation of private business enterprises on their campuses, except as otherwise provided by contract. All business enterprises operated on a campus of an institution of the University System shall be operated as auxiliary enterprises and shall be under the direct management, control and supervision of the chief business officer of the institution."

7.3 Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

7.4 Use of copyrighted or licensed materials

Unauthorized copying of software is prohibited. Software installed on any University of West Georgia computer or network device must be

accompanied with a valid license. Users may be asked to show a valid license agreement to ensure the legal use of software on University of West Georgia computers. Contact the department head responsible for the specific computer if you have any questions regarding licensing issues. Faculty, staff, and students who include copyrighted materials on their web pages or in any electronic format bear the responsibility for obtaining permission to use these materials from the author or creator.

8.0 Consequences of Violations

Violations of the policies contained in this document are subject to the same types of disciplinary action as violations of other University policies, or state or federal laws, including criminal prosecution in serious cases. All users are expected to be familiar with these policies and abide by them at all times. Penalties for violating this policy can include, but are not limited to:

* Suspension of University computing privileges
* Disconnection of the user's computer from the campus network
* Suspension from attending the University
* Expulsion from the University
* Criminal charges, if applicable
* Civil liability, if applicable

9.0 Definitions

Authorization is another word for permission, which is granted by the appropriate part of the University's governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.

Authorized use of University owned or operated computing resources is use consistent with the education, research and service mission of the University, and consistent with this policy.

Authorized users are (1) current faculty, staff, and students of the University, (2) anyone connecting to a public information service; (3) others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources.

Hosts constitute any computer, laptop, server, printer, or device connected to the campus data network including those devices connected by wireless means.

University computers and network facilities, or University computing resources comprise all computers owned or administered by any part of the University of West Georgia or connected to the University's telecommunications facilities, including departmental computers, and also the University's computer network facilities accessed by anyone from anywhere.

10.0 Relevant Links

Student Handbook and Catalogs
http://www.westga.edu/~registra/catalogs.htm
Board of Regents of the University System of Georgia Policy Manual

http://www.usg.edu/regents/policymanual/
Board of Regents of the University System of Georgia Policy Manual
Section 711.02 Business Enterprises
http://www.usg.edu/regents/policymanual/700.phtml

Board of Regents of the University System of Georgia Policy Manual
Section 712 Information Security Policy
Section 712.01 General Policy
Section 712.02 System Level Activities
Section 712.03 Institutional Responsibilities
http://www.usg.edu/regents/policymanual/700.phtml

Georgia Code 16-5-90 G - Cyber stalking Law
http://www.legis.ga.gov/legis/2003_04/gacode/16-5-90.html

Georgia Code 34-1-7 G - Harassing or Threatening Activities
http://www.legis.ga.gov/legis/2003_04/gacode/34-1-7.html

Georgia Code 16-9-90, 91, 92, 93, 93.1, 94 - Computer Crime, Computer Theft, Computer Trespass,
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-90.html
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-91.html
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-92.html
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-93.html
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-93.1.html
http://www.legis.ga.gov/legis/2003_04/gacode/16-9-94.html

11.0 Revision History
First Draft - 2003-12-03
2nd Draft -2004-11-15
3rd revision Oct. 2008
Harassment Section Updated March 2011

Institutional IT Security Standards

Access Authorization and Authentication Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 12.1-5 and 12.7 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

4.1 Discretionary Access Control (DAC)

DAC is the capability to restrict system user access to specific systems, functions, directories and files. This implements the principle that a user should be given only those privileges or access that enables the individual to do his or her job. DAC guards against "need-to-know" violations.

4.2 Methods of Access Control

A combination of physical security, personnel security, and system security mechanisms is used to control access to the UWG enterprise network. The method of access control is a combination of a personal user login ID (identification) and a unique password (authentication).

- Users must be properly identified and authenticated before accessing the UWG enterprise network.

4.3 Identification

Each user must be accurately, consistently, and positively identified, and positive identification must be maintained throughout the user's login session.

- ITS will develop and document procedures for the issue of user login IDs.
- ITS will delete user ID accounts within one workday of the user's departure from the university, or when a user no longer requires access to perform his/her duties.
- University Human Resources department will inform ITS when an employee leaves the university's employment, retires, or is reassigned to another department.
- The use of group login IDs does not meet the security requirement for positive identification to the granularity of a single system user. Therefore, group login IDs can only be issued as exceptions to the standard, and must be a) documented as such and b) kept up-to-date for audit review.

4.4 Authentication

- The use of a password is required to authenticate all user login attempts.
- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed at least every 120 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

- Passwords must not be inserted into email messages or other forms of electronic communication.
- When an automated password recovery system is used, a method of forcing a change of the compromised password shall be instituted.
- All user-level and system-level passwords must conform to the standards and guidelines described below.

4.4.1 General Password Construction Guidelines

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not words in any language, slang, dialect, jargon, etc
- Are not based on personal information, names of family, etc.
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

4.4.2 Password Protection

- Do not use identical passwords for different accounts or systems; especially do not reuse passwords from home.
- Do not share passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as confidential information.
- Use of the "Remember Password" feature found on many applications should be kept to an absolute minimum and is highly discouraged.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Never reveal passwords to anyone over the telephone or via email.

4.5 Applications

Applications developed or procured by the University must ensure their programs contain the following security precautions:

- Support authentication of individual users.
- Do not store passwords in clear text or in any easily reversible form.

- Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit

changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Added email to bullet five of item 4.2.2

Data Encryption Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.

These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 8.1-2, 8.4, 13.2, 9.1 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum encryption standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

Certain specific types of data transactions must be protected during transmission. They include but are not limited to: Electronic Commerce, Personal Identification data, Student records, Medical records, and Authentication credentials. Additionally, some or all of this data may need to be stored in an encrypted form. Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for this encryption.

Key length requirements must be reviewed periodically and upgraded as technology allows. UWG's minimum standard encryption strengths are:

- Symmetric cryptosystem key lengths must be at least 56 bits but 128 bits are preferred when the system is capable of using them.
- Asymmetric crypto-system keys must be of a length that yields equivalent strength.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed and approved by the University Information Security Officer. Be aware that the U.S. Government restricts the export of encryption technologies. For more information, see the U.S. Encryption Export Control Policy.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance is the responsibility of each UWG participant unit/organization IT department. Implementation is the responsibility of ITS.

5.2 Enforcement

The UWG Information Security Officer (ISO) and ITS will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Data Sensitivity and Asset Classification Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.

These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references sections 4, 6 and 9 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

4.1 Resource Criticality

IT resources will be classified as mission-critical, important, or supportive, and will thereby be given a Criticality Score of 1 – 3.

Level	Definition	Criticality Score
Mission-critical	Automated information resources whose failure would preclude the campus from accomplishing its core operations.	3
Important	Automated information resources whose failure would not preclude the campus from accomplishing core operations in the short term (a few hours), but would cause failure in the long term (a few hours to a few weeks).	2
Supportive	Automated information resources whose failure would not preclude the campus from accomplishing core operations in the short to long term (a few hours to a few weeks), but would have an impact on the effectiveness or efficiency of day-to-day operations.	1

4.2 Resource Sensitivity

Resource sensitivity is a function of requirements for a data resource's confidentiality, integrity, and availability: Each sensitivity criterion will be rated on a scale as follows:
High = 3, Medium = 2, Low = 1, Not = 0. The maximum of these ratings will be the data resource's Data Sensitivity Score.

Confidentiality	Assurance that information in an IT system is not disclosed to unauthorized persons, processes, or devices.
Integrity	Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction.
Availability	Assurance that information, services, and IT system resources are accessible to authorized users and processes on a timely and reliable basis and are protected from denial of service.

4.3 Tier Definition

The greater of the Criticality Score and the Data Sensitivity Score will be the data resource's Certification Score, which defines the resource's tier.

Tier	Certification Score
Tier 1	1
Tier 2	2
Tier 3	3

4.4 Minimum Security Standards for IT Resources in Each Tier

All assets classified Tier 2 or 3 are considered to be critical assets and will be located and housed in a securable area with independent environmental controls. Assets will be housed in such a way that access is restricted to those with direct responsibility for proper operation and system health.

Tier 3: A resource with a Certification Score of 3 must be deployed on a system that satisfies the minimum security requirements specified in all other UWG security standards documents in addition to these security requirements

- The hardware on which the system is deployed must be in a secure location with physical intrusion alarm systems and the ability to log entry and establish an audit trail of all accesses to location, with procedures for review of the log.
- The system must produce logs of system activity that are reviewed daily for suspicious activity.
- The system must be managed with comprehensive documentation, configuration-management, and change-management procedures and controls.
- The system's administrators must have a comprehensive contingency and disaster-recovery plan, with testing procedures.
- User authorization for the system must be given by senior university administrators.
- The system must enforce strict user authentication controls.

Tier 2: A resource with a Certification Score of 2 must be deployed on a system that satisfies all minimum security requirements specified in all other UWG security standards documents in addition to these security requirements.

- The system should be managed with comprehensive documentation and configuration-management.
- The system's administrators should have a comprehensive contingency and disaster-recovery plan.

- The system should enforce strict user authentication controls.

Tier 1: A resource with a Certification Score of 1 is not considered critical and is not subject to certain more stringent physical and environmental security policy and standards. However, tier 1 resources must be deployed on a system that satisfies a UWG standard with universal application and additionally those below.

- The system must have sufficient physical access controls to protect the University's investment.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security

audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Enterprise Firewall Management and Network Access Control Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 7.2, 8.3-4, 12.1, 12.3 and 12.6-7 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

4.1 Firewall Management

- The preferred method for controlling access to the enterprise network is the “Default Deny”
- Configuration changes to the rule sets in the various firewall boundaries within the campus network and at the perimeter must be requested through the Service Desk.
- The system or service for which access is required must be previously approved for use on the campus network, and meet all policy requirements for operation.
- The system or service for which access is required must not adversely affect network performance, unduly compromise the security of the network, nor expose the institution to excessive liability or risk.
- The implications of exposure of the system or service for which access is required must be fully understood and accounted for by the responsible IT unit.
- The request must precisely and completely document the requisite information needed by the firewall administrator for the system or service for which access is required
- Responsibility for security of the system or service for which access is required remains with the responsible party of the system or service.
- Configuration changes to the rule sets in the firewall boundaries are not approved for individual or personal use - such access must be accomplished by other means provided by ITS, such as email, sftp, shell access, VPN, etc.

4.2 Remote Access

- Remote access privileges will only be granted after being verified as necessary by ITS.
- Secure authenticated remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Access Authorization and Authentication Standards.
- It is the responsibility of university employees, student, contractors, vendors and agents with remote access privileges to the university’s network to ensure that their remote access connection is given the same consideration as a user's on-site connection to the University.
- Individuals granted access are responsible for ensuring that the access afforded them is not used inappropriately and is in accordance with the University’s Acceptable Use Policy. University employees and students shall not use access granted by the University to conduct outside business interests.

4.3 Access Monitoring

All devices which provide network access will log system events that can be used to audit unauthorized access to the device itself and/or the network. Such logs must be kept for a minimum of 30 days and be capable of being archived indefinitely in support of an incident investigation.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance is the responsibility of each UWG participant unit/organization IT department. Implementation is the responsibility of ITS.

5.2 Enforcement

The UWG Information Security Officer (ISO) and ITS will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Inserted Service Desk for Helpdesk (bullet 2 item 4.1)
- Removed missing link (bullet 6 item 4.1)
- Removed reference to IT units from bullet 6 & 7 of item 4.1)
- Identified ITS as verifier for Remote Access (bullet 1 item 4.2)

Enterprise Network Infrastructure Security Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 7.1-3, 12.1, 12.3 and 12.6 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

- Use of the enterprise network is governed by the University Acceptable Use Policy.
- Information Technology Services (ITS) Networking Services will manage and administer the university enterprise network.
- ITS Networking Services will determine the technical specifications, installation practices, standards, and operational criteria.
- ITS Networking Services will determine and document the security configurations for networking devices connected to the university enterprise network.
- All physical connections to the university enterprise network must be made in accordance with UWG's Telecommunications Wiring Standard.
- Colleges/Departments/users may not attempt to extend the University enterprise network without permission from ITS Networking Services. This includes, but is not limited to, basic network devices such as repeaters, switches, routers, network firewalls, and wireless access points.
- Colleges/Departments/users may not offer alternative methods of physical access to the University enterprise network, such as modems and Digital Subscriber Links.
- The University recognizes that certain organizations/departments within the institution may have a need to operate systems and networks for academic, research, or other special purposes. In some cases, such systems may be unable to meet one or more applicable UWG security standards. At the same time, it is understood that such systems have the potential to undermine any efforts to secure the enterprise IT infrastructure, thereby placing that infrastructure at risk. In such cases, the IT unit responsible for such systems will work with ITS Networking Services to implement an appropriate set of physical and/or logical network controls to isolate those systems from the enterprise network, such that the operational needs for those systems are met while at the same time ensuring that those systems cannot impact the enterprise IT infrastructure. These "sandbox" network environments must be fully documented with ITS Networking Services.
- UWG network traffic is monitored to address any network usage or quality of service issues. Although traffic is not being monitored for content, the content may be viewable. UWG reserves the right to monitor said traffic without prior permission per The Wiretap Act, the Pen Register and the Trap and Trace statutes "Provider Exception" clauses.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance is the responsibility of each UWG participant unit/organization IT department. Implementation is the responsibility of ITS network Services.

5.2 Enforcement

The UWG Information Security Officer (ISO) and ITS Networking Services will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Networked Devices Security Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 7.2-3 and 12.3-4 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

All devices connected to the UWG enterprise network shall be brought into compliance with these security standards before or immediately upon connecting to the UWG enterprise network. Examples of devices subject to these standards include but are not limited to: desktop systems, printers, scanners, multi-function copiers, Personal Digital Assistants (PDA) and IP Converters.

4.1 General Standards

All devices connected to the UWG enterprise network must be owned by an identified IT department that is responsible for the device's administration. IT departments must monitor configuration compliance or implement an exceptions policy tailored to their environment. Each IT department must establish procedures and documentation that adhere to the University's Policy on Classification and Protection of IT Resources. These documents must be kept up to date and available for audit review.

- All device passwords shall comply with the UWG password policy which can be found at http://policy.westga.edu.
- A plan and process should be in place for securing administrator and root passwords that allows appropriate access to the device in case of illness, turnover, or unforeseen circumstances.
- All devices shall only run the minimum services required to complete its function.
- All devices capable of being updated shall have the most current security patches and/or firmware applied.

4.2 Desktop Workstations

- A password-protected screen saver, with a relatively short time out, should be implemented on all faculty/staff workstations.
- End users are responsible for periodically backing up important data on their workstations. The best location for end users to place this data is on a file server. However, departments may provide alternate data backup strategies for end users.
- Any workstation that is intended to be physically accessible to users in an unauthenticated and un-trusted manner shall be considered a lab computer.
- Steps shall be taken to increase the difficulty of changing lab computer BIOS settings and reduce the ability of users to boot the lab computer with an unapproved operating system. An example of this would be preventing a user from booting a lab computer with a bootable CD in order to bypass restrictions placed on the lab computer by the system administrator.

- System administrators shall implement controls on lab computers to reduce the ability of users to execute unapproved programs or change system settings, where appropriate.
- Lab computers shall be restricted from having access to UWG servers and network resources that are not required for the function of the lab computer.

4.2.2 Event Logs

- The following comprise the minimum events to log.
    - Use of account login and logout.
    - Actions taken by system administrators. Examples include adding a user, changing user rights, or performing workstation restarts.
    - Any event that attempts to change the security profile of the system. Examples include changing access controls (rights or attributes) to files, directories, and user discretionary access, or changing a user password.
    - Any event that attempts to violate the security of the system. Examples include too many attempts to login or attempts to violate the access control limits of a device.
- The event log will record the following minimum information, where possible, for each event.
    - Date and time of the event.
    - Unique identifier of the user or device generating the event.
    - Type of event.
    - Success or failure of the event.

4.3 Printers

- Disable or delete network print queues that are no longer in use.
- If multiple users need to share a printer the printer should be connected to the network and a network print queue should be created.
- Change the SNMP Set Community Name from public to some other standard name where applicable.
- Secure access to the printer administrative interface, where applicable, to ensure that only authorized individuals may alter the printer's configuration.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Deleted “provided by their IT department” from end of second sentence on item 4.2 bullet 2

Telecommunications Security Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 12.1-5 and 12.7 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

All telecommunications devices connected to and telecommunications services used on the UWG telephone network must comply with the UWG Acceptable Use Policy.

All telecommunications devices connected to and telecommunications services used on the UWG telephone network are to be controlled by the following means:

4.1 Acquisition, maintenance, and use of telecommunications devices and services:

- Unit heads determine what telecommunications devices and services are required by the employees under their supervision and then meet with UWG's ITS telecommunications manager or place service requests via UWG's ITS Helpdesk system.
- New UWG telecommunication analog, digital or VoIP devices and services should be obtained from the agency/manufacturer contract in force or the cost center should obtain quotes from vendors and examine packages which will result in the lowest cost considering one time purchase and on-going maintenance costs.

4.2 Maintain and monitor accounting and event logs

- Monitor traffic and other logs to insure that an appropriate and not excessive number of trunks/lines/channels are leased for connection to the public telephone network.
- Audit events to ensure the confidentially, integrity, and availability of telecommunications equipment and services on the UWG telephony network.
- Monitor for activities of telephone hackers or incidents of PBX toll fraud.

4.3 Harassing phone calls

UWG users who receive harassing phone calls should report the problem to University Police Investigations. If necessary, UWG University Police will then request ITS Telecommunications to program a Call Trace function on the person's phone receiving the phone call. If no CallerID info is being sent to UWG's PBX then information will be prepared that will be sent by University Police along with an authorized court issued subpoena to UWG's local telephone service provider.

4.4 Wiretapping

Wiretaps on campus property are not permitted unless required for normal service technician maintenance functions, and no telecommunications recordings without the recorded parties' consent will be provided without authorization by a court issued subpoena, or under other appropriate authority.

4.5 UWG Voice Mail passwords

All UWG voice mail passwords have to be changed after being reset to the default before the mail box can be logged into, and a voice mail password has to be a minimum of 5 digits and non-trivial.

4.6 Intrusion Prevention

- Lock and/or restrict access to telecommunications closets and rooms. Access should be given to authorized personnel only.
- Pass protect with non-trivial or default pass codes all telecommunications PBX consoles and computer systems.
- Perform periodic PBX security audits.
- Maintain up-to-date PBX system documentation and schematics, but not in publicly accessible locations. Maintain an inventory of PBX components.
- Perform periodic backups of PBX systems and store backup tapes off-site.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Network Scanning Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 12.3 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

Regular scanning of computers and devices connected to the University's network can reveal potential security threats and vulnerabilities. Therefore, the information security personnel at the University of West Georgia may conduct network scans on any server, computer, network, or device on the University's campus or any satellite campus under the University's authority.

4.1 Authorized and Unauthorized Scanning Activities

No computer system or device connected to the University's network via wired or wireless connection will be used to perform network scans on ANY computer, network, or device, on or off of the University's campus, with the following exceptions:

- The University's networking staff may perform network scans in an effort to resolve a service problem, as a part of normal system operations and maintenance, or to enhance the security of University network.
- The University's Information Security staff may perform network scans to monitor compliance with University policy, to perform security assessments, or to investigate security incidents.
- System Administrators may perform local system scans prior to putting a system into production or as a part of continued system maintenance.

4.2 Service Degradation and/or Interruptions and Harmful Results

Network scanning is a formidable tool for testing and protecting the University's information resources when used properly. Unauthorized or improperly conducted network scans pose a threat to the availability, integrity, and confidentiality of the University's information resources. Improper and unauthorized network scanning can result in the following:

- **Disclosure of Sensitive Data**: Network scans yield a tremendous amount of information about our networked computing systems. This information is crucial to attackers in their efforts to compromise computer systems. If a critical system is compromised, an attacker may have unlimited access to confidential data.
- **Loss of Service**: Network attacks vary greatly in nature. The goal of the attack may be to gain control of a computing system or to simply make the system unavailable to others. Even the process of vulnerability scanning can cause a system to crash or behave erratically.
- **Loss of Network and System Performance:** Network scanning can involve hundreds or even thousands of computing systems. The sheer volume of network traffic requests can place an incredible strain on the resources of our computing systems and the University network, resulting in less than optimal performance for University users.

- **Loss of Reputation:** As a member of the global Internet village our actions directly affect the safety of information and information resources around the world. By allowing the University's computing resources to be used to compromise systems belonging to our global neighbors, our reputation as a responsible member of Internet may be tarnished.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Substituted “System Administrators” for “Departmental IT Personnel” in bullet 3 of item 4.1

Server Security Standards

1.0 Authority

To assure the security of Information Technology (IT) resources, the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy in sections 6, 7 and 10, items 8.5-6, and 12.3 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

The University IT server infrastructure falls into the following two categories: Unix OS based servers (Existing Environment: Solaris, Linux) and Windows based servers. Each has unique characteristics that must be addressed before connection to the UWG Campus Network.

4.1 Server Documentation:

Each IT department that administers servers connected to the UWG Campus Network must develop and maintain a set of configuration procedures for each unique system and a configuration history for each individual system. These documents must be kept up to date and available for audit review.

4.2 Ownership and responsibilities

All servers connected to the UWG Campus Network must be owned by an identified IT department that is responsible for the systems administration. IT departments must monitor configuration compliance and implement an exception policy tailored to their environment. Each IT department must establish procedures and documentation that adhere to the Universities' Policy on Classification and Protection of IT Resources. These documents must be kept up to date and available for audit review.

4.3 Security Patches

All servers shall have the most current OS and application security patches applied including operating systems and server applications. When new patches are released that are deemed by the manufacturer to be critical in nature, the patches shall be applied within five (5) working days to all servers. If there is justifiable reason to not apply a security patch, then steps should be taken to mitigate any risk associated with not applying the patch. All other security patches not deemed critical by the manufacturer shall be evaluated by the system administrator to determine the level of criticality for each specific server. Those deemed critical by the system administrator shall be applied within five (5) working days to all affected servers. All other patches shall be applied at the next update cycle, as determined by the system administrator.

4.4 General Configuration Guidelines

- Services and applications that will not be used must be disabled whenever practically possible.
- Access to services should be logged and protected through access-control methods

- The most recent stable security patches must be tested & installed on the system wherever possible and in a timely manner.
- UWG approved and supported virus protection must be installed and in compliance with UWG Antivirus Software Standards.
- System administrators should be aware that establishing trust relationships between systems can potentially allow unauthorized users to access resources that they should not have access. Administrators should only use trust relationships when its need has been clearly evaluated and weighed against any alternative methods. When one is implemented, administrators should take steps to reduce any possible areas of security vulnerabilities due to the trust relationship.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will satisfy the needs
- If a methodology for secure encrypted channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or web based SSL interface).
- System Administrators must ensure physical security by avoiding placement of servers in uncontrolled areas.

4.5 Audit Logs

Audit events are selected to ensure the confidentially, integrity, and availability of data placed on the UWG Campus Network. These events are primarily directed at the assignment and modification of a user's security rights and security attributes and are meant to satisfy the University Policy on Classification and Protection of IT Resources.

- The following comprise minimum required audit events.
  - Use of account login and logout.
  - Actions to execute programs.
  - Actions taken by system administrators. Examples include adding a user, changing user rights, or performing file server restarts.
  - Any event that attempts to change the security profile of the system. Examples include changing access controls (rights or attributes) to files, directories, and user discretionary access, or changing a user password.
  - Any event that attempts to violate the security of the system. Examples include too many attempts to login or attempts to violate the access control limits of a device.
- Specific Audit Information: The audit trail will record the following minimum information, where possible, for each audit event.
  - Date and time of the event.
  - Unique identifier of the user or device generating the event.

  - Type of event.
  - Success or failure of the event.
  - Name of the program executed.
- Review of Audit Logs: A periodic review and appropriate follow up on possible security violations identified in the system logs. For important servers this might be as often as daily.

Audit logs are sensitive data and must be handled according to the Universities' Policy on Sensitive Data Access and Use as well as the Information Handling Policy which give guidance on the storage and disposal of such data.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 6.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Reworded introduction of bullet 3 of item 4.5 to make consistent with other bulleted points for item 4.5

Third-Party Access Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 9.1 and 12.7 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

Third party access is non trivial access, unavailable to the general public, which is granted to a vendor or contractor. Examples include but are not limited to: contract vendors with network user ID's and passwords, suppliers with user ID's and passwords that grant them remote access in order to support a specific system and contract vendors with physical access to critical data or hardware.

Each department within the University that maintains a relationship with a product or service vendor that may intentionally or unintentionally be given access to non-public data will ensure that the vendor has formally agreed to protect the security of that data. These agreements will include the following points:

(1) The level of access granted to vendors and other third-party non-affiliates will be limited to those University of West Georgia information technology resources that are required to carry out the specified business need of the University. The access must be enabled for specified tasks and functions, and limited to specific individuals and only for the time period required to accomplish approved tasks. Vendor access must be uniquely identifiable, and password management must comply with the University of West Georgia Password Policy. Appropriate procedures for terminating access must be followed upon the departure of a vendor employee from the contract/agreement or upon the termination/ completion of the contract agreement.

(2) Prior to granting a vendor or other third-party non-affiliate access to University of West Georgia information technology resources, the vendor will be required to sign an agreement/ contract with the University that specifies:

- The University of West Georgia information technology resource(s) to which the vendor will be granted access.
- The business purpose for which access is to be granted and limiting access to that purpose.
- The information to which the vendor will have access.
- A statement indicating that the vendor agrees to comply with all applicable Federal and State statutes and University policies with respect to preserving the confidentiality of the information to which they have access and that they will not disclose in any way the information or the existence of the information.
- How the vendor intends to protect the University’s information.
- The acceptable method(s) for the return, destruction or disposal of the University of West Georgia’s information in the vendor’s possession at the end of the contracted period or completion of the service.

- A statement indicating that any information acquired by the vendor in the course of the contract/agreement cannot be used for the vendor's own purposes or divulged to others.
- A statement indicating the vendor will restrict access to University of West Georgia data/ resources to only those vendor employees who are required to provide the service.
- The vendor agrees to hold the University harmless for any suits resulting from their negligence or failure to abide by terms of the contract.
- The vendor will take all reasonable steps, based upon relevant industry standards to protect the University's data/resources from corruption, tampering, or other damage.

(3) Vendors and other third-party non-affiliates are expected to adhere to all applicable Federal and State statutes and University policies, including the University's Remote Access policy and the Acceptable Use policy, and must follow all applicable University of West Georgia change control processes and procedures.

(4) The University of West Georgia will provide a point of contact for the vendor. This contact person will work with the vendor to make certain that the vendor is in compliance with these statutes and policies.

(5) Each vendor must provide a list of employees working on the contract/agreement. This list must be updated and provided to the University of West Georgia within 48 hours of staff changes.

- Each vendor employee with access to University of West Georgia confidential and/or sensitive information must be approved to access that information by the data steward of that information.
- Any vendor employee who is required to be on site at the University of West Georgia in order to carry out the terms of the contract/agreement is expected to be able to provide adequate identification if requested, and the custodian of the specific information technology resource is expected to take the appropriate steps to verify the authorization for the vendor employee to access that specific resource.
- Vendor personnel must report all security incidents directly to the UWG Help Desk at (678) 839-6587. If vendor management is involved in University of West Georgia security incident management, the responsibilities and details must be specified in the contract.
- The Purchasing Department should be contacted for assistance in developing all contracts/agreements.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Email Usage Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy items 8.2 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

As an enhancement to the academic experience while at the University and productivity enhancement tool, the University encourages the academic and business use of electronic mail (email) systems.

- All email messages generated on or handled by UWG electronic mail systems are considered to be the property of UWG, unless the material is copyrighted by a third-party.

4.1 Authorized Usage

The University's electronic mail systems generally must be used for academic, business, or university authorized activities only. Incidental personal use is permissible as long as it does not interfere with worker productivity, impose on the rights of other individuals, and does not preempt any business activity or system resources. University authorized or sanctioned activities, i.e. charitable fund raising campaigns, political advocacy efforts, religious efforts, private business activities will be allowed after written authorization by the Provost & Vice President for Academic Affairs, Vice President for Business and Finance, Vice President for University Advancement, or Vice President for Student Affairs and Enrollment Management or their designee(s).
Users are reminded that the use of university information system resources must never create the appearance or the reality of inappropriate use and said message may require a disclaimer that the message does not reflect the position of UWG.

4.2 User Separation

Electronic mail systems must employ unique personal user IDs and associated passwords. UWG has established user separation and users must not employ the user ID or the identifier of any other user.

Departmental user names, "helpdesk" user names and system administrator accounts are permissible. When an administrative username and password are shared by authorized IT staff in the course of carrying out duties and responsibilities, account or access logging must be "turned on" and monitored.

If a password is compromised in the course of work performed by IT staff, the user must be advised to immediately change the password.

4.2.1 User Identity

Users may not, under any circumstances, use "spoofing" techniques or other means to disguise/masquerade their identities in sending email. Misrepresenting, masquerading, obscuring, suppressing, or replacing a

user's identity on an electronic mail system for malicious or misleading purposes is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. Electronic mail signatures or email addendums indicating job title, University affiliation, address, and other particulars are strongly recommended for all electronic mail messages internal or external.

4.2.2 User Authorization Form

All users who are assigned a User ID for a campus electronic mail system must sign an Authorization Form that notifies the user of his/her responsibilities, rights and privileges of using the email system.

4.3 Respecting Intellectual Property Rights

Users employing the UWG email systems may repost or reproduce material only after obtaining permission from the source; quote material from other sources only if these other sources are properly identified; and reveal internal UWG information only if the information has been officially approved for public release by the appropriate University administrative office. Official approval should be in written form and available upon request.

4.3.1 Respecting Privacy Rights

By making use of the UWG systems, users consent to permit all information they store on University of West Georgia information systems to be divulged to law enforcement upon probably cause of illegal activity, at the discretion of the designated UWG official or the Administration at the discretion of UWG executive management. The University is committed to respecting the rights of its users, including their reasonable expectation of privacy. However, it may be necessary to occasionally intercept or disclose, or assist in intercepting or disclosing, electronic mail. Except as otherwise specifically instructed in writing by the President of the University, the Provost & Vice President for Academic Affairs, the Vice President for Business and Finance, Vice President for University Advancement, or Vice President for Student Affairs and Enrollment Management or their designee, users must not intercept or disclose, or assist in intercepting or disclosing, electronic mail. All Open Records requests will be processed by the University Department of Institutional Research and Planning and the President's Legal Advisor.

4.3.2 No Guaranteed Message Privacy

UWG cannot guarantee that electronic mail will be private. Users must be aware that electronic mail can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Electronic mail that is not encrypted can be viewed by people other than the intended recipient, while in transit or on mail servers.

Because messages can be stored in backups, electronic mail actually may be retrievable when a traditional paper letter would have been discarded or destroyed.

4.4 Contents of Messages

Users must concentrate on business matters in University of West Georgia electronic mail. As a matter of standard business practice, all University of West Georgia electronic mail must be consistent with conventional standards of ethical and polite conduct. Please see the UWG Acceptable Use Policy for more information: http://www.westga.edu/policy

4.5 Email Systems Monitoring

The University of West Georgia reserves the right to collect statistical data about its electronic mail systems. UWG personnel monitor the use of electronic mail to ensure the ongoing availability, reliability, and security of these systems. The University employs computer systems that analyze statistical information to detect unauthorized usage, denial of service attacks, capacity planning and network problems.

4.6 Incidental Disclosure

IT personnel must not review the content of an individual user's mail out of personal curiosity or at the request of individuals who have not been granted authority. Electronic mail users must exercise caution when forwarding messages, either internally or externally. UWG's sensitive information such as: university ID numbers, addresses, age, gender etc. must not be forwarded to any party outside of the University without the prior approval of an appropriate authority. Blanket forwarding of messages is discouraged. Messages sent by outside parties must not be forwarded to other third parties unless the sender clearly intended this and such forwarding is necessary to accomplish a customary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

4.7 Social Security Numbers

Transmitting Social Security Numbers via email over any University email system is strictly prohibited. (UWG SSN Policy)

4.8 Harassing or Offensive Materials

Sexual, ethnic, and/or racial harassment, including unwanted/unsolicited bulk electronic mail, is strictly prohibited. Users who receive offensive unsolicited material from outside sources should forward the entire (with email headers)

email to abuse@westga.edu Please see UWG Acceptable Use Policy http://policy.westga.edu/ regarding harassment.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

October 2008

- Added hyperlink to the UWG SSN Policy for item 4.7

Information Handling Standards

1.0 Authority

To assure the security of Information Technology (IT) resources the University of West Georgia (UWG) uses its Campus Security Plan to identify, create and maintain appropriate IT policies and standards in conformance with the Campus Security Policy objectives referenced below in section 1.2 and in compliance with the Policy Manual of the Board of Regents (BOR) of the University System of Georgia. A copy of the BOR Policy Manual can be obtained at http://www.usg.edu/regents/policymanual/.

1.1 Availability

Upon initial approval and any subsequent approved revisions of this document, the affected individuals identified in the Scope below will be notified of the changes via email, the campus portal, written communication or some other form of communication that provides general notification of the acceptance or change.
These documents are freely available to everyone. Copies can be obtained on the web at http://policy.westga.edu.

1.2 UWG Security Policy Reference

This document specifically references policy item 9.1 within the UWG Security Policy.

2.0 Purpose

To establish and specify the minimum standards required to meet UWG policy items listed in section 1.2 above.

3.0 Scope

This policy applies to all UWG faculty, staff and students, in addition to any guests who are authorized to use the University's computers and/or data network. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy. This includes equipment owned, leased, rented, or otherwise controlled or maintained by University employees and students, and other authorized users. Authorized users accessing University computing resources and the University data network from off campus sites through dial-up access, broadband access, or other connections are responsible for ensuring the security and integrity of system(s) they are using to establish said access.

4.0 Standards

The University of West Georgia (UWG) will utilize the University System of Georgia's Board of Regents Records Retention Guidelines/Manual to establish record retention practices and handling, in order to allow ongoing compliance with federal and state law, including the Georgia Records Act (O.C.G.A. 50-18-90 et seq.), and to meet requirements of external entities, such as accrediting bodies. A copy of the BOR Records Retention Manual can be obtained at http://www.usg.edu/usgweb/busserv/series/index.phtml.

Definitions of confidential, sensitive, and vital records are listed in section 6.1 below.

5.0 Compliance

Compliance is as indicated in UWG Security Policy.

5.1 Responsibilities and Implementation

Compliance with and Implementation of these standards is the responsibility of each UWG participant unit/organization IT department.

5.2 Enforcement

Each UWG participant unit/organization IT department in conjunction with the UWG Information Security Officer (ISO) will be responsible for enforcing these standards.

5.3 Disciplinary Process

Disciplinary actions will be handled via existing Institutional governing bodies and procedures.

5.4 Clarification/Interpretation Process

Requests for clarification or appeals will first be directed to the appropriate Faculty Senate sub committee for review. The Faculty Senate has final review authority.

6.0 References

6.1 Definitions

Definitions can be obtained on the web at http://policy.westga.edu.

Confidential
Any record or information, regardless of its physical form or characteristics,

that is not open to public examination because it contains information which, if disclosed, might damage individual privacy or compromise public activities. This information is also protected from disclosure by state and federal laws.

Examples:
Social Security Numbers
Birth dates
Account Numbers (Bank deposits)
Insurance Information
Grades (FERPA)
Counseling/Mental Health Records (HIPAA)
Medical Records (HIPAA)

Sensitive
Any information or material, regardless of its physical form or characteristics, that is required to be protected against unauthorized disclosure, and is so designated.

Examples:
Identification Codes (Employee and Student)
Actions pertaining to renewal/termination of employment.
P-cards
Notes (maintained on Banner/PeopleSoft/Raizor's Edge)
Library Patron Records

Vital
Vital Records are defined as: records containing information essential to the survival of an organization in the event of a disaster; the resumption and/or continuation of operations; the re-establishment of the legal, financial, and/or functional status of the organization; and the determination of the rights and obligations of individuals and corporate bodies with respect to the organization. Vital Records typically make up a small percentage of the vast amounts of the recorded data which is created by a typical organization - normally 5%.

Examples:
Contracts/agreements that prove ownership of property, equipment, vehicles, products, etc.
Operational records such as current accounting and tax records, current personnel/payroll records, account histories, and shipping records
Software source codes (to include both licensed programs and systems and custom developed applications)

7.0 Policy Review

The UWG ISO will review this document in conjunction with major changes to the information infrastructure, as part of UWG's participation in system security audits, after each breach in system security, or every two years. The UWG ISO will submit changes and additions for review and approval by the appropriate Faculty Senate sub committee.

7.1 Review Process

Responsible parties referenced in section 5.1 of this policy will review and submit revisions per section 2 of the Campus Security Plan for the University of West Georgia.

7.2 Approval Dates

January 2006

7.3 Revisions

N/A

Section IV
Appendix

UWG IT Organizational Chart

http://www.westga.edu/assetsDept/its/Org_Chart_Orig.pdf

UWG Computer Support Contact List

(1) primary emergency contact for unit
(2) secondary emergency contact for unit
(3) primary person(s) responsible for application/system security for unit

Information Technology Services, ITS

Provides support for all campus-wide applications (Banner, BanWeb, Banner Imaging System, email, main campus web server, Resource25, OneCard System, the Luminis portal, Facilities Management System, Oracle Calendar, HelpDesk) and networking; primary contact for Level 1 support for President's Office, Institutional Research and Planning, University Advancement, Special Programs, VPAA Office, Learning Support, Sponsored Operations, Learning Resources, Continuing Education, International Programs, Graduate School, Advanced Academy, Honor's College, VP for Student Affairs and Enrollment Management Office, Athletics, Admissions, Alumni Services, Educational Technology Training Center, Student Development, Career Services, Excel Center, Financial Aid, Health Services, Intramurals, Publications and Printing, Registrar, Residence Life, Student Activities, Student Government, and University Communications and Marketing.

Name	Title	Building	Phone	Email
Adams, Blake	User Services Director	Cobb Hall	678-839-6585	badams@westga.edu
Aye-Addo, Benjamin	Computer Services Spec. II	Humanities	678-839-6585	bayeaddo@westga.edu
Barnes, Tamarsha	Customer Service Rep.	Cobb Hall	678-839-6585	tbarnes@westga.edu
Blumenberg, Mellonee	Information Systems Coordinator	Aycock Hall	678-839-6585	mblumenb@westga.edu
Browning, Josh	System Support Spec. III	Cobb Hall	678-839-6585	jbrownin@westga.edu
Chandran, Anuradha	System Support Spec. I	Cobb Hall	678-839-6585	achandra@westga.edu
Chasteen, Denny	Manager, Web Innovations	Cobb Hall	678-839-6585	dchasteen@westga.edu
Clay, Matthew	Computer Operations Manager	Education Ctr	678-839-6585	mclay@westga.edu
Crews, Tammy	Customer Service Rep	Cobb Hall	678-839-6585	tcrews@westga.edu
Driver, Dale	Lead IT Project Manager	Humanities	678-839-6585	ddriver@westga.edu
Farmer, Rolanda	Graphics Technician	Anthropology	678-839-6585	rfarmer@westga.edu
Geter, Joe	Database Administrator	Cobb Hall	678-839-6585	jgeter@westga.edu
Gibson, Vince	Programmer Analyst III	Aycock Hall	678-839-6585	vgibson@westga.edu
Goodwin, Abigail	System Support Spec. II	Aycock Hall	678-839-6585	agoodwin@westga.edu
Gunay, Vedat	Assoc. Director of Desktop Support	Boyd	678-839-6585	vgunay@westga.edu
Hall, Price	Systems Admin Manager	Boyd	678-839-6585	phall@westga.edu
Busti, Andrew	Tech Specialist II	Anthropology	678-839-6585	mlharris@westga.edu

Horton, Suzanne	Clerical Assistant	Anthropology	678-839-6585	shorton@westga.edu
Kral, Kathy (1, 3)	Chief Information Officer	Cobb Hall	678-839-6585	kkral@westga.edu
Laurent, Addison	System Support Spec. III	Boyd	678-839-6585	alaurent@westga.edu
Lewis, Calandra	Customer Service Rep.	Cobb Hall	678-839-6585	clewis@westga.edu
McCrary, Brian	Asst. Director of Classroom Support and Special Projects	Anthropology	678-839-6585	bmccrary@westga.edu
Silhan, Lisa	ERP Analyst	Aycock Hall	678-839-6585	lsilhan@westga.edu
Nahri, Keihan	Telecommunications Manager	Boyd	678-839-6475	knahri@westga.edu
Nichols, Janet	Web Associate	Cobb Hall	678-839-6585	jnichols@westga.edu
North, Tim	Network Services Spec. III	Boyd	678-839-6585	tnorth@westga.edu
Olson, Ben	System Support Spec. II	Cobb Hall	678-839-6585	bolson@westga.edu
Parrish, Todd	Computer Services Spec. I	Humanities	678-839-6585	tparrish@westga.edu
Pearson, Mike	Computer Services Spec. III	Humanities	678-839-6585	mpearson@westga.edu
Peterson, Brandon	Media Tech Specialist II	Anthropology	678-839-6585	bpeters@westga.edu
Petty, Judi	System Support Spec. III	Humanities	678-839-6585	jpetty@westga.edu
Phillips, Jon	Computer Services Spec. I	Aycock Hall	678-839-6585	jphillip@westga.edu
Plummer, Eugene	Network Services Spec. II	Boyd	678-839-6585	eplummer@westga.edu
Purcell, Matt	Computer Support Spec. I	Education Ctr	678-839-6585	mpurcell@westga.edu
Renfrow, Renee	Administrative Assistant	Cobb Hall	678-839-6585	rrenfrow@westga.edu
Richardson, Michael	Programmer Analyst IV	Cobb Hall	678-839-6585	mrichard@westga.edu
Rogers, Vicki	Service Desk Manager	Cobb Hall	678-839-6585	vickir@westga.edu
Rose, Laurence	Computer Support Spec. I	Humanities	678-839-6585	lrose@westga.edu
Sellers, Justin	System Support Spec. II	Education Ctr	678-839-6585	jsellers@westga.edu
Shumake, Mardel (3)	Information Security Officer	Boyd	678-839-6585	mshumake@westga.edu
Spruck, Chris	Web Associate	Education Ctr	678-839-6585	cspruck@westga.edu
Stogner, John (2)	Infrastructure Director	Cobb Hall	678-839-6585	jstogner@westga.edu
Tennant, Nathan	Computer Services Spec. III	Boyd	678-839-6585	ntennant@westga.edu
Upshaw, Bernard	Computer Support Spec. I	RCOB	678-839-6585	bupshaw@westga.edu
Valcke, Brenda	Staff Assistant	Boyd	678-839-6585	bvalcke@westga.edu
West, Karen	Asst. Director for Software Development	Cobb Hall	678-839-6585	kwest@westga.edu
Whitt, Gabe	Computer Services Spec. II	Cobb Hall	678-839-6585	gwhitt@westga.edu

Williams, Howard	Programmer Analyst III	Boyd	678-839-6585	hwilliam@westga.edu
Wilson, Garth	System Support Spec. III	Boyd	678-839-6585	gwilson@westga.edu
Winslett, Michael	Computer Services Spec. II	Education Ctr	678-839-6585	mwinslet@westga.edu
Wojcik, Rory	Media Tech Specialist II	Anthropology	678-839-6585	rwojcik@westga.edu
Yawn, Rob	Networking Manager	Boyd	678-839-6585	ryawn@westga.edu
Zinnerman, Ewa	Web Associate	Bonner Hourse	678-839-6585	ezenner@westga.edu

Department of Computer Science, Computer Science Technology Support
Provides computer support for the Computer Science Department.

Name	Title	Building	Phone	Email
Abunawass, Adel (Dr.) (1)	Professor and Chair	TLC	678-839-6652	adel@westga.edu
Rudolph, Edwin (2,3)	Laboratory and Assessment Coordinator	TLC	678-839-6650	erudolph@westga.edu
Young, Alexandra	Instructional Technology Specialist	TLC	678-839-6651	ayoung@westga.edu

University Library, Systems Librarian
Provides computer support for all Ingram Library Departments

Name	Title	Building	Phone	Email
Huff, Chris (1, 3)	Systems Librarian	Library	678-839-6366	chuff@westga.edu

Newnan Center, Technology Support
Provides computer support for the Newnan Center Campus

Name	Title	Building	Phone	Email
Smith, Rebecca (1)	Asst. Director	Newnan	770-254-7345	rsmith@westga.edu
Boyce, Javarus (2, 3)	Technology Specialist	Newnan	770-254-7287	javarus@westga.edu
Coppolella, Cheryl	Instructional & Student Support Specialist	Newnan	770-254-7435	cherylc@westga.edu

Student Affairs and Enrollment Management, Student Information Services
Provides computer support for all Student Affairs and Enrollment Management Departments

Name	Title	Building	Phone	Email
Colevins, Annelle (1, 3)	Student Affairs Web & Tech Coordinator	Mandeville	678-839-6384	acolevin@westga.edu
Barlow Justin (2)	Information Specialist	Mandeville	678-839-4000	jbarlow@westga.edu
Reeves, Becky	Technical Assistant	Mandeville	678-839-6421	rreeves@westga.edu

Definitions

Asymmetric Cryptosystem - A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Blowfish
A symmetric block cipher algorithm capable of using various key lengths

Cable Modem
Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities

Campus Network
The network used in the daily business of the University of West Georgia. Any network connected to the university backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the University of West Georgia.

CHAP
Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

DES
The Data Encryption Standard (DES) is a cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally.

Dial-in Modem
A dial-in modem is a peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Defense in Depth
Defense in Depth is an approach to IT Security that makes use of multiple security countermeasures to protect the confidentiality, integrity, and availability IT resources. The idea is that since IT resources are under constant "attack" and at risk the various countermeasures taken individually may fail. However, as a whole the countermeasures minimize the adverse impact and give IT staff a chance to deploy new or updated countermeasures.

Components of defense in depth include antivirus software, firewalls, anti-spyware software, strong passwords, monitoring, logging, and security awareness education. Defense in Depth requires a comprehensive approach to IT security with and ongoing strengthening, improving, and modifying of countermeasures.

DSL
Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Enterprise Network
The network used in the daily business of the University of West Georgia. Any network connected to the university backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to the University of West Georgia.

Executive Management
Personnel assigned at the Vice President level or above.

IDEA (International Data Encryption Algorithm)
A private key encryption-decryption algorithm that uses a key that is twice the length of a DES key

ISDN
There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Lab Network
Any network used for the purposes of testing, demonstrations, training, etc. that is stand-alone or firewalled off from the campus network(s) and whose impairment will not cause direct loss to the University of West Georgia nor affect the Enterprise network.

LDAP (Lightweight Directory Access Protocol)
A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet

PBX
A private telephone switch that provides switching (including a full set of switching features) for an office or campus.

Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

RADIUS (Remote Authentication Dial In User Service)

Authentication, Authorization and Accounting (AAA) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

RC5
RC5 is a block cipher notable for its simplicity.

Remote Access
Remote access is any access to a University of West Georgia network through a non-University controlled network, device, or medium.

RSA
The best known public key algorithm, named after its inventors: Rivest, Shamir and Adleman. RSA uses public and private keys that are functions of a pair of large prime numbers.

Sandbox Network
Any network used for the purposes of testing, demonstrations, training, etc. that is stand-alone or firewalled off from the campus network(s) and whose impairment will not cause direct loss to the University of West Georgia nor affect the Enterprise network.

Server
1) A computer program that provides services to other computer programs in the same or other computers; 2) the computer/device on which a server program runs

SFTP (secure file transfer protocol)
Secure File Transfer Protocol. SFTP uses SSL to encrypt the entire user session.

SSL
Secure Sockets Layer. SSL is a commonly-used protocol for managing the security of a message transmission on the Internet.

SNMP
A protocol used by network hosts to exchange information used in the management of networks.

Split-tunneling
Simultaneous direct access to a non-University network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into a University of West Georgia network via a VPN tunnel.

Spoofing
A generic term covering a range of computer network attacks whereby the attacker attempts to forge or intercede in a chain of communication. This can take a number of forms: email spoofing, IP spoofing and webpage spoofing.

Symmetric Cryptosystem - A method of encryption in which the same key is used for both encryption and decryption of the data.

TACACS+
Terminal Access Controller Access Control System. Authentication protocol that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual devices or systems.

Tunneling
Tunneling is the transmission of data intended for use only within a private network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network.

User Separation
Each computer and communication system user-ID should be unique and forever linked with the user to whom it has been assigned.

Virtual Private Network (VPN)
Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

X.509
Public key certificate standard developed as part of the X.500 directory specification. Used for secure management and distribution of digitally signed certificates across secure Internet networks