WILEY UNIVERSITY

Go Forth Inspired

Information Systems Policies and Procedures

Revision 11 — Final

Policy Title: Information Systems Policies and Procedures
Policy Type: Administrative
Policy Number: IS Policy #09-12-2024
Responsible Office: Office of Information Technology
Responsible Executive: Darren Ashley, Chief Technology Officer
Applies to: IT infrastructure Systems and End-users

Dr. Herman J. Felton, President and CEO
Submitted by George A. Stiell, Sr. Vice President for Business and Finance / CFO

Revision History

Revision	Date / Purpose	Person
1	June 3, 2003 (BOT Approval)	Terry Jordan, CIO
2	June 12, 2004 (Cab Approval)	N. E. Hewitt, CIO
3	February 17, 2004 (Rev)	N.E. Hewitt, CIO
4	September 26, 2005 (Rev)	N.E. Hewitt, CTO
5	October 3, 2005 (Cabinet approved revisions)	N.E. Hewitt, CTO
6	July 1, 2008 (review/update)	N.E. Hewitt, CTO
7	June 2, 2011 (review/update)	N.E. Hewitt, CTO
8	March 15, 2020 (review/update)	G. Stiell, SVP Bus & Fin
9	February 25, 2022 (review/update)	Darren Ashley, CTO
10	September 12, 2024 (review/update)	Darren Ashley, CTO
11	May 27, 2025 Adds Section 12.2 on personal wireless devices and network equipment	Darren Ashley, CTO

1.0 Introduction

The purpose of the Wiley University Information Systems Policies and Procedures Manual is to provide a guide for employees and students in the planning, acquisition, use, and management of information technology and telecommunications resources at Wiley University (WU). It assigns responsibility and defines the authority for implementing computer and network standards, operational standards, security policy and training, and is intended as a handbook for users, as well as an operations management tool.

The information technology resources at Wiley University, including computers, printers, local/wide/wireless area and telecommunications networks (LAN/WAN/WLAN/Telecom), software, electronic mail (e-mail), web sites, video, telephony (faculty, staff, and student), voice mail, and cable services are the property of the College and are provided for use by authorized students, faculty, and staff. Individuals who utilize these resources accept responsibility for their proper use.

2.0 College Mission

Wiley University, founded in 1873 in Marshall, Texas, is a historically black, primarily liberal arts, residential, co-educational, baccalaureate degree-granting institution affiliated with The United Methodist Church.

Committed to the principle of educational access, the College serves traditional and non-traditional students from diverse backgrounds who have expressed a desire and potential for learning in a Christian environment. The College, in fulfilling its basic purpose of providing a liberal arts education with a global focus, endeavors to provide an intellectually stimulating environment, promoting student competencies in communication, as well as, critical and analytical thinking. The College also supports spiritual, ethical, moral, and leadership development. To achieve these superordinate goals, the College promotes an atmosphere of academic freedom and employs a faculty committed to excellence and innovation in teaching, advising, and scholarship. The faculty provides a rigorous curriculum for preparing graduates for professional or graduate studies and/or productive careers in traditional and emerging career fields.

Wiley University is committed to shared governance and exemplary stewardship of its resources. The College employs innovative techniques and strategic planning in all its administrative processes, using cutting-edge technology in the delivery of services to its clientele. Acknowledging its covenant relationship with The United Methodist Church, the College affirms the ideal of social responsibility and seeks to contribute to the welfare and revitalization of its community. (Approved by the Wiley University Board of Trustees July 15, 2011.)

3.0 Information Systems and Technology Mission

The Information Systems and Technology Division (ISTD) exists to infuse information technology into all aspects of academic instruction and enhancement and business support functions; to develop faculty, students and staff in the use of information technology; to integrate information technology into planning, administrative, operational and academic activities of the College; to link and integrate the information technology infrastructure of the campus; and to provide responsive technical support to students, faculty, staff and community users.

4.0 Goals

The major goal of the Information Systems and Technology (ISTD) Division and its sub-components is to infuse College programs and operations with appropriate and cost-effective technologies that will measurably improve information access and management, impact student learning and scholarship, increase research initiatives, and streamline academic and administrative processes. ISTD will collaborate with departments and divisions to insure that the skills, tools, and information needed to succeed are available.

4.1 Academic Instructional Technology

Instructional technology is the infrastructure and process needed for the effective application of technology to instruction. ISTD supports instructional technology by focusing on using the Internet to enhance instruction to students, on campus, across the state, or around the world. The Internet allows cost-effective sharing and leveraging of the College's expertise in teaching with global citizens, breaks down barriers, and provides lifelong learning opportunities for many people.

As new technologies, such as multimedia presentations, course management systems, and Web-enabled course tools are deployed; active student-centered learning environments are created where instructors serve as facilitators, collaborators, coaches, and consultants. These technologies enable highly individualized, self-directed learning experiences unrestricted by time and location.

4.2 Administrative Information Systems and Operations

ISTD support for administrative systems and operations involves delivering reliable, secure, and efficient technology to simplify and streamline administrative processes. ISTD, in consultation with users, proposes strategic investments that will position information technology to both promote and serve the College's mission.

4.3 Community Outreach and Service

ISTD will support the College's goal for community service by designing and deploying an information technology infrastructure that is accessible to residents from the surrounding areas who are participants in College-sponsored activities and programs. An accessible infrastructure can help build communities of

interest and expertise, enhance collaboration and professional relationships, and leverage College expertise and resources to help solve community problems.

5.0 Guiding Principles

Information technology policies and procedures are guided by a set of principles that affect short- and long-term strategic decision-making:

- IT policies and procedures will support the College's mission and vision.
- Policies emanate from the highest level of authority of the College and therefore apply to all aspects of academic and business operations.
- The Chief Technology Officer (CTO) is the responsible authority for all College IT and technology-related systems, including computer hardware, software, networks, telecommunications (voice, audio and video), and related peripherals. The CTO receives policy mandates from the Wiley University Board of Trustees, the President and Cabinet.
- All users will be treated equitably in the allocation of resources and in the provision of technical support.
- All information technology activities will be conducted in accordance with industry standards and applicable state and federal guidelines including copyright laws, as they apply in the academic and administrative environments.
- All uses of information technology resources shall be managed and enforced under the guidelines found in the Wiley University Security Policy Manual.

6.0 Organizational Structure

The organizational structure for the Information Systems and Technology Division (ISTD) consists of the Chief Technology Officer (CTO), an Assistant Vice President of Information Systems and Technology, an Associate Vice President for Administrative Information Systems and other support staff. This structure includes a collective of components of necessary support services in four functional groups: Helpdesk and Technical Support Services, Administrative Information Systems, Academic Information Technology, and Network Systems Engineering.

6.1 Technical Support Services

Technical Support Services unit is a component of the ISTD that is housed within the office of the CTO. It is managed through the Helpdesk and is responsible for responding to and coordinating all user support services (technical and technological). The key service areas for this component include:

- Helpdesk (technical support services)
- Hardware/software support
- Training requests (general and specific)

6.2 Administrative Information Systems

The Administrative Information Systems unit provides support for and manages access to all institutional database resources, information systems, service and support for College administration and staff to manage business processes and to facilitate effective decision-making. It responds to the needs and questions of users concerning access to network resources and the operation of various software programs. The major administrative service areas include:

- Applications development
- Database administration
- End user application and portal support
- Administrative systems applications training and portal

6.3 Academic Information Technology

The Academic Information Technology unit provides support for planning, coordination, implementation and evaluation of academic technologies intended to enhance teaching and learning. It leads initiatives in faculty and student technology skill development and web-based instruction, as well as provides a liaison between information technology and academic departments. The main service areas include:

- Management systems – Jenzabar Enterprise Resource Planning System and Internet Campus Solution (JICS)
- Canvas
- Computer labs
- End-user training

6.4 Networked Systems Engineering

The Networked Systems Engineering unit is responsible for designing, installing, and maintaining the institution's technical infrastructure. This includes the management of local, wireless, and wide area networks, hardware, software, and network related resources. This includes network communications systems software, software applications, security policies, network security applications and monitoring, servers, routers, bridges, switches, modems, and cabling. The key network service areas include:

- Remote and virtual resources
- Email
- Network engineering
- Telecommunication engineering
- LAN/WAN/wireless networks
- Video-conferencing systems
- Information systems security
- VOIP (Voice over IP)
- Residential telecommunications services (cable/phone/security)
- Network, support and security training

- Access control and surveillance

6.5 Information Systems Security Team

The purpose of the Information Systems Security Team (ISST) is to ensure that all information systems are in compliance with the College's established security policies and procedures plan; to provide faculty, staff and students with on-going information systems security training; to enforce established information systems security policies and procedures and to install, manage and monitor physical and digital network security, back-up, and disaster recovery policies.

6.5.1 Chief Security Officer

The Chief Technology Officer will serve as Chief Security Officer. The Chief Security Officer is responsible for establishing and enforcing the College's security posture, both physical and digital. The major responsibilities include:

- Managing network security personnel and vendors who are responsible (or contracted) to support the College's information systems, assets and digitized intellectual property.
- Identifying information systems security goals, objectives and metrics consistent with the strategic plan of the College.
- Managing the development and implementation of the College's information security policy, standards, guidelines and procedures to ensure ongoing maintenance of security.
- Implementing and enforcing policies and procedures that ensure the safety (and security) of the College's data, physical and digital assets (hardware, software and associated equipment), and access control systems. This includes infrastructure architecture, access and monitoring policies, and training/awareness.
- Providing guidance to the Cabinet on prioritizing security initiatives and spending based on appropriate risk management and/or financial methodology.
- Maintaining relationships with local, state and federal law enforcement and other related government agencies.
- Coordinating disaster planning and recovery.
- Coordinating investigations of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.
- Working with outside consultants as appropriate for independent security audits.

6.5.2 Network Security Officer

The Network Engineer will serve as the Network Systems Security Officer (NSSO). The NSSO is responsible for managing and enforcing security policies (physical and digital) on all network systems, monitoring security systems, conducting annual (and random) system audits and providing training and guidance on best security practices such as:

- Managing, maintaining and monitoring all network systems.
- Providing and monitoring access to network resources (including the provision of necessary credentials).

- Working with vendors responsible for or contracted to support the College's information systems, assets and digitized intellectual property.
- Enforcing the College's information security policy, standards, guidelines and procedures to ensure ongoing maintenance of security.
- Ensuring the safety (and security) of the College's data, physical and digital assets (hardware, software and associated equipment), and accessing control systems. This includes infrastructure architecture, access and monitoring policies, and training/awareness.
- Providing guidance to the Chief Security Officer on security initiatives based on appropriate risk management methodology.
- Maintaining relationships with local, state and federal law enforcement and other related government agencies.
- Assisting the Chief Security Officer with disaster planning and recovery.
- Assisting the Chief Security Officer with investigations of security breaches, and assisting with disciplinary and legal matters associated with such breaches as necessary.

6.5.3 Data Systems Security Officer

The Database Administrator will serve as the Data Systems Security Officer. The Data Systems Security Officer is responsible for managing and enforcing security policies (physical and digital) on the College's administrative information/data systems, monitoring security systems, conducting annual (and random) system audits and providing training and guidance on best security practices including:

- Managing, maintaining and monitoring the College's administrative information (database) systems.
- Providing and managing access to database resources (including the provision of necessary credentials).
- Working with vendors responsible for or contracted to support the College's information systems, assets and digitized intellectual property.
- Enforcing the College's information security policy, standards, guidelines and procedures to ensure ongoing maintenance of security.
- Providing guidance to the Chief Security Officer on security initiatives based on appropriate risk management methodology.
- Assisting the Chief Security Officer with disaster planning and recovery.
- Assisting the Chief Security Officer with investigations of security breaches, and assisting with disciplinary and legal matters associated with such breaches as necessary.

6.6 Disaster Recovery Team

The purpose of the Disaster Recovery Team is to provide support for data recovery in the event of a natural disaster or emergency that may disrupt information systems operational status. In the case of a natural disaster or emergency, the Vice President for Information Systems (or designee) will serve as the Disaster Recovery Team leader and will be responsible for the coordination of all data recovery activities. Individual team members will be assigned to assist with the coordination and support of

recovery efforts within each major area of the College. Specific responsibilities of this team are listed below and included in the Wiley University Disaster Recovery Plan. The responsibilities of the Disaster Recovery Team include:

- Determining the extent and seriousness of the disaster.
- Immediately notifying the President and Executive Vice President and keeping them informed of the activities and recovery progress.
- Invoking the Disaster Recovery Plan with approval from the President, Executive Vice President, or the senior administrator who is available.
- Coordinating the re-route of all critical data and network services with alternate recovery locations/institutions (if crisis deems appropriate).
- Coordinating the appropriate personnel to assist with all hardware and data recovery efforts (if crisis deems appropriate).
- Supervising the recovery activities.
- Coordinating with the President and Cabinet on priorities for clients while going from partial to full recovery.
- Naming replacements, when needed, to fill in for any disabled or absent disaster recovery team members. Any members who are out of town and are needed will be notified to return.

The Chief Technology Officer and the Disaster Recovery Team, in conjunction with the Director of Public Relations, will keep all College constituents informed regarding recovery activities and status.

7.0 Access to Information Technology Resources

Computers, networks and electronic information systems are essential resources for accomplishing the Wiley University mission. The College grants users shared access to these resources in an effort to support the accomplishment of its mission. Such access is a privilege, not a right, and users should be aware of the responsibilities associated with this privilege.

7.1 Eligibility

Every student will be provided credentials to access the College Portal (My Wiley) upon completion of the registration process. This account will remain active for life for all students and alumni. In addition, all enrolled students will be provided with access to College governed Google Email accounts, which will remain active for life.

All regular full-time and part-time employees requiring access to information systems as part of their job responsibilities are provided a network user's account upon hiring. Temporary employees are not eligible unless they receive special permission from their immediate supervisor and appropriate vice president. In this case, the supervisor must send a written request to ISTD for an account and notify ISTD upon completion of temporary assignment. Accounts assigned to workers, students or others are the property of Wiley University.

7.2 User Names

The network/computer "Username" must be unique for proper user authentication and secure access to network/computer resources. The standard naming convention for the network/computer "Username" consists of the first initial of the first name, middle initial (if available), followed by the last name. If duplications are found, a number will be added to the last name. The following examples are provided:

The person's name is John M. Doe.

Example 1 (the Username would be jmdoe and is unique): Username: jmdoe

Example 2 (the Username would be jmdoe1 as jmdoe was not unique): Username: jmdoe1

Note: Typically, the Username is also incorporated in the e-mail address, as it too must be unique for proper routing over computer networks. Listed below are e-mail addresses that follow the same naming conventions as aforementioned.

Examples: jmdoe@wileyc.edu or jmdoe1@wileyc.edu

7.3 Campus Network Connectivity

All offices, laboratories, classrooms and other applicable areas on campus are wired for physical and/or wireless access to the computer network. Any department that requires additional network connections should seek approval from the appropriate vice president who will request the service through the Information Systems and Technology Division Helpdesk (support@wileyc.edu or (903) 927-3310).

7.4 Residence Centers Network Connectivity and Resources

Residence Center connections are intended to provide students with access to campus computing services and resources, the Internet, telephony (voice services), and cable. The College does not provide peripheral connection equipment, such as phones, cables (category 5 for network or RJ45 for phone), splitters (cable), etc.

7.4.1 Residence Center Network Access

While each room is equipped with a physical network connection, students with IT certified wireless computing equipment also have access to Wiley University's "WCGoForth" wireless network (WLAN).

Each residence center is equipped with a mini-computer lab equipped with 5-10 computers, a networked printer, and access to the Wiley University network (WAN/WLAN). Residence center labs schedules are posted in public areas.

7.4.2 Residence Center Cable Television Services

If residents require technical support for television services, they are to contact the Helpdesk (support@wileyc.edu or (903) 927-3310) for assistance.

7.4.3 Residence Center Phone Service

Residents are provided local telephone services within each room. One phone number is assigned to the room and not the individual.

Students are encouraged to purchase calling cards from local vendors for long distance services.

Student directories are compiled and e-mailed to resident center management each semester.

If residents require technical support for telephone services, they are to contact the Helpdesk (support@wileyc.edu or (903) 927-3310) for assistance.

7.5 Off-Campus Connectivity

Off-campus users may access network resources by connecting to the College web site, portal and library resources using their user name and password.

If users require technical support, they are to contact the Helpdesk (support@wileyc.edu or (903) 927-3310) for assistance.

8.0 Equipment

The goal of the College is to provide technology needed to maximize educational opportunities for students, faculty and staff in the support of administrative functions. Any department that needs additional equipment should seek approval from the appropriate vice president. The ISTD must approve all technology equipment requests to ensure compliance with the College's standards and policies.

Requests for personal equipment that may be used to access the Wiley University network must be submitted in writing to the appropriate vice president and approved by the ISTD for network compatibility and support. Personal equipment to be attached to the Wiley University network must have antivirus software or other appropriate safeguards to help protect the integrity of the network.

Questions regarding these network protection safeguards may be sent to the Wiley University Help Desk (support@wileyc.edu or (903) 927-3310) for assistance.

8.1 Equipment Standards

Many of the proposed improvements in information technology depend upon the establishment of campus-wide standards for hardware, software and systems. This is essential for effectively sharing information. Therefore, no campus group or individual will be allowed to introduce technology onto the College network that is outside of and/or incompatible with the standard hardware and software. The Chief Technology Officer or designee should approve all technology requisitions in order to insure that equipment (and applications) comply with the College's standards at the time of order/purchase.

8.1.1 Technology-Related Vendor Selection

All technology-related purchases must be made through a college-approved vendor. Purchases made outside of the approved vendor list must be approved by the division vice president, Vice President for Information Systems and Technology, and the Vice President for Business and Finance.

8.1.2 Computer Purchases

All computers connected to the Wiley University network must meet the minimum standards established by the College. The configurations listed below will satisfy most office requirements:

PC Specifications

Desktop: Intel Core i7 Processor, 3.1GHz, 6M Cache; 8GB Dual Channel DDR3 SDRAM at 1333MHz (4 DIMMs) Memory; 512GB SATA 3.0 7200RPM; Windows 11 Professional Operating System with appropriate service pack; 256 Video Adapter; 16X DVD+/-RW; USB Keyboard and Optical USB Mouse; Ethernet Port; 22 inch Analog Flat Panel Monitor.

Laptop: Intel Core i7 Processor, 3.1GHz, 6M Cache; 8GB Dual Channel DDR3 SDRAM at 1333MHz Memory; 250GB SATA 3.0 7200RPM; Windows 10 Professional Operating System with appropriate service pack; Intel HD Graphics 3000 w/1.6GB Dynamic Memory Video Adapter; 8X DVD+/-RW; Ethernet Port; 802.11 N/AC Wireless LAN.

In all cases, an AppleCare Protection Plan agreement is required.

Mac (Apple) Specifications

Desktop (iMac): Intel Core i7 Processor, 2.5GHz, 6M Cache; 8GB Dual Channel DDR3 SDRAM at 1333MHz Memory; 500GB SATA 3.0 7200RPM; OS Monterey 12.0.X Operating System.

Laptop (MacBook Pro): Intel Core i5 Processor, 2.4GHz, 3M Cache; 4GB SO-DIMMs at 1333MHz DDR3 (2 DIMMs) Memory; 500GB SATA 3.0 7200RPM; OS X Lion 10.7.X Operating System.

In all cases, an AppleCare Protection Plan agreement is required.

Apple iPad

Presently, there are two versions of the Apple iPad. All versions will meet the College minimum specifications.

The Apple iPad 10 and Air and the New iPad currently has two color choices (black or white) and Memory configurations consisting of 64GB or 128GB.

A primary model distinction is how the iPad fundamentally connects to the Internet as follows: Wi-Fi Model — Connects to the Internet over a Wi-Fi network. In this case, the user must have viable access to a Wi-Fi network to access the Internet.

All requisitions for technology equipment require the appropriate approvals including the division vice president and the Chief Technology Officer as applicable.

8.2 Assignment of Computers

Wiley University provides desktop computers to all regular faculty and staff members where appropriate. Administrative and professional employees, who are required to travel extensively for work-related duties, or hold jobs that require them to work regular and significant numbers of evening and weekend hours beyond the normal workweek, may be assigned a laptop computer, as approved through their department and the ISTD. In general, the ISTD is not responsible for providing laptop computers.

Laptop computers may be requested for use on a temporary basis for some special projects, as available, but must be requested and approved by the vice president for the division and Vice President for Information Systems and Technology. The request must be made through email by contacting the Helpdesk (support@wileyc.edu) to begin processing the request.

In all cases, approval must be obtained from the appropriate supervisor, vice president, and Vice President for Information Systems and Technology. An Equipment Check List form, available through the Helpdesk (support@wileyc.edu or (903) 927-3310), must be signed by the recipient of the laptop to acknowledge acceptance of the use and care guidelines.

8.3 Faculty and Staff Technology Purchases

Vendors will often contact faculty and staff members about technology (and purchase programs) at the same or similar price as the institution that is using their products. Regularly, ISTD and the Office of Business and Finance will negotiate such agreements with vendors and make the faculty and staff aware of these discount programs. However, the College is under no obligation to provide discount programs in this regard.

Faculty and staff members may arrange to purchase technology through payroll deduction as governed and approved by the College. Financial arrangements for the purchase of equipment will be between the individual College faculty/staff member and the College Office of Business and Finance.

Purchase arrangements cannot exceed 12 months. Additionally, the financial balance must be paid in full by the end of employee contracts with the College or at separation/termination.

8.4 Student Technology Purchases

At Wiley University, students are encouraged to utilize technology to support their learning experiences. Students may have the opportunity to purchase technology through the College's approved vendors where these arrangements have been qualified and approved. In all cases, student purchases must be configured and approved by the ISTD prior to any purchase processing through College approved vendors:

8.4.1 Direct Payment

Students may purchase a laptop (or desktop) computer from the approved vendor based upon their qualification and purchase arrangement policies and guidelines. Alternatively, based upon qualification, payment arrangements may be made through the College Office of Business and Finance.

8.4.2 Financial Aid Purchase

Governed by the Financial Aid and Business & Finance offices, approved students may be reviewed to determine if they qualify to use financial aid funds to purchase a computer. Available and approved financial aid funds may be used to purchase or supplement the funds necessary to purchase the computer.

8.5 Grant-Funded Equipment

Individuals pursuing grants for computing equipment are required to discuss their plans with their divisional vice president and the CTOD. The CTOD or designated alternate must approve all technology requisitions to ensure the compatibility and compliance with College networks and computing resources. The College's policies and procedures for grant approval are to be followed in all instances. Computing equipment acquired under grants will be entered into the College inventory system and may be upgraded under standard cycles as applicable and approved. All grant-funded equipment should be ordered through the College's purchasing process and will not be upgraded or replaced by the College. Exceptions include cases where grant funds have been allocated for maintenance, upgrade or replacement purposes.

The College will retain ownership of all general purpose computing equipment that is purchased through a grant. Any special use equipment, such as that used in the science disciplines, will be subject to grant terms and conditions. A written consent must be obtained from the funding agency prior to the disposal of equipment considered to be outdated.

8.6 Printers and Other Peripheral Equipment

The College strives to provide network-printing locations for workgroup clusters. Some departments may be provided with at least one non-networked printing location based upon departmental needs. Individual desktop printers may be provided depending on the unit's availability of funds and adherence to applicable College policy and guidelines.

Color printers are not typically provided for individual offices for general printing purposes due to the high equipment, maintenance and supplies costs except in cases where it is justified. Requests for color printers should be made to the appropriate vice president who, in turn, will present a recommendation with justification to the President's Cabinet.

8.7 Upgrades and Replacements

Wiley University ISTD will upgrade technology equipment based upon application requirements, availability of upgrade funds and applicable equipment life cycle schedules (approximately 3-5 years), in some instances. The ISTD staff will consult with users prior to ordering and installing new equipment to determine current and anticipated application requirements. The Office of Sponsored Programs monitors grant funded technology equipment to help determine whether funds are availability and applicable for equipment upgrades and/or replacements. The Office of Sponsored Programs, the Office for Business and Finance and the ISTD will collaborate in some instances, to make recommendations to reassign, sell, or otherwise dispose of the equipment with the proper approvals.

8.8 Equipment Repairs

The ISTD is responsible for initiating repair for equipment owned by Wiley University. Whenever possible, service will be provided at the on-site location. Wiley University-owned equipment that is approved for off-campus use must be returned to the campus for repairs as applicable. Problems should be reported immediately to the HelpDesk by email at support@wileyc.edu.

In order to more effectively manage technical support requests, a College Service Level Agreement (CSLA) has been defined. Given the importance of every user's technical support needs, each problem call will be responded to promptly depending on severity and other planning guidelines in accordance with the CSLA as defined below:

1. Emergency/Critical – technical problems that impact academic instruction and/or the operation of the College, or impact a large number of users; for example, a network failure.
2. Urgent – technical problems that affect a department(s), but not the entire College.
3. Important – technical problems that affect one person, where their use of technology is impacted, but various alternatives may be available until the problem is resolved such as temporarily using another computer.

8.9 Personal Equipment

Wiley University ISTD will provide a Tier 1 level of support for student, faculty and staff personal computers. Tier 1 support is defined as:

- Limited software installation support
- Limited software troubleshooting and design support
- Limited assistance with hardware installation (peripherals)
- Printer support
- Select training

Wiley University will not maintain, repair or upgrade personally owned computers or facilitate warranty work.

9.0 Software

Software is a critical element in building reliable and efficient information systems. It may be developed in-house or purchased from an outside vendor. In-house software development will be pursued only if no commercially available software can be found that meets application requirements. ISTD is responsible for managing the purchasing of software that will affect multiple groups, departments, or the entire campus. The ISTD will recommend specific vendors as applicable based upon standards compliance, College guidelines and funding sources. The division head and the CTOD must approve technology related software purchases prior to purchase and installation.

9.1 Software Standards

Software standards must be maintained in order to facilitate compatibility with computing hardware requirements.

Listed below are the current baseline standards for software utilized on any computer on the Wiley University network:

PC Software

- Microsoft Windows 7 Professional operating system with applicable Service Packs
- Microsoft Office 2010 with applicable Service Packs
- Microsoft Internet Explorer version 7 or above, Firefox version 10.x or above
- Adobe Acrobat Reader 10.x or above
- Antivirus/Malware protection
- Skype Free (latest version)

Mac (Apple) Software

- Mac OS X 10.7.x or above with applicable updates
- Microsoft Office for Mac with applicable updates
- Firefox version 10.x or above
- Antivirus/Malware protection
- Skype Free (latest version)

The College has site licenses for most of the software listed above that is applicable to all users — faculty, staff, and students. Note: due to software licensing agreements, all software may not be available campus-wide; there may be restrictions. The ISTD will not install any unauthorized software on Wiley University equipment. If unauthorized software is discovered on a Wiley University computer, it will be removed immediately and/or reported to the President, CTO, and division vice president for appropriate action.

9.2 Licensing

The use of all software at the College is protected by copyright laws and must be used in accordance with software licenses. All software licenses will be maintained by the ISTD.

Please Note: It is against College policy to copy or reproduce any licensed software. This includes downloading music and video files from the Internet or duplicating CDs for commercial purposes.

The unauthorized use or copying of software is a serious violation of policy and violators will be subject to disciplinary action. Such unauthorized use or copying may also subject the offending individual to legal litigation.

9.3 Faculty and Staff Software Purchases

Vendors often make software available to faculty and staff at the same or similar price as the institution that is using their software products. The ISTD and the Office of Business and Finance will negotiate such agreements with vendors, when possible, and ensure that the targeted group is aware of the discount programs.

9.4 Wiley University Software on Personal Equipment

Wiley University's educational licensing agreements for software are specifically limited to installation on College owned equipment. Therefore, software purchased by Wiley University under these agreements is not to be installed or distributed on personal equipment.

9.5 Personal Software

User owned software should not be loaded on Wiley University equipment. This constitutes illegal use of the end-user licensing agreement for the software. Violators of this agreement will be subject to disciplinary action and may also be subjected to lawsuits by third parties.

10.0 Training

Faculty and staff members may contact the Helpdesk (support@wileyc.edu) to schedule available technology training. Training will be scheduled upon request.

11.0 E-mail

E-mail addresses are assigned to individual users in accordance with College e-mail standards and policy.

Please Note: E-mail addresses are considered public information and may be listed in various College documents and other applicable and appropriate communications media.

11.1 Appropriate Use of E-mail

Access to individual e-mail accounts requires proper authentication. The access methodology includes a Username and Password. A Username and temporary Password will be assigned when an e-mail account is created. College policy requires users to change their temporary Password to a private password that

meets standards outlined in Section 13.0. The e-mail password is considered private and should not be shared with others. Any person issued a Wiley University e-mail account is expected to manage the privacy of their e-mail password. This is a necessary College information access security policy.

Wiley University strongly recommends that e-mail not be used for confidential communication. E-mail is an official means of communication for the College. It is a formal written record with similar legal weight as a formal memorandum. Users should be aware that e-mail messages become the possession of the receiver and easily can be duplicated and redistributed by recipients. Messages that have been deleted can be retained unintentionally on system backup files. In addition, secure passwords are not completely confidential. A message that should not be preserved must be deleted immediately. State and federal laws, especially in regard to copyrighted material, photographic images and libelous remarks, also govern e-mail.

College policy prohibits certain types of e-mail. These include messages that may be perceived as pornographic, harassment, political campaigns or commercial solicitations. "Chain-mail" and "SPAM" are also prohibited because they consume large amounts of system resources.

Certain types of e-mail, including, but not limited to, harassing e-mail, may subject the sender to civil or criminal penalties. In spite of College policy, malicious users who know the owner's network account and password have the potential to abuse the e-mail system. Users are responsible for protecting their own passwords. These policies will be enforced when violators are brought to the attention of the College administration.

Access to and use of e-mail is a privilege and should be treated as such by all users. The use of e-mail to participate in any unlawful act is illegal and may result in prosecution by state and federal authorities. Use of e-mail for private business purposes unrelated to the College is NOT authorized.

All e-mail sent through the Wiley University Email System (Microsoft Exchange Server) will include the following disclaimer and confidentiality statement:

> *This e-mail and any attachments are intended only for use by the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution or copying of this e-mail, and any attachments thereto, is strictly prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

12.0 Security

In order to minimize security risks and comply with applicable College, state and federal laws, policies and guidelines and to help prevent service disruptions on Wiley University's networks, students, faculty, and staff are asked to observe the following:

- Do not reconfigure the network portion of your computer's setup. This may result in network congestion, thus impacting the College's network operations.
- Do not change the name of your computer under network setup.
- Personally owned computers cannot be used on the Wiley University network, unless authorized by the ISTD in accordance with College policy and guidelines.
- Do not setup a computer server of any type without written approval and confirmation from the ISTD.
- Do not allow someone else to use your e-mail address, password, or other forms of personal authentication to College secured network/computing resources.

Some abusers may attempt to mask ownership of a particular machine for purposes of fraud or harassment. Using the network and e-mail to participate in such acts is illegal and may be subject to disciplinary action by the College and/or prosecution by state and federal authorities.

All Wiley University network access requires user authentication using a Username and Password.

User Responsibility for Technology Equipment

Individual users are responsible for safeguarding the equipment entrusted to them by the College. This includes reasonable protection of equipment from damage and theft.

Note: If equipment has been stolen, the user must notify his/her division dean, vice president, Security, and the ISTD immediately.

For additional information concerning security policies, refer to the Wiley University Security Policy Manual.

12.2 Personal Wireless Devices, Routers, and Network Equipment

To preserve the integrity, security, and performance of the Wiley University network (LAN/WAN/WLAN), users may not install, connect, or operate personal network infrastructure equipment on or adjacent to the College network without prior written authorization from the Information Systems and Technology Division (ISTD). This policy applies to all faculty, staff, students, contractors, and guests on Wiley University property, including residence centers.

12.2.1 Prohibited Equipment

The following devices may not be connected to the Wiley University wired or wireless network, nor operated on College property in a manner that broadcasts a competing or overlapping wireless signal:

- Wireless routers, wireless access points (APs), and mesh networking nodes
- Personal/portable WiFi hotspots and MiFi devices used to extend or bridge the College network
- Network switches, hubs, and unmanaged bridges
- Range extenders, repeaters, and signal boosters
- Powerline networking adapters connected to College network ports

- Any device configured to provide DHCP, DNS, NAT, or routing services on a College network segment
- Any device that creates an unauthorized wireless SSID on or near campus

Operating such equipment constitutes "Connecting unauthorized equipment to the campus network" as defined in Section 19.3 (Inappropriate Access) and may also constitute setting up an unauthorized server as defined in Section 12.0 (Security).

12.2.2 Rationale

Unauthorized wireless and networking equipment creates the following risks to the College:

- Radio frequency (RF) interference with the WCGoForth WLAN, degrading service for all users in the affected area
- Security exposure through rogue access points that bypass College perimeter controls, content filtering, and intrusion prevention
- Network instability caused by rogue DHCP servers issuing conflicting IP addresses
- Compliance risk under applicable federal regulations and the College's data protection obligations
- Inability to support or troubleshoot issues on segments containing unmanaged equipment

12.2.3 Personal Cellular Hotspots

Personal cellular hotspots that operate solely over a user's own cellular data plan and are used exclusively for that user's personal devices (not connected to the College wired network and not shared with other users) are permitted, provided they do not interfere with the College WLAN. ISTD reserves the right to require deactivation of any personal hotspot that causes RF interference or is used to circumvent College network controls.

12.2.4 Residence Centers

Residence center rooms are provided with both wired network access and coverage by the WCGoForth wireless network as described in Section 7.4. Residents may not install personal wireless routers or access points in residence center rooms. Residents experiencing wireless coverage or performance issues should contact the Helpdesk (support@wileyc.edu or (903) 927-3310) rather than installing personal equipment.

12.2.5 Approved Exceptions

Departments or individuals with a legitimate academic, research, or operational need for specialized networking equipment may submit a written request to ISTD through the Helpdesk. The request must include:

- Business or academic justification
- Equipment make, model, and intended configuration
- Physical location and operating area

- Identification of the requesting department and responsible individual
- Proposed duration of use

ISTD will evaluate the request for network compatibility, security posture, and RF impact. Approved equipment must be configured, deployed, and monitored by or under the direct supervision of ISTD. Approval may be revoked at any time if the equipment is found to interfere with College operations.

12.2.6 Enforcement

ISTD conducts periodic and on-demand wireless surveys and network audits to identify unauthorized equipment. Upon discovery of a violation:

4. The device will be immediately disconnected from the network or, in the case of a wireless device, the responsible user will be required to power it down.
5. The user will be notified through their Wiley University email account.
6. Repeated or willful violations will be referred to the appropriate vice president and may result in disciplinary action under Section 19.5 (Schedule of Penalties), including suspension of computing privileges.
7. Equipment that cannot be attributed to a specific user and is found to be actively interfering with College operations may be confiscated by ISTD and held pending identification of the owner.

12.2.7 Questions

Questions regarding this policy, or requests for evaluation of specific equipment, should be directed to the ISTD Helpdesk at support@wileyc.edu or (903) 927-3310.

13.0 User Accounts and Passwords

Only the person responsible for the assigned account should have access to the password. Access to user accounts may not be loaned and/or sold. Any suspected breach of password security should be reported immediately to the ISTD HelpDesk (support@wileyc.edu or (903) 927-3310). Listed below are some common rules to follow in protecting one's password:

- Do not store passwords at any workstation that can be used to gain access to computing resources.
- Never share passwords; and never tape passwords to a wall or under a keyboard or write them down on paper.

As part of routine operations, the College will randomly test access to network accounts and other computing services made directly or indirectly available to the campus community. Suspected policy violations discovered during such routine operations will be reported to the CTOD and/or other appropriate College officials. All other information accessed during such routine operations will be treated as confidential, except as otherwise required by this policy, state, or federal law.

The College will report suspected criminal activity to law enforcement authorities. Unless otherwise prohibited by law, and subject to legal requirements, the College and law enforcement personnel may access computers, network accounts, electronic information or technology necessary to investigate suspected violations of this policy or unlawful activity.

Wiley University students and employees are strongly encouraged to remove all "personal" information stored on their computers (or network accounts) prior to ending their relationship with the College. Generally, the College will destroy information left on computers and network accounts. Information will be retained if retention is in the College's best interest.

14.0 Paper Printouts

Everyone is responsible for picking up his/her printer output in a timely fashion to avoid theft or disposal. Documents should be edited prior to printing for mistakes, grammar usage and format. Do not print unnecessary copies from the Internet. When using the Internet as a research tool, it is strongly recommended that users copy the information they wish to use to a word processing document along with the URL for the Web page. The report should be created from the word processing document. Please be aware of copyright restrictions. For clarification of copyright restrictions, contact the Wiley University Reference Librarian at extension 3271 or the ISTD HelpDesk (support@wileyc.edu or (903) 927-3310).

15.0 Operations and Maintenance

The ISTD staff is responsible for providing advance notice of system shutdowns for maintenance, upgrades, and/or changes so that users may plan around periods of system unavailability. Every effort will be made to provide users the opportunity to save their work and log out safely before the system is taken out of service. The ISTD staff will undertake reasonable efforts to maintain the privacy of a user's files, electronic mail, and printer listings.

Data Backup

Files stored on desktop equipment are the responsibility of the user. Users must backup critical work files on a regular basis. ISTD will provide training and assistance to users and departments requiring assistance in backing up critical work files and other College mission critical digital data.

The ISTD maintains standard backup policies and guidelines for College mission critical technology-based systems. These backup standards are designed to help recover and restore digital data in the advent of data loss or corruption.

These mission critical systems include:

- Jenzabar (Enterprise Resource Planning (ERP) system)
- Microsoft Exchange Server (E-mail platform)

- Virtual Servers (PC Desktop Hard Drive Images)
- ISTD Network Shared Drives

16.0 Institutional Privileges

Wiley University reserves the right to allocate (reallocate) resources necessary to complete the mission of the institution. To accomplish this, the system administrator, by direction of the President, may suspend or terminate privileges of individuals without notice. There are occasions when privileges may be suspended to meet critical operational needs. In addition, the system administrator may place a storage limit on a user's network account.

17.0 Legal Compliance

All existing federal and state laws and the College's regulations and policies apply to the use of campus computing resources. Users of such resources are required to be in compliance with the laws, regulations and policies at all times. These are not limited only to laws and regulations that are specific to computer and network usage, but those that apply to personal conduct.

Individuals are responsible for ensuring that their activities comply with copyright laws. Copyright laws apply to all materials published on the web, unless the site specifically states otherwise. Users must seek permission from owners to use materials, text or graphics, from any web site.

18.0 Indemnification of Wiley University

Upon the granting of access to the College's computers and networking services, users agree to indemnify, defend, and hold harmless the College from any suits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the College's computer resources and all other media services and facilities.

19.0 Noncompliance and Sanctions

The ISTD, in consultation with the appropriate vice president or the Executive Vice President, will suspend or terminate all computing privileges of any individuals who engage in improper computing activities. Serious cases, as determined by ISTD, will be referred to the President for consideration of further disciplinary action, which may include, but may not be limited to the suspension, expulsion, or termination of the offending individuals, as deemed appropriate. Where violations of state and federal laws are involved, the cases may be referred to the proper legal authorities for action.

The following serves to provide various examples of violations of policies governing Wiley University computing and/or computing facilities.

19.1 Malicious Misuse

Examples of malicious use include:

- Using accounts or passwords assigned to others; disrupting the network
- Destroying information; removing software from public computers
- Spreading viruses
- Sending e-mail that threatens or harasses other people (a Class A misdemeanor under Texas State law)
- Invading the privacy of others, and subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their approval

19.2 Unacceptable Use of Software and Hardware

Some examples of unacceptable use of software and hardware include the following:

- Installing or using unlicensed software on any computer system or network
- Giving another user a program intended to damage the system
- Unauthorized running or installation of any program that places an excessive load on a computer system or network
- Violating software licensing agreement
- Violating copyright laws
- Improper application of fair use provisions that includes the inappropriate reproduction or dissemination of copyrighted text, images, or other materials, and the use of imaging equipment to duplicate, alter and/or reproduce official documents

19.3 Inappropriate Access

Inappropriate access may be regarded as any of the following:

- Unauthorized use of a network account
- Providing misleading information in order to obtain access to computing facilities
- Using the campus network to gain unauthorized access to any computer system
- Connecting unauthorized equipment to the campus network
- Unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data)
- Knowingly or carelessly performing any act that will interfere with the normal operation of computers, terminals, peripherals, or networks, and deliberately wasting or overloading computing resources, such as printing too many copies of a document

19.4 Responsibility for Equipment

Every employee is responsible for taking reasonable precautions to safeguard Wiley University-owned computer equipment. Employees will be held responsible for excessive damages to such equipment arising out of their negligence or intentional misconduct.

19.5 Schedule of Penalties

Wiley University may impose the following penalties on users who continuously misuse the services provided:

Minimum of Three Days to One Week Suspension

Disruptive or abusive use of electronic mail, locally or over external networks. For example:

- Sending an electronic chain letter
- Sending an unsolicited message, mail or communication of any kind to persons who have not requested it or who cannot be expected to welcome such communication
- Frequent frivolous use of computing resources
- Intentionally distracting others who are using computing facilities
- Smoking, eating, or drinking in any personal computer laboratory
- Use of Wiley College computing resources for commercial soliciting or advertising of any kind

Minimum of Three Months Suspension

"Lending" an account or online disk storage to another person. Using an account or online disk storage that belongs to another person.

Minimum of Six Months Suspension

Using a stolen account.

Grounds for Termination

Use of computer resources to defame, defile, attack, scandalize, or otherwise damage the institution or any representation thereof.

Additional Penalties: Wiley University will consider additional penalties for continuing abuses of privileges. These penalties include, but are not limited to:

- Civil and criminal penalties in cases of infringement of copyright laws for the use and reproduction of Wiley University site licensed microcomputer software
- Monetary charges for illegally using computing resources

20.0 Guidelines for Web Site

Wiley University is a church-related institution and is therefore committed to maintaining the highest educational and ethical standards. The Wiley University web site is an official publication, in electronic format, and is subject to the same review and approval process required for official written materials.

General responsibilities for updating and maintaining the institutional web site reside with the Webmaster, in consultation with division representatives, with final approval from the Executive Vice President. The creation and organization of the Wiley University web site must reflect the College's mission and educational purpose. To ensure quality, the Committee on Information Technology will be responsible for conducting an annual review of the site, while the Office of Public Relations will conduct a periodic review. These reviews will encompass an assessment of the factual integrity of the site, currency and appropriateness of the information, technical feasibility, and the appropriate use of language, that is, grammatically and stylistically correct.

Examples of materials that are appropriate for the Wiley University web site include College publications, course schedules, job announcements, requirements of academic departments, the campus directory and upcoming events. If material is for an identifiably small, on-campus audience, an electronic medium other than the institutional web site must be used.

Certain individuals affiliated with Wiley University (faculty, staff, students and alumni), and who have network accounts, may have custom web pages. These web pages may be linked to the College's official web pages once the content has been approved through the institution's document approval process and permission granted. If a complaint arises about material in a custom web site attached to the College's web page, that object will be deleted and (uploading) privileges will be suspended pending further review.

21.0 Software Piracy

The academic community thrives on respect for the ideas and rights of others; privileges are balanced by responsibilities. This policy focuses on respect for intellectual property and especially computer software. As used in this policy, the term "software" includes commercial or other licensed program software and other works published in electronic form.

Unauthorized copying of software has tangible negative results for the academic community, for the developer of the software, and for the community at large. Wiley University and software developers both benefit from mutual trust and shared responsibilities. Unauthorized copying of software damages this trust.

Wiley University, the State of Texas, the United States, and international law prohibit the unauthorized copying of software. Members of the Wiley University community of users are prohibited from unauthorized copying of software. Users who ignore this policy and copy software without proper authorization will be disciplined.

Each member of the College community is responsible for making a good faith effort to assure adherence to this policy. Unit administrators are responsible for insuring that their units make a good faith effort to comply with this policy. If an authorized user is using software on a Wiley University

machine and is not sure it is properly authorized, consult with the appropriate vice president who will contact the Chief Technology Officer to make sure it is properly authorized.

It is not only illegal to copy software without proper authorization, but also unfair. Wiley University does not tolerate physical theft or plagiarism and will not tolerate unauthorized copying of software. Copyright law does not permit operating software on two or more computers simultaneously unless the license agreement specifically allows it. However, it may be legal to loan software temporarily as long as a copy is not kept.

Unless it has been placed in the public domain, copyright law protects software. The owner of a copyright holds exclusive rights to the reproduction and distribution of his or her work. Therefore, it is illegal to duplicate or distribute software or its documentation without the permission of the copyright owner. However, a back-up copy of any licensed software program may be made for use in case the original is destroyed or fails to work. A request for this service must be made to the Information Systems and Technology Division. Lack of copy protection does not constitute permission to copy software in order to share or sell it. "Non-copy-protected" software enables protection of the investment by making a back-up copy. In offering non-copy-protected software, the developer or publisher has demonstrated significant trust in the user's integrity.

22.0 Opt Out Mass Mailings

Employees not interested in receiving mass mailings should configure their individual mailbox to filter them out. The ISTD HelpDesk, extension 3310, can provide instructions. Because the mass mailing lists are built from individual departmental mailing lists, the College will not remove a person's name without also removing such individual from the departmental list. Faculty members, who wish to be removed from the department or mailing list, should submit a written request to the Vice President for Academic Affairs. Staff members who wish to remove their names from a list must submit a written request to their area vice president and to the Executive Vice President.

All users of campus e-mail should recognize that e-mail is an official means of communication for the College and that many notifications are sent through e-mail instead of through the campus paper mail system. Removal from the distribution list means that users may not receive important messages that are germane to their positions or contractual responsibilities.

23.0 Computer Ethics

No one may authorize another person to use his or her computer account for any reason. The account holder is responsible for all use of the account and must take all reasonable precautions, including password maintenance and file protection measures, to prevent the use of the account by unauthorized persons. Furthermore, ISTD advises that passwords be changed regularly.

Computer resources must be used only for authorized College-related purposes. As with all College equipment, the use of computer facilities, including the campus network, for private or commercial purposes is prohibited, except as expressly authorized. The College's information technology resources must not be used for any unlawful practices, such as the installation or distribution of fraudulent or illegally obtained software. Use of external networks connected to the College's network must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.

Users must not access, alter, copy, move or remove information, proprietary software or other files (including programs, members of subroutines libraries, data and electronic mail) without prior authorization from the appropriate College data trustee security officer, or other responsible party.

Users must not copy, distribute, display, or disclose third-party proprietary software without prior authorization from the licensor. Proprietary software must not be installed on a system not properly licensed for its use.

Users are encouraged to report any violation of these guidelines by another individual and any information relating to a flaw in or bypass of computing facility security to the College ISTD.

Users are expected to respect others who are contacted electronically. Electronic mail should adhere to the same standards of conduct as any other form of mail. It should be noted that in an academic community, the free and open exchange of ideas and viewpoints is preserved by the concept of academic freedom.

Users should ensure that they are known to those whom they contact. Others have a right to know who is contacting them.

Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the passwords of others or access files under a false identity.

The distribution of unsolicited mail is not authorized. Beware of the legal implications of computer usage.

The Internet enables users to disseminate materials worldwide. Remember that the larger audience means a greater likelihood that someone may object to material with or without legal basis. Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity apply to network-based communications.

Because the Internet is international, the laws of other countries may apply. This does not mean that members of the College community should allow extremely restrictive foreign laws to censor their communications, but in some situations, the College must take into consideration whether violations of foreign laws may affect the activities of the College in those countries.

Use computer resources lawfully and responsibly. The College reserves the right to take responsible steps after it learns of illegal or irresponsible uses of its computer facilities. With the exception of web pages, the College does not regularly monitor the content of electronic mail or other online

communications, unless directed by the President or his representative. Any activities or content that may be considered questionable will be reviewed and actions will be determined subsequently.

The College is responsible for providing all network related accounts. Individuals are expected to use their account in a responsible/professional manner, adhere to all policies and procedures, and to report any network related problems and/or concerns to ISTD.

Although a respect for privacy is fundamental to the College's policies, it should be remembered that all information can, in principle, be read or copied. At Wiley University, user information is maintained in system logs and archived as a part of regular computer system maintenance. At any time, the College may be compelled by law or policy to examine information, be it personal, professional, and/or confidential, which is maintained with College computing facilities.

Users are granted privileges and responsibilities with their account. While these vary among groups, the use of College resources for personal commercial gain or for partisan political purposes (not including the expression of personal political views, debate and the like) is inappropriate and illegal.

Individual College computer systems have varying resources and demands. Some have additional guidelines, which may be more restrictive than those contained here, applicable to their own users.

24.0 Computer Laboratories

It is prohibited to use Wiley University computers for any illegal, immoral, or offensive purpose, including those in computer laboratories. This includes accessing Internet materials of a lewd or offensive nature, printing any such materials, or displaying them on the computer screens. It is prohibited to use computers for games or other non-class or non-work related activities.

24.1 Logon/Logoff

When finished with the computer, select "Close all programs and log off." DO NOT turn off the power.

24.2 Behavior

Students are expected to be quiet and orderly when utilizing the computer lab, to treat the computer equipment with care, and to keep the lab clean and neat. EATING, DRINKING, and/or SMOKING are NOT ALLOWED in any Wiley University computer laboratory facility.

24.3 Violations

Faculty, staff and students are expected to adhere at all times to the rules and guidelines established by this document, state and federal law, and all related documents adopted by other academic departments. Individuals who violate these policies and guidelines are subject to disciplinary action as indicated below. The disposition of situations involving a violation of the policies set forth in this

document and the penalties that may be imposed upon the person guilty of the violation(s) are described in this section. Accidental infractions of this policy such as poorly chosen passwords, overloading systems, excessive disk space consumption, poor judgment, and so on, are typically handled internally and in an informal manner by electronic mail or in-person discussions. More serious infractions, such as unauthorized use, denial of service, attempts to steal passwords or data, attempts to steal licensed software, violations of Wiley University policies, harassment, or repeated minor infractions, may result in the temporary or permanent loss of academic computer system privileges without advance notice or warning. Offenses that are in violation of state or federal laws can result in immediate loss, without advance notice or warning, of all academic computing privileges.

25.0 Bringing of Charges

Any member of the student body, staff, or faculty may bring charges for violations of these rules. Charges should be directed to the faculty or staff member responsible for the academic computing system involved with the infraction. The official will determine if further action is required. He or she may require that the charges be made in writing. Normally, charges will be brought within ten days of the alleged violation, but in special cases, the time limitation may be extended. Conduct which violates this policy includes, but is not limited to:

- Engaging in any activity that might purposefully be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to College data.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Making or using illegal copies of copyrighted software, storing such copies on College systems, or transmitting them over College networks.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with either legitimate (file backup or archive) or malicious (denial of service attack) activities.
- Using the College's systems or networks for personal gain; for example, by selling access to your user account or College systems/networks, or by performing work for profit with College resources in a manner not authorized by the College.

It is a violation of College regulations to: (1) intentionally and without authorization, access, alter, interfere with the operation of, damage or destroy all or part of any computer, computer system, computer network, computer software, (2) intentionally or knowingly and without authorization, give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or database.

26.0 Client Privileges and Responsibilities

Prior to receiving the privileges associated with a network account, users must sign a statement that they also accept the responsibilities that accompany these privileges. Those using the College computer facilities are responsible at all times for using these facilities in a manner that is consistent with this policy and its intent. Users are responsible for obeying all official notices posted in local policy newsgroups by appropriate staff members, or announced using electronic mail. They are also responsible for knowing and abiding by the policy set forth in this document, along with any changes announced by any of the means noted in this paragraph.

Users are also responsible for any and all activity initiated by their account. For this reason, as well as to protect their own data, users should select a secure password for their account and keep that password secret at all times. Users are responsible for protecting their own files and data from reading and/or writing by others, with whatever protection mechanics are provided by the operating system in use. They are also responsible for picking up their printer output in a timely fashion to avoid theft or disposal.

27.0 Research

Anyone conducting research on computer security or investigating self-replicating code must have that activity initially, and then periodically, reviewed to address the risks the work may place upon the rest of the College community. The CTO must be notified of the activities of such work well in advance of their occurrence in order to evaluate the risks involved. When possible, special arrangements will be made to provide an adequate environment for these efforts without risking damage to, or impairment of, others' work. Codes that fall into the above categories would include, but are not limited to, virus code, worm code, password cracking code, and password grabbing code. The state of system security at any given time is not to be interpreted as an opportunity for abuse either by attempting to harm the system, or by stealing copyrighted or licensed software. Deliberate alteration of system files can be considered vandalism or malicious destruction of Wiley University property. For additional information, see the Wiley University Security Policy Manual.

The ability to connect to other systems via the network does not imply the privilege to make use of or connect to other systems unless properly authorized by the owner(s) of the system(s) in question. College facilities and network connections may not be used for the purposes of making unauthorized connections to any systems, on campus or off.

28.0 Audio/Video (Multimedia)

ISTD responsibilities have been recently expanded (2012) to include defined multimedia (audio/video) technology management in various locations across the campus. This management encompasses the technical planning and operational aspects of multimedia based equipment such as sound reinforcement systems and video projection systems from an infrastructure support perspective.

In order to effectively manage this essential technology and associated equipment, stringent policies and procedures must be defined. These policies and procedures are designed to help ensure the proper operation, maintenance, and deployment planning for College audio/video assets.

ISTD Managed Multimedia Locations include:

1. Julius S. Scott, Sr. Chapel
2. Freeman P. and Carrie E. Hodge Building
3. Pemberton Auditorium
4. Locations where portable multimedia equipment is viable and has been approved for use

Policy

ISTD will provide management and planning resources to establish purchase, deployment and operational guidelines for multimedia audio and video applications campus-wide. The objective is to work with College departments to define and refine their requirements for audio/video applications to help ensure various levels of standardization and management.

Procedures

5. Arrangements must be made at least 48 hours ahead of the intended use by contacting the Helpdesk (support@wileyc.edu or (903) 927-3310) and completing a requested services form. All fields on the form must be completed. When the request has been approved, a staging and/or rehearsal may be required to ensure proper support for the event.
6. Questions regarding ISTD managed multimedia services should be requested through the Helpdesk or (903) 927-3310.
7. Only properly trained and certified audio/video technicians will be authorized to operate this equipment. The ISTD will systematically provide multimedia operations training and certification to applicable students, faculty and staff that have been designated to operate the equipment. The ISTD will serve to manage trained and certified technicians to provide service for College events and develop a roster listing these personnel. Every effort will be made to provide qualified technical multimedia services to support College events. However, there may be cases where outsourcing or other means are required to meet specific needs and schedules.
8. Control rooms/booths and other designated areas that house multimedia control equipment will remain locked and only available to authorized personnel.
9. The ISTD will systematically provide multimedia operations training and certification to applicable students, faculty and staff who have been designated to operate the equipment.

Special Notes:

10. The ISTD is not responsible for developing or operating/navigating multimedia content such as slide presentations, webinars, websites, music, etc.
11. The ISTD managed multimedia equipment is not guaranteed to be compatible with all multimedia content and media. Equipment will be selected that meets the majority of industry and academic standards for multimedia operations.
12. This policy is primarily focused on non-classroom multimedia technology such as that used in campus large-event spaces (Julius S. Scott, Sr. Chapel, Freeman P. and Carrie E. Hodge Building

Auditorium, Pemberton Auditorium, etc.) and approved locations requiring portable multimedia equipment.

13. The ISTD is not responsible for supporting general student musical or video entertainment events.
14. The ISTD continues to provide planning and technical support services for multimedia classrooms.

29.0 Conclusion

This manual is provided for the purpose of addressing some of the most frequently asked questions regarding the proper use of information technology (IT) at Wiley University. IT is a vital resource for the fulfillment of academic and administrative purposes. Therefore, it is essential that all faculty, staff and students exercise responsible and ethical behavior when utilizing this resource.

Technology is constantly changing and therefore this manual will need to be revised and updated periodically. Comments and corrections are welcomed and should be sent in writing to the Chief Technology Officer or by e-mail to support@wileyc.edu.