
Anderson University
Information Technology Policy Statement
March 2007

Table of Contents

1. Statement of Purpose
 2. Privacy Statement
 3. Copyright Statement
 4. Acceptable Use of Computer Resources
 5. Unauthorized or Inappropriate Uses
 6. Computer Support Policy for Faculty, Staff and Students
 7. User Accounts
 8. Administrative Systems
 9. Network and Internet Use
 10. ResNet
 11. Network Extension Devices
 12. Email
 13. Web sites
 14. Allocation of Computer Resources
 15. Lab Use
 16. Technology Classroom Use
 17. Handheld or Portable Computing Devices
 18. Lines of authority/accountability/enforcement
 19. Information Security
 - a. Information security plan
 - b. Remote access/ work from home (pending)
 - c. Laptops Use and Security
 - d. Security Incident Response
 20. Password policy
 21. Glossary and definitions
- Appendices

1. *Statement of Purpose*

Anderson University's computer resources and information network are vital for the fulfillment of the academic, research and business needs of our community. Their use is provided as a privilege. In order to ensure a reasonable and dependable level of service, it is essential that each individual student, faculty and staff member exercise responsible, ethical behavior when using these resources. Misuse, even by a few individuals, has the potential to disrupt the legitimate academic work of students and faculty, as well as the business processes of the institution.

The policies that follow outline the principles that govern our academic community in the appropriate use of computer resources and its information network. Unless otherwise stated, these policies apply to all members of the University community and to all University owned or managed computers and network equipment, as well as all information contained therein. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means. These policies do not override any existing Anderson University policies as outlined in the Student, Faculty or Staff Handbook and are intended to be congruent with all applicable local, state and federal laws.

2. *Privacy Statement*

Anderson University will take reasonable precautions to maintain privacy and security within our electronic systems. The University cannot guarantee that these efforts will always be successful and, therefore, users must assume the possibility of a breach of University privacy and security systems. The University does not intend

to sell, swap, rent, or otherwise disclose for purposes outside the scope of ordinary University functions user's name, mailing address, telephone number, e-mail address, or other information. While the University makes reasonable efforts to protect information provided to us, we cannot guarantee that this information will remain secure and are not responsible for any loss or theft.

No administrator or user will view, use, or otherwise access personal user data unless there is:

- a.) the consent of the owner of that information; or
- b.) an adequate support or service reason as to aid the user without completely compromising their privacy; or
- c.) sufficient cause based on a violation of this acceptable use policy or violation of federal or state law; or
- d.) as necessary to responsibly manage University technology resources.

Notification of this privacy policy and the accompanying cautionary notes will be repeated annually as a reminder to all members of the community.

All technology and information resources will be managed within FERPA guidelines.

3. *Copyright Statement*

As an institution dedicated to pursuits of the mind, Anderson University recognizes and respects intellectual property rights. Our commitment is to provide an environment that supports the teaching and learning activities of our faculty, staff and students. To that end, all members of the community are expected to comply with applicable laws regarding copyright and intellectual property and to exercise in good faith the principles of "fair use" in education. The respect of copyright includes all media: print, audio, video and digital. The University does not condone nor support the illegal use or reproduction of copyrighted materials in any form.

Additionally, Anderson University intends to fully comply with all software licenses and their provisions and will take reasonable and prudent steps to assure these intellectual property rights are respected.

Recognizing the complexity and ever-changing environment within which copyrighted works exist, the University will strive to educate all members of our community on the laws as well as the practices of copyright and fair use.

4. *Acceptable Use of Computer Resources*

Acceptable and responsible use of the University computer and network resources requires that all users follow these guidelines:

- Respect the copyright and license provisions as they apply to all programs and data made available on the campus computers and the Internet.
- Respect the copyright of all materials with respect to their incorporation into software, presentations, multimedia applications and Internet servers.
- Respect the rights of others by not tampering with their accounts, passwords, programs or data.
- Use only those computer IDs and passwords for which you are authorized, and use them only for the purposes for which they are intended. Do not share computer accounts or passwords with others.
- Avoid misuse or overuse of the network or printing resources or other shared computing resources.
- Avoid the misuse of University computing and network resources for private, commercial or political purposes unless such arrangements have been made with the appropriate University official.

Anderson University prohibits unauthorized or misuse of University email addresses for any purpose, including unauthorized or misuse of campus electronic mail lists.

All users should respect and preserve the privacy of personal and institutional data to which they may have access by:

- Choosing an obscure or hard password that contains both letters and numbers and changing it frequently.
- Providing for the security of computer systems and networks for which you are responsible. This includes, but is not limited to, providing for prevention of unauthorized access or destruction of programs and data, and providing for adequate backups.
- Logging out or securing your workstation when stepping away from computer to ensure personal account security and protect the security of our University systems.

5. *Unauthorized or Inappropriate Uses*

Unauthorized use of technology resources is prohibited and, in many cases, may be violations of the law. We are guided by the law in noting that unauthorized use includes, **BUT IS NOT LIMITED TO**, the following types of activities:

- a.) harassment or threats to individuals or classes of individuals
- b.) interference or impairment to the academic activities of others
- c.) unauthorized access or unauthorized use of the resources of others
- d.) damage or impairment of University technology resources
- e.) unauthorized commercial or political activities
- f.) violation of city, state or federal laws
- g.) anything deemed inappropriate by other campus policies or regulations

It is the user's responsibility to promptly report any suspected unauthorized or inappropriate use, or misuse of Anderson University technology resources to their supervisor or to the Director of Information Technology Services. Anderson University has the right to investigate such uses, including the inspection of data stored or transmitted on the network or stored on any University-owned desktop computer. If a use is determined to be in violation of this or any other University policy, appropriate measures will be taken which may include, but are not limited to verbal or written warning, permanent or temporary suspension of user privileges, deletion of files, disconnection from the AU network, referral to the appropriate disciplinary process, and cooperation with appropriate law enforcement officials or agencies.

6. *Computer Support Policy*

Faculty and Staff

Computers purchased by Anderson University have a standard hardware and software configuration which has been chosen for functionality and "supportability" within our institution. Computers owned by the institution will be supported, within those standards, to the full extent of our abilities. If we are unable to repair a computer, a substitute will be found. All users are encouraged to practice responsible computing practices such as regular backup of files from the local hard drive to the user's network drive, assuring virus and Windows updates/patches occur, enabling the archive function for email and calendars, and promptly reporting computer problems to the ITS HelpDesk (x4300).

Personal faculty and staff computers will not be supported by ITS. We encourage all users to install and regularly update virus protection software, download and regularly run spyware and ad removal programs and updates of Windows (if applicable).

If personal computers are attached to the University network, they will be required to comply with Anderson University's Computer Security policy, including updated Windows patches and updated antivirus software.

Students

The support we provide to students is for the purpose of maintaining a safe and fully functional network. For this reason, IT support for student-owned computers is limited to network connectivity. Through enforcement appliances, we will insure all computers have virus software installed and updated, and that Windows patches are up-to-date before allowing a connection to the network. We also recommend anti-spyware software be installed since malware routinely interferes with computer performance. Students must provide their original, licensed copy of Windows and other essential software if those are needed to resolve identified problems.

Assistance beyond virus protection and Windows patches is outside the scope of ITS support for students.

Neither Anderson University nor ITS shall be liable to any user or other person for loss or damage of any kind related to the operation or reconfiguration of that user's computer equipment including, but not limited to: out-of-pocket expenses; consequential damages, inconvenience; loss of data, profits, or use; emotional stress; physical injury; or damage to software or hardware. ITS will endeavor to perform requested assistance in a timely manner, but will not be liable for failure to do so. ITS makes no warranty, expressed or implied, that computers will be able to be configured or repaired.

For a statement of User Support Procedures, see Appendix C.

7. *User Accounts Policy*

All users of Anderson University computing and network resources are bound to abide by *Statement of Responsibilities for Computer Network Users*

<http://it.anderson.edu/Students/NewStudents/StatementofResponsibility/tabid/82/Default.aspx>.

There are no exceptions to this policy.

Electronic mail user accounts are extended to Staff, active or emeritus Faculty and active students. An account request form <http://it.anderson.edu/FacultyStaff/Forms/tabid/71/Default.aspx> must be completed before accounts are created.

User file server accounts are extended to active students, Faculty and Staff members.

Guest accounts are extended only to selected external users with department sponsors. A written request for guest accounts should be submitted at least 2 weeks prior to guests' arrival to campus to the Director of Information Technology Services.

Student accounts will be deleted upon leaving the University as a withdrawal, transfer or graduate. Graduates may keep their accounts for a few months after graduation to facilitate their job search process. A schedule for account deletion will be announced via email. Responsibility for the backup/transfer of all personal files on AU systems will lie with the graduate, transfer student or other. AU is not responsible for lost personal files after accounts are deleted.

Students on temporary leave may maintain their file space and account for approximately one (1) year. Absences longer than 1 year will be considered on a case-by-case basis. In all other cases, the Registrar will be consulted about the status of the student and, based on information received the decision to delete or maintain the account will be made.

Faculty accounts will be deleted after that faculty member completes their employment with the University. Faculty members leaving are responsible for the transfer of their files from AU systems before their final official date of employment. AU is not responsible for lost personal files after accounts are deleted.

Staff accounts are deleted after that staff member completes her/his employment with the University. Important work-related files should be retained and transferred to the appropriate staff within that department for departmental reference and archives. All email and personal files should be removed from University systems by the last day of employment. AU is not responsible for lost personal files after accounts are deleted. The

University reserves the right to forward all email from the account of a departing staff member to another staff member within the department in order to maintain continuity of service for that department.

In the case of a termination of a staff member, the University will immediately disable the account and move stored files on both networked and local computer storage devices to the staff member's supervisor.

Name changes

Students wishing to change their user name should initiate the process through the Registrar's Office. The Registrar's Office will notify ITS and changes will be implemented in a timely fashion. Account names may be changed only for legal reasons (marriage, legal name change) or if the username that results from the standard process is offensive.

Faculty or staff needing to change their user name should contact the User Support Manager to begin the process.

8. *Administrative Systems*

Administrative Systems represents the information processing of the major administrative offices: Admissions, Student Financial Services, Registrar, Student Life, Alumni/Development, Human Resources, and the Business Office.

Administrative Systems also includes interfaces with various internal and external systems, such as Library, Dining, State of Indiana Aid, Student Loans and Pell Grants, Tuition Payments, web services and many more. Additionally, there are special purpose applications like Room Scheduling, PPD work orders, ID cards, Chapel attendance tracking, web services, etc. Administrative Systems policies and procedures apply to all of the above.

Anderson University uses a partnership approach to system management. Each individual functional area of the University is responsible for researching and developing their functional needs, policies and goals. They also perform routine data processing and reporting. The Director and Technical Liaison work with the Programmer/Analyst (P/A) to implement robust systems supporting their goals. Information Technology Service P/A provides technical, procedural, evaluation, design and support throughout the process. The underlying principle is co-operation and participation so that maximum benefit is achieved.

[Further information will be available in Appendix A when revision of this document is complete.]

9. *Network and Internet Use*

Any computing device that attached to the Anderson University computer network must comply with the University's security policies, including current Windows patches and updated antivirus software.

Since most University computer systems are connected to the Internet, it is essential for each user to recognize his/her responsibility in using these services and systems. The "Internet" is not a single network; rather, it is a group of thousands of individual networks that have chosen to allow traffic to pass among them. The traffic sent out to the Internet may actually traverse several different networks before it reaches its destination. Therefore, users involved in use of the Internet must be sensitive to loads placed on other systems and participating networks.

Each network or system has its own set of policies and procedures. Actions that are routinely allowed on one network or system may be controlled, or even forbidden, on other networks. It is the user's responsibility to abide by the policies and procedures of these other networks/systems.

Free access to the network is a privilege that may be revoked at any time, with or without warning, for abusive conduct. Such abusive conduct includes, but is not limited to:

- Using the network for any purposes that violate federal or state laws;
- Using the network to make unauthorized entry to Anderson University's or other computational information communication resources;
- Use of another person's account on the computer systems;
- Tampering or moving with network cabling or routing devices;
- Use of software or hardware designed to disrupt the security of the network or devices on the network, or to spy on the network traffic of other users;
- Knowingly and intentionally engaging in any activity that spreads computer viruses and/or SPAM mailings to campus computers or other computers on the Internet. This includes users who do not take adequate precautions against or seek IT support in taking adequate precautions against viruses and the proliferation of viruses;
- Impersonating another user in the use of the computers, networks or in email or other messages;
- Use of abusive or otherwise objectionable language in either public or private messages;
- Sending of messages that are likely to result in the loss of recipients' work;
- Sending of "chain letters", novelty messages or lengthy unsolicited messages to individual accounts and/or lists of addresses;
- Distribution of unsolicited advertising; and any other types of use that would cause congestion of the networks or otherwise interfere with the work of others;
- Unauthorized use or abuse of University mail lists and listservs;
- Removal of any equipment from its designated location (clusters, labs, classrooms, offices, etc.).

For further information and procedures, see [Appendix B](#) *Network Systems Procedures and Responsibilities*.

10. ResNet

The Residence Hall network is (ResNet) provided to support the academic mission of Anderson University and is not made available for unrestricted use for other purposes. The network connection supplied by ResNet is solely for the use of the individual subscriber assigned to that connection. Users cannot use any mechanisms (either hardware or software) to provide network connectivity to anyone outside the University.

The use of switches, wireless access points, and similar devices require configuration by Information Technology Services to prevent them from interfering with University-owned access points. Use is limited to personal use by the individual student. Contact ext. 4300 to make arrangements for assistance in configuration. Improperly configured access points will be blocked, disabled or confiscated.

Network users may not manually assign an IP address to their computers. Doing so may disrupt connectivity for other users. Network services and wiring may not be modified or extended beyond their intended use. This policy applies to all University network infrastructure and services.

Computer names, computer descriptions, computer desktops, messages broadcast, and other content should not be defamatory, lewd, or obscene.

Network users are responsible for any network activity linked to their data ports. For this reason, passwords should be secure and not shared with anyone (including family members, roommates, and friends). Users who believe that another person is using their account should notify Anderson University IT Services immediately and change their password.

Users are prohibited from attempting to circumvent the authentication systems. In addition, users should not attempt to hide their identity or impersonate another's identity on the University network.

Anderson University has implemented basic security and privacy measures as part of routine operations to help protect from service degradation and the effects of illegal activity, such as computer attacks. Each individual also take reasonable security and privacy precautions to protect against computer viruses and other computer attacks which may result in loss of data, unintentional release of personal information, or negative impact on Anderson University's network performance.

In order to access ResNet, users must pass through a policy-enforcement gateway which requires up-to-date Windows patches and the University antivirus program installed. Antivirus software is made available at no charge to students in residence halls. Failure to comply with these requirements will prevent the user from accessing the University network.

Federal law prohibits the transmission (sharing) of copyrighted materials without express written permission from the copyright holder. Copyrighted works (including original writings, software, movies and music) may not be shared on the local network.

Anderson University has the right to restrict access to any service detrimental to the Anderson University's information resources. Attempts to bypass these restrictions (such as the use of tunneling protocols) will be considered a violation of this policy. Due to potential competing enterprise services, Anderson University does not allow network users to run SMTP, DHCP or Kerberos services on ResNet

Audio, video and game servers are permitted, but due to bandwidth concerns, may be disconnected without notice. In addition, all use must comply with existing copyright laws.

The use of defective or malfunctioning equipment on the network will result in the offending ports or logins being disabled without prior notification.

Hardware and/or software designed to detect and exploit network vulnerabilities is forbidden on Anderson University networks.

Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited regardless of intent.

Violation of these policies will result in loss of service for a period of time based on the severity of the violation and the recommendations of ITS personnel. Violators may also be referred to the Dean of Students for further action.

11. Network Extension Devices (including Wireless Access Points)

Any and all network technologies are subject to University policies and Anderson University's *Statement of Responsibilities for Computer Network Users*.

It is the responsibility of the Anderson University's Information Technology Services to provide reasonable security, enforce appropriate use, and allocate access to network resources and bandwidth in an equitable manner to our community. The following guidelines are provided to help users understand specifics issues to consider when network extension devices are under consideration.

Only those network extension devices (including devices such as hubs, switches, routers, and wireless access points) installed and managed by Anderson University will be allowed for use on the Anderson University network (with the exception of some residence halls [see below]). University faculty and staff are not permitted to install their own network extension equipment. Departments wishing to extend their network connectivity or implement wireless networking should contact the Information Technology Services.

Anderson University reserves the right to request the removal of any network extension devices at any time for any reason.

Residence Halls

One network port per student is provided in residence hall rooms. This is sufficient for connecting to the network one computer or network device at a time.

Some students on Anderson University's ResNet may wish to extend the network in their room and have more than one computer in their residence hall room, or may want to have other network devices, such as printers or game consoles, in addition to their primary computer. If more than one network port is desired, managed switches or (in some residence halls) wireless access points are permitted, but on a 'use at your own risk' basis. In the case of Wireless Access Points, the user must bring these to Information Technology Services for configuration to assure they will not interfere with normal network functions and to implement security on the access point. Network security devices may prevent the proper functioning of some equipment and service to those devices may be disrupted. Routers are not permitted on the residence hall network.

Anderson University reserves the right to request the removal of any network extension devices at any time for any reason.

12. *Email*

The following statements apply to our standard campus email system, Groupwise. All members of our campus community are expected to have and regularly check their Groupwise accounts. Groupwise is an official channel of communication between administration, faculty and students.

While widely used as a primary method of communication between members of our campus community, all users should keep in mind that electronic mail is not a secure means of communication. No system connected to the Internet is completely safe from attack or infiltration. Anderson University encourages all members of the community to be cautious in email communications and not send information over email that is highly private, sensitive, or potentially offensive to some members of the community.

Anderson University owns the email system and its contents. Email is not private communication.

The University does not intend to monitor the contents of e-mail sent to or from University servers, except to identify and correct problems with e-mail delivery or receipt, to work with email system problems, or to deal with misconduct or security issues. An electronic log of who sends and receives e-mail through University servers is maintained for a short period of time and used to analyze trends, create summary statistics for internal planning purposes, and to otherwise aid in maintaining system performance and security. E-mail-related information is stored on a temporary basis and will be released only if legally mandated by law enforcement investigators, required by court proceedings, or it is deemed necessary to internal investigations of violations of University rules and regulations. There are no backups of email servers. Lost or deleted email cannot be recovered.

Users should regularly monitor their email storage volume and cull those messages, keeping only those of lasting value or importance.

13. *Web site policy*

Anderson University has provided all faculty/staff and students a place to store and make available a website. All members of the Anderson University community are expected NOT to display material or information deemed offensive. Offensive material is described as any substance or activity prohibited by the Faculty/Staff and the Student Handbook. Any persons who are found to be in breach will have their website removed. Websites stored on the Anderson University servers are not allowed to be of a business or commercial nature or contain any illegal material posted on the site.

Any person wishing to include a link to a website not hosted by Anderson University should obtain prior permission to link to the outside website before including this link on their webpage hosted by Anderson University. If the owner of the linked page at any time objects to linking, the webpage will be taken down. ITS recommends a Site page on every web page giving credit to the author, or creator of text and pictures and the permission granted for each link on the website.

No website may infringe upon another person's rights or violate Anderson University community standards. A website found to be in violation will be taken down without notice.

14. *Allocation of Technology Resources*

Institutional resources will be directed into technology that improves learning, expands and enhances the academic process, and increases the effectiveness and efficiency of the management of this institution. Priority will also be placed on improving student access to technology resources, including web-based learning resources, academic records and access to the library and Internet.

Anderson University provides the following resources and services to members of our community (students, staff and faculty):

- a) A campus network with access to the Internet and network connections in residence halls, classrooms, offices, and other learning spaces.
- b) Desktop computers for full-time faculty and most staff. Access will be made available, although perhaps not by an individual desktop computer, for part-time/adjunct faculty and staff.
- c) Access to printing resources via a network connection.
- d) Network and email accounts; email is a primary means of communication between members of our community.
- e) Public computer labs for general use and specialized labs for specific academic uses
- f) Multiple classrooms with permanent LCD projectors and desktop computers plus various audiovisual devices and network connections.
- g) Web-accessible library information system.
- h) Integrated and web-accessible administrative computer system
- i) User support and training through ITS staff assisted by student workers.
- j) Protection from computer viruses, worms and email spamming.

Desktop Computers

Desktop computers are primarily configured with the Windows platform. Macintosh purchases will be approved only where there is a demonstrated professional need. Macintosh OS is not compatible with our administrative computing system.

Desktop computers will be configured in line with current technology standards.

Faculty on sabbatical should make individual arrangements for access to computer desktop resources during their sabbatical leave.

Laptop computers

Laptops are an option for persons whose jobs require regular off-campus work or whose jobs require mobility within the campus environment (i.e. ITS staff doing network support). Laptop purchases beyond these categories will be decided on a case-by-case basis. Requests should be made through the normal budget process. As a general practice, users are not permitted to have two University-owned computers assigned to them personally. Exceptions will be rare and made on a case-by-case basis.

Laptop Purchase Priority:

- Only full-time, permanent members of the University community are eligible for consideration for laptops. Efforts will be made to allocate laptops to users based upon job responsibilities and need.
- Management team members will identify any key staff that is to be considered for a laptop.

In general, users must choose either a laptop or a desktop. Laptops may be connected to a monitor, keyboard, and other peripherals (docking station or port replicators are to be provided by the department

or office of the laptop caretaker). Faculty or staff who are assigned laptops are required to keep them on campus while at work. Because of the need for specialized equipment or software, laptops may not be adequate or cost effective for some users. In these instances, users will continue to be assigned desktops.

Printers

Networked printers are provided in many department locations and are intended for use by workgroups of 2 to 20 users. The features made available on the printers (i.e. duplexing, multiple paper trays) will be determined at the time of purchase and are dependent **on** cost versus demonstrated need.

ITS will supervise a maintenance contract for repair of printers, but this contract does not include regular preventative maintenance. When network printers reach the end of their lifespan, they will be removed from the University maintenance contract and users will be directed to other printing resources.

Departmental printers are intended to print one to five copies of any computer-generated document.

Printers are not intended to serve as copiers. Such a use of networked printers is considered an abuse of resources and may negate the contracted repair agreement.

Multifunction digital copier/printers are available in many locations on campus. These devices are intended to serve as primary printers in some locations. Some have the ability to print and copy in color.

Departmentally-based accounts are established and maintained through Information Technology Services. These devices are appropriate for 5 to **100** copies of digitally prepared documents. Connection to these devices should be arranged through ITS.

Printing more than **100** or more copies should be directed to the high-speed printer in Printing Services. Connection to this device can be arranged through ITS.

Determining the appropriate device to direct print jobs to is the responsibility of each individual user.

Reports exist that enable a department to review monthly print volumes by device. The institution makes multiple types of devices available and recommends printing levels based **on** cost per copy. Users are requested to think institutionally and assist in keeping printing/copying costs under control by selecting the most cost-effective device for each print job.

Individual ink-jet printers (color or black-and-white) are not supported **by ITS**. Individuals who purchase them are responsible for their installation, maintenance and supplies. If these printers interfere with networked printer installation, they will be uninstalled.

Storage and backup

Network storage for files will be made available within reasonable limits. These limits are flexible and may be increased upon request. Excessive use of storage will be monitored and addressed on an individual basis. Data stored on network drives will be backed up on a daily basis and backups retained for 45 days.

Software

Campus software falls into three general categories, each with its own level of support and funding:

Universal software: those programs typically installed on every institutional computer. Support for this category of software includes installation, orientation for new users, and assistance in resolution of problems. This software is purchased and maintained with institutional funds.

Special software: those programs used for a specialized, usually academic, purposes and made widely available for use in computer labs. Support is limited to installation and basic functionality. Faculty requesting the installation of this software in labs should be prepared to instruct students on its use. Decisions on the funding of this software (departmental, institutional or shared) will be made prior to the time of purchase. Consideration must also be given to on-going (maintenance) costs.

Departmental/individual software: programs that are used specifically in one department or by an individual to perform a specific function or process that is unavailable within the standard software configuration. Such software may be installed on one computer only, or may be hosted on network applications servers. Support is limited to installation only. Users should be prepared to support themselves in the functionality of the software. Purchase of this software will be from departmental funds; oversight of software licenses or maintenance fees may be managed by ITS when departmental funds are allocated and transferred to ITS for that purpose. Otherwise, the department or individual will be responsible for proper maintenance of licenses.

Before the purchase of non-standard software, ITS staff will assess the capabilities of the computers upon which the software will be installed, the compatibility of the software with our core network, or other technical requirements imposed by the software. Consideration must also be given to on-going (maintenance) costs.

Installation of personally-owned software on office computers **MUST** be congruent with copyright laws and/or licensing agreements implied by installation. Individuals are responsible for installation and must keep evidence of the software's legality in their office in case of a software audit. If the software interferes with the intended functioning of that individual's computer, ITS will return the computer to its original configuration and advise against reinstallation of the software. Repeated infractions will be reported to the Vice-President of Enrollment Management and Information Services for executive action.

Replacement Cycle

With rapid technological advances, regular replacement of computer resources is critical. Our goal is to replace all desktop computers for those in full-time positions every three to four years. In many cases, the newest machines will be placed in high-use locations such as student computer labs, or on the desks of those campus users requiring higher functionality, with a cascading of older equipment to less demanding situations. Each department should review annually (during the budgeting process) their replacement or upgrade needs. Technology requests should come through the regular budgeting process (see below).

Special Needs

University employees requiring special accommodations due to physical limitations or health concerns should make those needs known to their supervisor. Accommodations will be made as necessary to allow the user to adequately perform tasks that are part of their written job description. Funding of these accommodations will be shared by the affected department and institutional computer funding.

Technology Request Process

Technology enhancements are funded through the normal budget process. At the time budget forms are submitted, department heads should submit a survey of their current computer needs and make requests for additions, enhancements and improvements – both hardware and software – for the coming year. ITS may also recommend changes in desktop computers based on the maintenance record of individual pieces of equipment or other known problems.

Computer technology items purchased by the University must be requested, approved and purchased through a centralized process no matter what the source of funds. This ensures compatibility, cost efficiency, and awareness of inventory on campus. Cost, consistency, functionality, life-span, supportability and overall quality are some of the factors balanced in the purchase of technology resources.

Individuals who bring personal computer equipment to campus for their own use should consult with ITS prior to bringing it to campus to assure that it will work within our standard environment. We will provide assistance to the best of our ability and available time; however we cannot guarantee that all equipment can be made to function within our environment. Before any personal computer equipment is allowed to be used on campus, it **MUST** have antivirus software installed and regular Windows updating.

Departments that purchase computer equipment or software outside the process defined in these policies will receive no support for that equipment.

15. Lab Use

Anderson University student computer labs are equipped with computers and software primarily to support the academic work of our students.

Classes being held in a lab have first priority of use; students doing academic work have second priority; students using lab computers for optional or recreational reasons have the lowest priority. Students using a computer for recreational use (games, correspondence, social E-mail, etc...) are expected to relinquish their computer promptly in response to a request from a lab assistant or another student. Recreational computer use is not allowed at times when students with academic work are waiting.

Students must produce their Anderson University ID card when asked to do so by lab assistants or ITS staff. Failure to do so may result in immediate expulsion from the labs.

Loud, disruptive, intimidating or vulgar behavior will not be tolerated in the student computer labs. Threatening, intimidating or vulgar behavior toward lab assistants or other students or failure to leave the labs when requested by lab assistants or staff will result in the revocation of the privilege to use student computer labs.

16. Technology Classroom Use

Technology-equipped classrooms are a resource made available by the University to faculty who wish to use these resources as a part of their teaching and learning environment. Faculty wishing to hold a regularly scheduled class in a Technology Classroom should make that need known to their Department Chair and/or school Dean and then file a request through the Assistant Registrar on a semester basis. Technology Classrooms are supported and maintained cooperatively by the Instructional Materials Center and Information Technology Services. Problems with Tech Classroom equipment should be reported to the IMC at 4293.

17. Handheld and Portable Computing Devices(PDAs)

Handheld devices are those devices used for portability of information, usually including calendars, contact information, task lists and electronic mail. Check with ITS to determine which devices are currently supported before making a purchase.

Any PDA to be installed for synchronization on an Anderson University computer must be installed by ITS. This is done to ensure the greatest reliability of the PDA and to avoid interference with other installed software or network services.

PDAs are considered to be personally owned and therefore no maintenance will be performed on the device itself.

Handheld devices have the potential to present a significant risk to the University's data security, depending on what information is stored on them and what resources they are configured to synchronize. Handheld device users should take reasonable and prudent steps to password protect information stored on their device in the event of loss or breach of control.

If University information security is compromised by a lost or stolen device, the user of that device may be personally liable for any outcomes that result from that breach of security.

18. Lines of authority/accountability/enforcement

Any breach or violation in the policies contained in this document should first be reported to the appropriate supervisor or to the Director of Information Technology Services where applicable. The supervisor or the

Director of Information Technology Services will investigate and take appropriate action; or refer the situation to the Vice-President of Enrollment Management and Information Systems or the Director of Human Resources, as appropriate.

19. Information Security

- a) Anderson University's Information Security Plan describes Anderson University's safeguards to protect *covered data and information*. These safeguards are provided to ensure the security and confidentiality of covered data and information; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

See [Appendix D Information Security Plan](#) for further details.

- b) Work-from-home/Remote Access (security of)
Users who need access to University data to work at home must use a VPN (Virtual Private Network) connection for security purposes. Users should request to be included in the VPN group and necessary software will be installed on their machines.

- c) Laptop Security Policy
Laptop computers provide important functionality, allowing University faculty and staff to have computing resources available in meetings or classes, during travel on University business, and for those who occasionally work from home. With this convenience comes additional responsibility. Laptops present an increased level of risk to both the user and to the institution. In requesting and accepting a laptop from the University, users are acknowledging their acceptance of this risk and agree to make every attempt to follow the steps outlined below to reduce it.

This policy applies to all faculty and staff who use a University-owned laptop. These individuals are hereinafter referred to as "caretakers." Each caretaker of a University-owned laptop is responsible for the security of that laptop and the data contained therein, regardless of whether the laptop is used in an office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport.

All laptops should be protected with multiple "hard" passwords. Confidential or "covered" information (see Appendix D) stored in files on the laptop should be individually passworded with secure "hard" passwords that are different from the laptop access passwords. Users who do not follow these guidelines are putting the institution at risk and may also be personally liable for any disclosure of covered information.

When you receive a laptop, you accept responsibility for safeguarding it and the data it contains.

Please observe the following guidelines:

- Employ provided network resources for regularly backing up data from your laptop. Because laptops are mobile computing devices, they are much more prone to equipment failure. Regular backups performed by the user are a critical responsibility. If you cannot do this, you should not accept a laptop.
- Install personal software cautiously; if your laptop needs support, one of the first steps will be to restore it to its original configuration. This is another compelling reason to complete regular file backup.
- When leaving your workspace overnight, store your laptop in a locked drawer or cabinet.
- If you have a private office, close and lock the door if you leave during the day.
- If you take your laptop home, be sure to lock all doors when you go out. If you have a home security system, be sure it is on when you leave.

- If you are staying in a hotel, lock your laptop in a safe if your room has one. If no safe is available, lock your laptop in a suitcase when you go out.
- All laptops owned by the University must be engraved to identify ownership. This will be done by ITS before the laptop is distributed to the user.
- Keep laptop in your sight when going through airport checkpoints. Many travelers find it helpful to tape their business card to their laptops. This will help you identify your laptop in airport security.
- If you are traveling by car, lock your laptop in the trunk when you park.
- Do not use the computer in locations that might increase likelihood of damage.
- Keep food and drinks away from the computer.
- Users are responsible for purchasing padded carrying case for your laptop.

If laptops are lost, stolen, or otherwise damaged such that they cannot be restored to normal working order, they will be replaced with desktops from the pool of available cascaded computers. These computers will subsequently be upgraded according to the University's lifecycle refresh plan for desktops. At that time, users may be request for consideration for another laptop. Caretakers are responsible for reporting a loss or theft to appropriate law-enforcement agencies, as well as reporting the loss to ITS and campus police as soon as the loss occurs.

Users are encouraged to check their home insurance policies regarding coverage. The University will evaluate the circumstances of the theft or loss on a case-by-case basis to determine if reimbursement should be required.

To ensure that virus protection and other security patches are current, laptops must be connected to the campus network overnight at least once every two weeks. Users who are off-campus for more than two weeks must contact the ITS Help Desk before reconnecting their laptops to the campus network. In the case of a significant security alert, users may be contacted by e-mail and/or voicemail, to bring in their laptops to the helpdesk to ensure proper security is enabled on the laptop.

ITS support of University-owned laptops will be equivalent to that provided for University-owned desktop computers. Direct support will only be provided while laptops are on campus. Users will need their own ISP accounts if they wish to connect to the Internet from home, and may install any drivers or other software required by their ISP for remote connectivity. Users who will be accessing private, covered information (see Covered Data Security Policy) must use a VPN client to connect to University computer resources.

Because laptops are provided for University-related work, personal software should be installed very cautiously. If personal software is installed and the laptop comes to ITS for servicing, the laptop will be returned to its original configuration. Personal software or data will not be recovered.

d.) Security Incident Response Policy

Due to a variety of issues, including the safety and privacy of Anderson University students, faculty and staff, it is imperative that a reporting and response policy be followed when potential security incidents are identified.

These policies and procedures are intended for Anderson University faculty, staff and students to report any potential security incidents, and will also outline the anticipated response by ITS.

Procedure for Reporting a Security Incident

ITS should be notified immediately of any suspected or real security incident involving a University Information Technology Asset. If it is unclear as to whether a situation should be considered a security incident, ITS should be contacted to evaluate the situation.

When faced with a potential situation, faculty and staff should do the following:

- If the incident involves a compromised computer system
 - Do not alter the state of the computer system. The computer system should remain on and all of the currently running computer programs left as is. Do not shutdown the computer or restart the computer.
 - Immediately disconnect the computer from the network by removing the patch cable from the back of the computer.
- Reporting the security incident
 - Security incidents involving possible violation of Federal or state law should be immediately reported to ITS, who will report it to Anderson University Police and Security. ITS will work with AU Security and other law enforcement agencies as necessary to help resolve the incident.
 - All other security incidents should be reported to ITS for evaluation. ITS staff will then determine the appropriate response.

Document any information known while waiting for ITS response. This may include date, time, and the nature of the incident. Any information provided will aid in responding in an appropriate manner.

The Director of Information Technology services will notify the Vice-President of Enrollment Management and Information Technology who will determine others who need to be notified regarding the incident.

Response

- ITS will first attempt to determine the scope of the incident. In cases where a security incident does not require an incident response, the situation will be forwarded to the appropriate ITS staff to ensure that all technology support services required are rendered.
- An incident response may range from getting a critical system back online, gathering information or evidence, taking appropriate legal action against individual(s), or in some cases notifying appropriate ISP's or other third parties of inappropriate activity originating from their network, and completing required post-incident documentation.
- Any communications with the media regarding the incident will be coordinated through the Anderson University Office of Public Information.

Conclusion of Incident

Each security incident should be documented in such a manner that the University can learn and act proactively to prevent future instances. This documentation will also provide a reference to be used in case of other similar incidents. (System and network log files, network message traffic, user files, results produced by intrusion detection tools, analysis results, system administrator console logs and notes, and backup tapes that capture the before-intrusion and after-intrusion states of the affected system must be carefully collected, labeled, cataloged, and securely stored until the analysis of the incident is complete.)

Documentation may include:

- An explanation about how the incident happened.
- Steps required to recover from the incident.
- Assess the impact and damage of the incident
- Processes or procedures which prevent further exploitations of the same vulnerability.
- Determine who was responsible (if appropriate and possible).

Of course, depending on the seriousness of the attack, all of the objectives above may not necessarily have to be instigated. A tiered response and escalation procedure for detected potential security breaches is implemented as part of Anderson University's incident response.

20. Password Policy

Password administration is necessary to combat the forces that can compromise valuable electronic resources.

Passwords should be a minimum of 6 alphanumeric characters in combination. All passwords should contain at least one number or one letter. Passwords should be changed at least one time each semester.

The ideal password is a nonsensical or random string of characters and numbers known only to the individual who will be using them. Passwords should never be:

- Written, e-mailed, or spoken.
- Shared with other people.
- Hinted at or made easy to guess.
- Used in sync with or duplicated by personal passwords or Web accounts.
- Shared when out of the office.
- Typed or saved in electronic documents.

Failure to comply with this password policy could result in curtailed or restricted access to University information systems. Users may also incur individual liability if any University-owned or managed information system is compromised due to their negligence in the management of passwords.

21. Glossary and Definition of Terms

Our University community consists of:

Students—individuals currently enrolled in classes at Anderson University.

Faculty—current full or part time employees with faculty status.

Retired faculty—former full time faculty who have retired from teaching but who maintain a connection to the University.

Staff—those employed by the University on a full or part time basis as salaried or hourly personnel.

Access

Ability given to individual or groups of users to use information stored on or via University resources. This includes but is not limited to the ability to read, write, view, create, alter, store, retrieve, and disseminate information.

Account

That combination of user name and password that provides an individual with access to a computer system or computer network

Administrator

An individual responsible for administering and managing a computer system.

Authorized University Officials

Administrators or designees with the authority to make decisions about or approve a specific action, activity, service or use of a specific resource

Non-Authorized, Unauthorized

Applies to individuals without the authority or permission, as defined by the University, to initiate or approve an activity or service and/or to access or use a specific resource

Broadcast

Method for sending a uniform message to an entire set of users qualified by membership in a definable group such as faculty, staff, students, music majors, etc.

CDD

Click Drag and Drill. A reporting tool for use against IFAS administrative data.

Campus Online

Previously known as IRISLINK; provides Web-based access to administrative data.

Campus-wide Shared IT Resources

Information technology resources implemented and managed by Information Technology Services. Examples include the Anderson University network and modem pool, HP minicomputer, computing labs, network, etc.

Chain Letter

An e-mail message asking the recipient to indiscriminately forward or pass it along; may involve money-making pyramid schemes or be disguised as innocent (e.g., collecting post cards for a dying child) or helpful (e.g., warnings about computer virus hoaxes)

Commercial Activity

An activity conducted for commercial/private profit or gain or non-profit fundraising. This includes but is not limited to soliciting sales or funds, marketing or advertising a product or service, posting an advertisement to a newsgroup, and reselling University resources. University authorized commercial activities are excepted, e.g., Bookstore, Development, sports Booster clubs, etc.

Computer Systems

Any computing resource, service, or network system, including workstations, servers, networks, storage devices, peripheral equipment, input/output and connecting devices, data processing functions, and related records, programs, software and documentation.

Copyright Infringement

Copying, distributing, publicly performing, publicly displaying a copyrighted work, or creating a derivative work, without the permission of, or a license from, the copyright owner

Core systems/server

Electronic Communications

Any electronic method used to communicate, including but not limited to electronic mail, the Internet/World Wide Web, video recordings, facsimiles, pagers, telephones, etc. Electronic communications has the same meaning as the term defined in Subsection 12 of Section 2510 of Title 18 of the United States Code.

E-mail

Electronic method of sending and receiving messages from and to electronic addresses associated with specific owners

E-Mail Reflector

The automated or otherwise forwarding of an e-mail message to multiple recipients triggered by the content of the mail message being forwarded

Family Educational Rights and Privacy Act (FERPA)

Federal law protecting students (and former students) from the release of educational related records retained by the University

Hand-held devices

Small (capable of being held in one hand) electronic information devices. For example Palm, Handspring, etc.

IFAS

Integrated Financial and Administrative Solution

Inappropriate Use

Activities that interfere with the primary intended use of supporting instructional activities, e.g., excessive game playing

Information Technology Resources

Any data or information stored in digital form and the computer systems or other means used to access that information.

Information Technology Asset

A system or systems comprised of computer hardware, software, networking equipment, as well as any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network lines, email and web-based services.

Information Technology Services

The administrative entity charged with implementing and managing campus-wide information technology resources under the direction of the Vice President for Enrollment Management and Information Services.

Institutional Data

Information about individuals and departments that is recorded, maintained, administered and retained by the University, e.g. information in student records and employee files, financial data, etc.

Intellectual Property

Inventions, discoveries, innovations, and literary and artistic works that may be patented, copyrighted, trademarked or licensed for commercial purposes

Mail Bombing

The practice of bombarding someone with a large volume of unsolicited mail in an attempt to disrupt them or their site

Mission-critical applications

Those applications and the data generated which are essential to the daily functioning of the University. Without these, the business of the institution would soon come to a halt.

Monitoring

A standard practice by information technology resource administrators of reviewing transaction activity and other similar logs generated by the system/network, analyzing performance anomalies and traffic patterns, and/or running programs designed to identify the source of a specific problem, alarm or pattern potentially indicative of illegal or inappropriate use

Network

A group of computers and the associated equipment and transmission media used for the purpose of sending and receiving data, voice or video signals

Network/System Integrity and Reliability

Maintaining optimum performance and availability of information technology resources in support of the University mission

Personal Gain

Receiving money or other goods or services as a result of soliciting, promoting, selling, marketing or advertising products or services

Political Advocacy

Promoting, advocating or supporting a specific candidate, political party or issue

Port Scanning

Using software to access or query all known TCP ports on a system to try to identify which services and levels of security are associated with those ports. A method for determining if a network or system can be compromised.

SBI

SunGard Bi-Tech, Inc., provider of IFAS administrative software.

Security Incident

An incident meeting one or more of the following conditions:

- Any potential violation of Federal law, Texas law or Anderson University policy involving a University Information Technology Asset.
- A breach, attempted breach or other unauthorized access of a Anderson University Information Technology Asset. The incident may originate from the Anderson University network or an outside entity.
- Any Internet worms or viruses.
- Any conduct using in whole or in part a Anderson Information Technology Asset which could be construed as harassing, or in violation of Anderson University policies.

"Spam"

Indiscriminate mailing or forwarding of unsolicited e-mail to a larger group of users

System Administrator

Person responsible for administering the hardware, operating system, and software that constitutes a computer system or network

Systems

See "Computer System"

Trademark

A name, symbol, or other device identifying a product, legally restricted to the use of the owner or manufacturer

Trojan Horse

A malicious, security-breaking program that is disguised as something benign, e.g., a directory lister, archiver, or game

Unauthorized Access

Any action or attempt to utilize, alter or degrade a University owned or operated Information Technology Resource in a manner inconsistent with university policies.

University / Anderson University

The institution as a whole or the collective authority of the institution represented by established policies and designated officials responsible for enforcing them

University Resources

Any resource belonging to or employed by the University, including equipment, facilities, data and staff

User

Anyone who has been provided access to Anderson University's information technology resources

Virus

A program that searches out other programs and "infects" them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the "infection." A virus may write messages on the terminal, or play strange tricks with the display or cause irreversible damage such as deleting all of a user's files. Unlike a worm, a virus cannot infect other computers without assistance.

Web Site

Web page files (beginning with an initial home page) located on a server owned or leased by the University and which is managed through a computer account of University faculty, staff, students, administrative units, organizations, clubs and auxiliaries

Worm

A program that propagates itself over a network, reproducing itself as it goes

Policy Version 1.0

Created by Cynthia Smith/ITS staff

Approved by

Updated

Appendix A – Administrative Systems Procedures and Responsibilities

Appendix B – Network Systems Procedures and Responsibilities

Appendix C – User Support Mission and Service Standards

Appendix D – Information Security Plan

Appendix A

Administrative Systems Procedures and Responsibilities (Under revision 3/2007)

Appendix B

Network Systems Procedures and Responsibilities

Network Systems Group

This group is responsible for the design, maintenance and management of all campus server systems and network infrastructure, and core systems and services for the campus.

Some of these responsibilities regarding core systems and services are:

- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol service (DHCP)
- Shared file services
- All core server operating system related process software, patches, and maintenance
- Network management for core routing as well as edge and core switching.
- External connectivity to campus services (i.e. VPN)

- Wireless networks
- Management/Coordination of high-speed circuits to the Internet via service providers.
- Management of dial-in communication systems
- Backup systems and services for all core systems
- Logical and physical design of the campus network
- Support of and communication with staff and users as it is related to supporting end users.
- Other services as necessary to the ongoing operation of University core systems and networks.
- University electronic mail services (GroupWise)

Notification of Outages (planned and unplanned)

Notifications for planned outage will be given whenever possible and shall contain the following information:

Subject: Planned Maintenance <date and time>

Body of message should include:

- date and time of planned outage
- length of outage and approximate time of system up
- an explanation of system outage, if possible
- contact person on IT staff for outage questions

Systems and Networks staff will need to do recurring maintenance. Reminders will be sent to campus users on the day of the maintenance activity. Every attempt will be made to schedule non-critical maintenance at the least disruptive time, within the constraints of staff and support availability.

Notification for unplanned outages will be announced (as possible) during the outage/problem. If the outage affects students, they will be sent a separate message.

It is possible that, given abnormal conditions, systems may need to be rebooted/repared without the prior notification time. Information Technology will make every attempt to notify as many users as possible when systems must be brought down due to abnormal conditions.

All outages will be communicated to the HelpDesk and other IT staff immediately as well as system up notifications with a brief explanation and (if possible) an expected recovery time. IT staff may have functional service groups that they will wish to notify of an outage or problems.

When messages are sent via email to faculty and staff regarding an outage, it is the responsibility of the Manager of Student Information Services to decide if these messages need to be forwarded to student users. The Manager of Student Information Services is the point of contact for all system and networking inquiries from students. These will either be answered by the Manager of Student Information Services or forwarded to the Director of ITS.

Network monitoring

The AU network will be monitored either by individuals or software to ensure optimal service. In the event of an outage during non-business hours, users should contact 4300 and leave a message as to the nature of the outage.

Off-campus access to systems and networks

Only authorized University students, faculty or staff are allowed access to Anderson University systems and networks. Access should be secure by encryption, VPN, gateway authentication and/or other necessary means as dictated by the Director of ITS. Computer-to-computer dial-in access is prohibited.

Communication of problems with the network and systems

All outages or problems with systems and/or networks should be immediately reported to the HelpDesk. HelpDesk staff will distribute that information to appropriate staff in order to begin resolution of the problem.

Access to network switches and systems operation room (server room).

Access to network and systems operation areas is restricted to authorized personnel only. Access to these areas is authorized by the Director of Information Technology.

Network security policy- Firewall, filtering, VLAN restrictions, routing

The network security policy for Anderson University will be developed by the Director of Information Technology and the senior IT personnel. The Director of ITS will develop and maintain this policy as an ongoing document based on the changing needs of the campus. All changes to this policy will be communicated to the IT staff where necessary to their work. The Director must review any major policy changes before they are implemented.

Bandwidth usage by students

The campus network is a resource for the entire University community. Academic use of the campus network is paramount to its existence. As much bandwidth as necessary and financially possible will be given to faculty and students for academic use. Recreational use is low priority as it relates to the purpose of the campus network and systems. A certain amount of bandwidth is necessary for University operations. The University will reserve whatever bandwidth necessary for ongoing operations. Policies on bandwidth and restrictions will be made by the Director of Information Technology and IT senior staff. These policies will be communicated to the campus community through this document in its web-based form in an ongoing manner.

AU reserves the right to restrict some or all network traffic related to the following Internet services or other activities that could interfere with academic Internet use for campus users. Some examples could be:

- MP3 music downloads
- selected types of video/audio streaming related to some personal webcam devices and associated software
- selected types of online/network gaming

Departmental use of web servers and “personal server” software

Currently, AU does not officially support the use of “personal server” software on faculty, staff, or student computers.

Request procedures for network jack/cabling placement

Members of the campus community requiring a new data network connection should make a request in writing to the Director of ITS. Please be thorough in your request including building, room number, location in room, your name, organization/department name and number of connections needed. Approval of network connections will be based on need, feasibility and budget issues.

Students in residence halls are provided with one network connection per room resident. Students in campus apartments are provided with one network connection per apartment and a 100 Mb 4 or 8 port switch (available for loan through ITS D47). Additional connections will not be provided.

Network equipment standards

All departments and students must adhere to network equipment quality standards. All devices should be approved by ITS before being connected to the campus network to ensure quality of service for the user and the avoidance of problems for other users of the campus network. ITS is not responsible for network equipment that has not been approved by ITS staff and reserves the right to disconnect any equipment that is found to impede the performance of the campus network or user service.

Server systems software licensing

It is the responsibility of the Director of ITS to ensure that server-based systems software is legally licensed and available to the appropriate number of users by those licenses.

Access to systems and servers

The Director of Information Technology is responsible for administrator-level passwords and access to administrator-level accounts. No non-University personnel shall have access to administrator-level accounts without prior approval of the Director of ITS.

Any access to the systems for functional/operational reasons shall be given only with prior written approval of a departmental-level director or appropriate University sponsor. This written approval should include all details about needed access including reasoning and information on outside entity(ies) that will be accessing University systems. All final approval for access to systems to outside users lies with the Director of Information Technology to ensure the security and integrity of University systems and network services.

Access to service management agents and facilities is given as needed by the Director of ITS to empower the agent to do their work in the best way possible.

Any unauthorized access can result in disciplinary action, dismissal from the University and/or legal action.

Use of Listservs and Distribution lists

ITS maintains Groupwise Distribution Lists for Faculty, Staff, FacultyStaff, Forum and Classifieds. Access to the Students distribution list is through Dean of Students. To request a distribution list, please contact the Director of ITS.

Listservs are available to faculty upon request for specific classes. Contact ITS.

Appendix C

User Support Mission and Service Standards

User Support Mission Statement

The mission of User Support Services is to reliably connect people, processes, and content through the effective use of standardized technologies and consulting services in support of the University's core mission: to educate persons for a life of faith and service in the church and society.

We are dedicated to the highest professional standards in support of the teaching and learning mission at the university. To ensure the best possible service for all users, we are committed to the guidelines below as they relate to technology resources supported by ITS.

Answering inquires and resolving problems

ITS Staff will:

- Own the problem until it is resolved or until it is referred to a person or department that can resolve it.
- Acknowledge and attempt to respond to a problem as quickly as possible (e.g. within 24 hours, same or next business day).
- Engage in a collaborative problem solving when appropriate.
- Encourage users to call the Help Desk if the problem is not resolved or continues.
- Keep users informed of progress or referral of their problem to another resource.
- Contact and inform end-user that the problem is resolved.
- Utilize the Service Feedback Form (sent automatically when a call is closed) to ascertain if end-user is satisfied with how the problem was resolved.

Give clear, accurate and consistent information about User Support Services procedures to all customers

Strive to have someone available to answer end-user calls at all times during the business day.

Call Request Procedure for Users

Calls are placed by contacting x4300, sending a request to its@anderson.edu, or forwarding a request through the ITS web page. Requests placed directly with other ITS staff or student workers are easily lost in our triage system; thus we encourage all users to follow the channels for placing help requests.

Completing a Request

- Users are asked to be aware that your call is one of dozens we receive every day. While your need is important to us, it will be handled within our system of call management. Not every request can be resolved immediately. Every request, however, should be acknowledged and the end-user updated regularly on the status of their request.
- All requests will be acknowledged either by email or by a staff contact. If request has not been responded to in some way within 36 hours, feel free to contact us again and ask for an update on the status of your request.
- All requests are “triaged.” Those most disruptive to the work of the institution are handled first; those disruptive to a single user are handled next; non-disruptive calls are handled last.

Examples of service prioritization;

- Network Outage
- Server Outage
- Mission-critical task or critical time frame
- Inoperable equipment due to hardware failure
- Network connection issues
- Possible virus infection
- Other requests including software updates or upgrades, hardware upgrades, malfunctioning software, or other equipment.

Requests with no priority (will be handled when ALL other work is done or not at all)

- Those which involve non-supported software.
 - Those which involve equipment which is not owned or managed by Anderson University.
 - Those which violate copyright, licensing or other restrictions.
- All requests will be worked on by an ITS employee until complete, or until an agreement is made between the user and the ITS employee on the level of completeness.
 - If a user has a question about the ITS employee who worked on their equipment or request, or the completeness of a request, please contact the Help Desk Manager. Student workers will be asked to return to complete the request to ITS standards.
 - If a request has not been completed to the user’s satisfaction, ITS asks that the user report that to the Help Desk Manager. If this does not resolve the problem, please report that to the Director of Information Technology Services.

Student Workers

Information Technology Services employs a number of students to assist in our daily work. These students bring a variety of skills and talents to our office and play a major role in our ability to complete our mission. As such, they should be accorded same respect and courtesy given to full-time staff members.

At the same time, their primary reason for being at Anderson University is academic. Matters concerning academics are placed above all other tasks. Students are expected to perform to a high standard in the classroom. If this standard is not met, a student’s hours may be reduced in order to assure academic success.

ITS views the employment of student workers as an extension of their educational process. We provide an environment in which students put into practice what is learned in the classroom. We expect the highest level

of workmanship from all student employees, both related to the tasks they are assigned and in their dress, personal hygiene, and work habits.

Appendix D Anderson University Information Security Plan

This Information Security Plan describes Anderson University's safeguards to protect *covered data and information*. These safeguards are provided to:

Ensure the security and confidentiality of covered data and information;

- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by Anderson University;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the plan; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Identification and Assessment of Risks to Customer Information

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

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Anderson University recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, Information Technology Services will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

Anderson University believes ITS current safeguards are reasonable and, in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the University. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Information Security Plan Coordinators

The Vice President for Enrollment Management and Information Technology Services has been appointed as the coordinator of this Plan. He is responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to Anderson University. Internal audit personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that Anderson University departments comply with the requirements of this policy.

Design and Implementation of Safeguards Program

1. Employee Management and Training

- References of new employees working in areas that regularly work with covered data and information (Cashier's Office, Registrar, Development and Financial Aid) are checked.
- During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information.
- Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling" and how to properly dispose of documents that contain covered data and information.
- Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.
- Further, each department responsible for maintaining covered data and information should coordinate with Information Technology Services on an annual basis for the coordination and review of additional privacy training appropriate to the department.
- These training efforts should help minimize risk and safeguard covered data and information security.

2. Physical Security

Anderson University has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to Anderson University employees with an appropriate business need for such information.

Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

3. Information Systems

Access to covered data and information via Anderson University's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to Anderson University employees in appropriate departments and positions.

Anderson University will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. ITS requires that all servers must be registered before being allowed through Anderson University's firewall, thereby allowing ITS to verify that the system meets necessary security requirements as defined by ITS policies. These requirements include maintaining the operating system and applications, including application of appropriate patches and updates in a timely fashion. User and system passwords are also required to comply with the Anderson University Password Policy. In addition, an intrusion detection system has been implemented to detect and stop certain external threats, along with an Incident Response Policy for occasions where intrusions do occur.

When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are behind Anderson University's firewall. All firewall software and hardware maintained by ITS will be kept current. ITS has a number of policies and procedures in place to provide security to Anderson University's information systems. These policies are available upon request from the Director of Information Technology Services.

Social Security Numbers (SSN) as Unique Identifiers

Anderson University collects SSNs for the purpose of processing student loans and to meet other legal obligations, such as the reporting of income for tax purposes. The Social Security Number is considered personal information and its dissemination must comply with FERPA guidelines. SSNs will not be used as

primary identification numbers within the Anderson University system. They will, however, be considered as one point of data when attempting to match or authenticate users.

Management of System Failures

ITS will develop written plans and procedures to detect any actual or attempted attacks on Anderson University systems and will develop an Incident Response Policy which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This policy is available upon request from the Director of Information Technology Services.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that Anderson University determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information.

Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles Anderson University to terminate the contract without penalty; and
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within ITS, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Plan Coordinator who will assign specific responsibility for ITS implementation and administration as appropriate. The Coordinators, in consultation with the University Counsel, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

Covered data and information for the purpose of this policy includes *student financial information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required under federal law, Anderson University chooses as a matter of policy to also include in this definition any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

Student financial information is that information that Anderson University has obtained from a customer in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.