ASU System Policy

DRAFT

Effective Date: December 11, 2009

Subject: Appropriate Use of Information & Technology Resources

---

1. Purpose

Arkansas State University System (University) invests substantial and sufficient resources to acquire and operate information technology (IT) assets, such as hardware, software, and Internet connections. The University has a responsibility to manage its resources in the most efficient and effective manner possible and in compliance with all laws, regulations, and sound business practices, while at the same time protecting and preserving the right to academic freedom. Effective management of information technology resources will assure students, faculty, and staff adequate access to information and technology over the long term. The following regulations are established to define acceptable uses of University Information resources, and to assure that information technology resources promote the basic functions of the University in teaching, learning, research, administration, and public service. These regulations apply to any entity or individual accessing the Arkansas State University information technology infrastructure and associated resources.

2. Definitions

IT Resources. These are the computers, terminals, printers, networks, telecommunications systems, modem banks, networked peripherals, online and offline storage media and related equipment, software, and data files that are owned, leased, managed, or maintained by Arkansas State University. For example, IT Resources include institutional and departmental information systems, faculty research systems, desktop computers, the University's campus network, and University general access computer labs, and the University's administrative systems.

User. A "User" is any person, whether authorized or not, who makes any use of

any University IT Resource from any location. For example, Users include a person who accesses IT Resources within the confines of the University plant or via an electronic network.

University Community. Any person who accesses the University's IT infrastructure who is not classified as a member of the faculty (full- or part-time), staff (full- or part-time) or enrolled student.

Systems Authority. Arkansas State University delegates oversight of particular systems to the head of a specific unit of the University or to an individual faculty member, in the case of IT resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator. A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT Resources.

Certifying Authority. This is the Systems Administrator or other University authority who certifies the appropriateness of an official University document for electronic publication in the course of University business.

Specific Authorization. This means documented permission provided by the applicable Systems Administrator.

3. Arkansas State University System Appropriate Use of Information & Technology Resources Policy

Information and Technology Resources may be used only for their authorized purposes – that is, to support the research, education, administrative, and other functions of Arkansas State University.

4. Process

Although this policy sets forth the general parameters of appropriate use of IT Resources, faculty, students, and staff should consult their respective handbooks and campus operating procedures for more detailed statements on permitted use and the extent of use that the University considers appropriate in light of their varying roles within the community. In the event of conflict between other guidelines and the System Appropriate Use of Information & Technology Resources Policy, the Appropriate Use Policy will prevail.

A. Proper Authorization.

Users are entitled to access only those elements of IT Resources that are consistent with their authorization. Access is limited to members of the University Community, faculty, staff, students, and other specifically authorized individuals.

B. Ownership.

All data stored on University IT Resources is owned by the University. Intellectual Property rights will, of course, be recognized as established by policy.

C. Privacy.

Users agree to access only data that they are authorized to use and/or view. Privacy in an electronic environment should never be assumed and cannot be guaranteed. Because Arkansas State University is a state agency, all electronic communications and documents are presumed to be subject to the Freedom of Information Act.

D. Specific Proscriptions on Use.

The following categories of use are inappropriate and prohibited:

1. Use in violation of law. Illegal use of IT Resources – that is, use in violation of civil or criminal law or regulation at the federal, state, or local levels – is prohibited. Examples of such uses are: promoting a pyramid scheme, accessing or distributing illegal material, copyright infringements, and making bomb threats.

With respect to copyright infringements, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and “fair use,” for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

2. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny, attempt to deny, or interfere with service to other users in any way, including by “resource hogging,” misusing mailing lists, propagating “chain letters” or virus hoaxes,

"spamming" (spreading email or postings widely and without good purpose), or flooding an individual, group, or system with numerous or large email messages. Other behavior that may cause excessive network traffic or computing load is also prohibited.

3. Use that is inconsistent with the University's public service status. The University is a non-profit, public service organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Resources for non-University purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization. Commercial advertising is strictly prohibited unless authorized by contract with the commercial vendor.

Utilization of IT Resources in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Resources for the purpose of lobbying that connotes University involvement.

4. Harassing or threatening use. This category includes, for example, repeated unwelcome contacts with another.

5. Use damaging the integrity of University or other IT Resources. This category includes, but is not limited to:

a. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking", decoding, guessing or applying the identification or password of another User, or compromising system/data security mechanisms. (This provision does not prohibit, however, ITS or Systems Administrators from using security scan programs within the scope of their Systems Authority.)

b. Unauthorized access or use. The University recognizes the importance of preserving the integrity of data stored by individuals in IT Resources. Users must honor this principle by neither seeking to obtain unauthorized access to IT Resources, nor permitting or

assisting any others doing the same. For example, a non-University organization or individual may not use non-public IT Resources without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-University organizations or individuals across the University network without specific authorization. Similarly, Users are prohibited from accessing IT Resources that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

c. Disguised use**.** Users must not conceal their identity when using IT Resources, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

d. Distributing computer viruses. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

e. Modification or removal of data or equipment. Without specific authorization, Users may not remove or modify any University-owned or administered equipment or data from University property or IT Resources.

f. Use of unauthorized devices. Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to the IT infrastructure or related resources.

6. Use in violation of external data network policies. Users must observe all applicable policies of external data networks when using such networks.

E. University Access.

In accordance with state and federal law, the University may access all aspects of IT Resources, without the consent of the User. Such access will be made in circumstances including but not limited to the following:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Resources; or

2. When authorized by federal, state, or local law or administrative rules; or

3. When there are reasonable grounds to believe that a violation of law or a breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

4. When such access to IT Resources is required to carry out essential business functions of the University; or

5. When required to preserve public health and safety.

University access without the consent of the User will occur only with the approval of the appropriate Vice Chancellor, or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The University, through the Systems Administrators, will log all instances of access without consent. Systems Administrators will also log any emergency entry within their control for subsequent review by appropriate University authority.

In addition to accessing the IT Resources, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

By attaching privately owned personal computers or other IT Resources to the University's network, Users consent to University use of scanning programs for security purposes of those resources while attached to the network.

Most System Administrators routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post procedures concerning logging of User actions including the extent of individually identifiable data collection, data security, and data retention.

Encrypted files, documents, and messages may be accessed by the University under the above guidelines.

F. Enforcement Procedures

1. Complaint of Alleged Violations. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established University grievance procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the University Information and Technology Services unit, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

2. Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the University Information and Technology Services unit, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

3. Disciplinary Procedures. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the applicable Handbook.

Systems Administrators and the Information and Technology Services unit may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators, and the Information and Technology Services unit are authorized to investigate alleged violations.

4. Legal Liability for Unlawful Use. In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT Resources.

5. Appeals. Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

(Adopted by the Arkansas State University Board of Trustees on December 11, 2009, supercedes Arkansas State University-Jonesboro Appropriate Use of Information and Technology Resources Policy (Appropriate Use Policy) of March 8, 2002.)