ANDERSON UNIVERSITY
Academic and Christian Discovery

Acceptable Use Policy

Overview

Information Technology Services (ITS) is committed to protecting Anderson University's students, employees, alumni, retirees and the University from illegal or damaging actions by individuals, either knowingly or unknowingly. The intent of this Acceptable Use Policy is to establish a culture of openness, trust and integrity aligned with the ethos of Anderson University.

Effective security is a team effort involving the participation and support of every Anderson University student, employee, and affiliated person who deals with information and/or information systems. It is the responsibility of every computer user to read, understand, and comply with this Acceptable Use Policy.

Purpose

The purpose of this policy is to outline the acceptable use of computer resources at Anderson University. These rules are in place to protect the students, employees, and affiliated persons and Anderson University. Inappropriate use exposes Anderson University to risks including virus attacks, compromise of network systems and services, loss of critical institutional and personal data, and legal issues.

Scope

This Acceptable Use Policy applies to the use of information, electronic and computer devices, and network resources to conduct Anderson University business or interact with internal networks and business systems, whether owned or leased by Anderson University, students, employees, or third parties. All students, employees, contractors, consultants, and other affiliated persons of Anderson University are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Anderson University policies and standards, and local, state and federal laws and regulation.

Requirements for Use of Anderson University Resources

- Familiarize self and comply with the complete Acceptable Use Policy
- Indicate agreement with expectations by signing the Acceptable Use Policy
- (Administrative Users) Sign the Administrative Systems Confidentiality Agreement
- Obtain proper authorization to access resources

Acceptable Use of Resources

Acceptable and Collegial Use of Resources

Anderson University computing and information technology resources are to be used appropriately and in a manner consistent with the instructional, research, and administrative objectives of the University. Anderson University computing resources are shared resources, which need to be used collegially.

Acceptable use includes:

- Instruction
- Independent study
- Official work of faculty, staff, students, offices and departments
- Official work of recognized student and campus organizations
- Official work of agencies of the University
- Occasional or incidental noncommercial, personal use by authorized users

Collegial use includes:

- Using common sense
- Using resources responsibly, for authorized purposes, and in an approved manner
- Observing standards of decency
- Respecting the privacy of others
- Respecting the rights and wishes of others in the use of sounds and visuals in public areas
- Being sensitive to the impact of your traffic on network performance
- Practicing good stewardship of connect time, information storage space, printing facilities, processing capacity, and network services

Unacceptable Use of Resources

Anderson University's computing and information technology resources are of substantial benefit to everyone in the University community. However, an individual's benefit could be diminished appreciably if only a few people were to misuse these resources.

The following activities are, in general, prohibited. The lists are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Any use that violates

- Local, state and/or federal laws
- Copyrights or other intellectual property rights
- License agreements
- Purchase agreements
- Acceptable use agreements of any other entity traversed or used through Anderson University resources
- Political involvement expectation as a tax-exempt nonprofit institutions (see Section 3.94 "Political Involvement" in the Faculty Handbook and p. 24 "Political Activity" in the Staff Handbook).

Posting, distributing, and/or propagating

- Unsolicited advertising
- Computer worms or viruses

- Chain letters
- Material copyrighted by another
- Fraudulent or misleading information
- Libelous, slanderous, threatening, or harassing materials of any description
- Any materials that demean, defame, or ridicule another person
- Obscene, pornographic, sexually explicit, or patently offensive materials
- Any materials contrary to the mission or values of Anderson University

Attempting, whether successful or not

- To enter another device on the network (e. g., computer, network device, etc.) without authorization
- To enter another's account, files, or file space without authorization
- To modify any software or information without authorization
- To conceal or falsify one's identity in any electronic communication or activity
- To intercept network traffic intended for another device on the network other than your own
- To set up, operate, or maintain a server, network analysis tool, or network management tool on the AU network without authorization
- To use any Internet Protocol (IP) address inside or outside the AU domain(s) without prior approval
- To damage or destroy any equipment, software, or data

Any use that

- Is illegal, immoral, unethical, or dishonest in nature
- Unreasonably denies or could deny access or service to others, including excessive use for recreational games or personal purposes
- Is for commercial purposes or personal gain
- Promotes a political position or cause célèbre
- Interferes with the University's activities or the University-related activities of any authorized user
- Is, or could reasonably be expected to be, damaging to the reputation of the University

Exceptions to Acceptable Use

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., ITS systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). For security and network maintenance purposes, authorized individuals within Anderson University may monitor equipment, systems, and network traffic at any time during the course of their legitimate job responsibilities.

Anderson University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Responsibilities of Users

Account holders are responsible for adhering to this Acceptable Use Policy.

Account holders are responsible for anything done with their accounts. Accounts, passwords, and other types of authorization that are assigned to individual users should not be shared with others. If a user suspects account security has been violated, the password should be changed immediately and ITS notified immediately.

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- The user should assign an obscure account password and change it frequently.
- The user should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive or confidential information.
- The computer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes.
- Primary responsibility for resolution of problems related to the invasion of the user's privacy or loss of data rests with the user.
- The computer user should consider whether information distributed using University resources should be protected from unauthorized use by the use of copyright notices or by the restriction of distribution of certain materials to the campus.

Responsibilities of the University

The University, through ITS, is responsible for providing central system and network security and for taking reasonable steps to protect central systems and networks and the information stored thereon from excessive or inappropriate use, damage, or destruction. These responsibilities include:

- Instructing, encouraging, and, for critical systems, forcing users to select reasonably secure passwords and to change them periodically;
- Implementing measures to protect systems from hacking, invasion, viruses, and similar threats, and maintaining these measures at a reasonably current level;
- Removing any viruses or other malicious software that may be found on central systems;
- Monitoring use of systems and networks for traffic volume, log activity, or other symptoms of excessive or unauthorized use;
- Promptly taking appropriate measures to halt unauthorized or inappropriate use including, if necessary, imposing appropriate resource allocations or restrictions;
- Performing regular backups of centrally-stored information and maintaining these backups for a reasonable length of time;
- Periodically removing selected backups to a safe offsite location;
- Diligently pursuing and working with other interested offices, departments, agencies, vendors (within the University or outside the University) to resolve violations of the Acceptable Use Policy or other threats to the availability and security of University computing resources;
- Advising owners and custodians of other University computing resources on the manner and means of accomplishing these objectives with respect to the systems they manage.

Security

Anderson University assumes users are aware that electronic files and transmissions are not necessarily secure.

Users of electronic mail systems should be aware that electronic mail is extremely vulnerable to unauthorized access, modification, and forgery.

Users should be aware that information sent or received via the Internet is not necessarily secure. Moreover, many Internet sites collect information about the source of inquiries, and some store markers (known as "cookies") on the user's computer system for later retrieval by their site or other sites. It is possible for software on a web site to explore and retrieve information from the user's computer without the user being aware of the invasion.

Anyone who downloads software, certain applications, or certain file types (such as Microsoft Word documents) should be aware of the possibility that such material could incorporate viruses, worms, or other destructive materials.

Protecting Your Computer Accounts

- Select obscure passwords. Passwords should be at least 8 characters and contain a combination of letters and numbers or special characters but no spaces. Birth dates, social security numbers, and other identifying information do not make secure passwords.
- Change your password(s) regularly, and at any time you believe it (they) may have been compromised. ITS requires all users to change passwords at least every 180 days on ITS-managed systems.
- Do not share your login id(s), password(s), or other types of authorization with others.

Protection from Viruses, Worms, etc.

- Download materials only from reliable sources.
- Scan for viruses whenever you introduce new software or documents to your computer. ITS provides anti-virus software, and routinely scans its servers and ITS-managed workstations. Anti-virus software is a part of ITS software installation on any University-owned workstation.

Confidentiality of Accounts and Communication

Anderson University provides computers, networks, network connections, and other telecommunication services to support the work of teaching and learning, conducting research, completing University tasks, and conducting the affairs of the University. The University reserves the right to access, review, and monitor electronic communications, computer files, and computer usage.

ITS staff members will not gratuitously scan others' communications, files, or usage; and the University specifically disclaims responsibility for the content of any individual's communications and files that are not manifestly related to University business.

In the normal course of managing computer and network resources, an ITS staff member may incidentally become aware of content of certain communications or files, or of certain usage patterns. In the event an ITS staff member becomes aware of any information that suggests activity that is illegal or in violation of the Acceptable Use Policy, that staff member is honor-bound to report it to proper authority.

University employees must understand that University computing and communication accounts (including, but not necessarily limited to file spaces, e-mail accounts, and local computer space) are presumed to be used for University business. In situations where an employee leaves the employ of the university that employee's accounts and any information remaining therein may be accessed to ensure continuity of business operations, research, teaching and educational programs.

In addition, in circumstances where University business requires immediate access to information known to exist in an employee's account, and that employee is not available, access to the employee's accounts may be granted for the sole purpose of gaining access to the needed information. For the purposes of this paragraph, "not available" shall be taken to mean that the employee cannot be contacted via normal means of communication sufficiently soon to enable the University to protect the health, safety, or legal interests of the University or persons associated with the University, as determined by appropriate authority and agreed by the Provost's Office and/or the President's office.

ITS staff will also provide access to centrally-stored communications and files at the written request of duly constituted authority having jurisdiction over any investigation of activity that is illegal or in violation of the Acceptable Use Policy. All members of the University community should be aware that the University has the capability of retrieving computer information, including but not limited to electronic mail messages, files, and information about Internet sites visited.

When sources outside the University request an inspection and/or examination of any University owned or operated communications system, computing resource, and/or files or information contained therein, the University will treat information as confidential unless any one or more of the following conditions exist:

- When approved by the appropriate University official(s)
- When authorized by the owner(s) of the information
- When required by federal, state, or local law
- When required by a valid subpoena or court order

Note: When notice is required by law, court order, or subpoena, computer users will receive prior notice of such disclosures.

Violations

Jurisdiction

Violations of the Acceptable Use Policy may be of many different characters, and the procedures to be followed may be governed by different University policies, depending on the nature of the offense and the status of the offender.

In cases where the violation is primarily a violation of other University policies as set forth in official University documents including, but not limited to, the Student Handbook, the Faculty Handbook, or the Staff Handbook (University Violation), the procedures and sanctions set forth in those documents shall apply.

In cases where the violation is primarily a civil violation of federal, state, or local laws or regulations, the matter should be referred to the appropriate University official — Dean of Students, Provost, Copyright Officer, etc. — (whether or not the violator is a member of the Anderson University community), and the normal policies and procedures of the office having jurisdiction should be followed.

In cases where the violation is primarily a criminal violation of federal, state, or local laws or regulations (Criminal Violation), the matter should be referred to the Anderson University Police/Security Services Department (whether or not the violator is a member of the Anderson University community), and the normal policies and procedures of AU Police/Security Services should be followed.

In cases where the violation is a simple violation of the Acceptable Use Policy, with no other ramifications (Simple Violation), the matter should be referred to ITS.

Procedures

Violations should be referred to the appropriate jurisdiction. Such jurisdiction should immediately refer any concerns affecting network traffic, access, or security to ITS staff.

Whenever ITS becomes aware of a violation of this Policy, ITS staff will review the violation and refer it to the appropriate jurisdiction if that has not already been done.

As soon as ITS becomes aware of a violation of this Policy (whether or not that violation has been referred to other authority), ITS staff will take appropriate measures to halt the violation, secure the network and resources, and comply with applicable laws and regulations pending resolution of the matter. These measures may include halting a program running on central systems; disconnecting remote systems from the network; removing offending material from Anderson University systems or rendering it inaccessible; disabling user accounts; or any other measures necessary to accomplish cessation of the violation, preservation of the integrity of University resources, and compliance with legal and regulatory mandates.

In the case of a first Simple Violation (see above) of Acceptable Use Policy, ITS staff will contact the offender, advise the offender of the violation, and attempt to secure the violator's cooperation.

In the case of repeated Simple Violations or any University Violations (see above) of Acceptable Use Policy, ITS will confer with the Dean of Students in the case of a student or the supervisor in the case of a regular employee to determine what further action needs to be taken.

In the case of a first Civil Violation (see above), the University will follow the procedure for University Violations and, in addition, take appropriate steps to protect its interests, including conferring with University Legal Counsel.

In the case of Criminal Violations, the matter will immediately be referred to Anderson University Police/Security Services for investigation and possible prosecution. In addition, other appropriate steps will be taken as necessary to protect the University's interests.

In the case of Criminal Violations, repeated Civil Violations, or egregious University or Simple Violations of Acceptable Use Policy, the violator's computing privileges will be terminated and the matter will be escalated to higher administrative authority for final resolution.

Sanctions

In addition to sanctions, disciplinary action, or legal action that may be imposed by the authority having jurisdiction over the violator, violations of the Acceptable Use Policy may lead to suspension or loss of computing privileges.

Revision History

Date of Change	Responsible	Summary of Change
September 14, 2017	Michael Tucker, Director, ITS	Updated and converted to new format
March 2007		