Policy Contents

- Purpose and Summary
- Scope
- Definitions
- Policy
- Compliance and Responsibilities
- Revision History*

Policy Information

Effective Date:
March 1, 2004

Last Revised Date:
February, 2010

Policy Number:
IS-701

Reference:
Classified Staff Human Resources Policy Manual 419.0
University Handbook for Appointed Personnel 2.07.05
Student Employment Manual 112.0

Responsible Unit:
UA Information Security

Phone:
(520) 626-8324

Email:
infosec@email.arizona.edu [1]

Purpose and Summary

The University of Arizona provides a wide variety of computing and networking resources to all qualified members of the University community. Access to computers, computing systems, and networks owned by the University of Arizona is a privilege which imposes certain responsibilities and obligations and which is granted subject to University policies and codes, and local, state, and federal laws. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources, including wireless. The purpose of this policy is to promote the efficient, ethical, and lawful use of the University of Arizona’s computer and network resources.

Individuals using computer resources belonging to the University of Arizona must act in a
responsible manner, in compliance with law and University policies, and with respect for the rights of others using a shared resource. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.

Violations of this policy are subject to sanctions prescribed in, but not limited to, the following policies: Arizona Board of Regents Code of Conduct, Student Code of Conduct, Code of Academic Integrity, Classified Staff Human Resources Policy Manual, and University Handbook for Appointed Personnel. Some potential sanctions are listed below.

Scope

This policy applies to all users of University of Arizona computing and network resources, whether initiated from a computer and/or network device located on or off campus.

Definitions

"Antivirus Software" is software specifically designed for the detection and prevention of known computer viruses.

"Spam" is unsolicited junk e-mail sent to large numbers of people to promote products or services.

Policy

Acceptable Use Guidelines

The specific usage guidelines that follow are not intended to be comprehensive, but rather to establish and clarify the intent of this policy. Situations not enumerated here will inevitably arise, and they should be interpreted according to the spirit of this policy.

Each person using the University of Arizona's computer and network resources should

1. Take no actions that violate the Codes of Conduct and Academic Integrity, UA Human Resources policies, or other applicable policy or law. This is not a comprehensive list of applicable University policies. In the event of a conflict between policies, the more restrictive use policy shall govern.

   See the following related manuals/documents for more information:
   ○ University Handbook for Appointed Personnel [2]
   ○ Classified Staff Human Resources Policy Manual [3]
   ○ Student Code of Conduct [4]
   ○ Misuse of University Assets [5]
   ○ Approved Use of University Computing and Communications Equipment [6]

2. Use security measures to protect the integrity of information, data, and systems.

   Users shall protect their computer systems and accounts by using strong passwords; installing "Antivirus Software" consistent with management directives; and keeping such software, as well as the operating system and application security patches, up to date. Users are responsible for safeguarding their identification codes and passwords, and for using them only as authorized. Examples of misuse include using a computer account and/or obtaining a password that you are not authorized to use, using the campus network to gain unauthorized
access to any computer system, and using a "sniffer" or other methods in an attempt to "crack" passwords.

See the following related documents for more information:
- Information Security Policy (IS-100) [7]
- UA Electronic Privacy Statement (IS-1000) [8]
- Family Educational Rights and Privacy Act (FERPA) Compliance [9]

3. **Clearly and accurately identify one's self in electronic communications.** Do not forge or misrepresent one's identity. Concealing or masking the identity of electronic communications, such as altering the source of an e-mail message by making it appear as if the message was sent by someone else is a violation of this policy.

See the following related policies for more information:
- Official Student E-mail Policy [10]
- Use of E-mail for Official Correspondence with Employees [11]

4. **Use computer and network resources efficiently.** Computing resources are finite and must be shared. Users may use the University's computer and network resources for incidental personal purposes, provided that such use does not (a) unreasonably interfere with the use of computing and network resources by other users, or with the University's operation of computing and network resources; (b) interfere with the user's employment or other obligations to the University; or (c) violate this policy or other applicable policy or law. The University retains the right to set priorities on use of the system, and to limit recreational or personal uses when such uses could reasonably be expected to cause, directly or indirectly, strain on any computing facilities; to interfere with research, instructional, or administrative computing requirements; or to violate applicable policies or laws. Examples of inappropriate use include circumventing the editor or moderator to post messages to private (closed) listservs, sending "chain letters" or engaging in pyramid schemes, or engaging in unauthorized peer-to-peer file sharing. Sending "spam" or posting inappropriate promotional or commercial messages to discussion groups or bulletin boards, is not permitted.

See the following related policies for more information:
- Approved Use of University Computing and Communications Equipment [6]
- Misuse of University Assets [5]

5. **Do not harass or intimidate or use computer and network resources for unlawful acts.** The University, in general, cannot and does not wish to be the arbiter of content maintained, distributed, or displayed by users of the University's computing and network resources. For example, the University, in general, cannot protect users from receiving e-mail they may find offensive. Using the University's computer or network resources for illegal activities, however, is strictly prohibited. Unlawful use of University computer and network resources can expose the individual user and the University to damages claims or potential criminal liability. Unlawful uses may include, but are not limited to, harassment and intimidation of individuals on the basis of race, sex, religion, ethnicity, sexual orientation, or disability; obscenity; child pornography; threats; theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws. Do not use computer systems to send, post, or display slanderous or defamatory messages, text, graphics, or images. By using the University's computer and network services, each user accepts the responsibility to become informed about, and to comply with, all applicable laws and policies.

6. **The use of University computer resources and networks is for legitimate academic or administrative purposes.** Incidental personal use is permissible to the extent that it does not
violate other provisions of this policy, interfere with the performance of the employee's duties, or interfere with the education of students at the University. Use of your computer account or the network for commercial activities that are not approved by appropriate supervisory University personnel consistent with applicable policy, or for personal financial gain (except as permitted under applicable academic policies) is prohibited. Examples of prohibited uses include using your computer account for engaging in unauthorized consulting services, software development, advertising products/services, and/or other private commercial activity.

See the following related documents for more information:
- Acknowledgment and Advertising on UA Web Pages [12]
- Misuse of University Assets [5]

7. **Respect copyright and intellectual property rights.** Users must adhere to the U.S. Copyright Act, the Intellectual Property Policy, and the terms and conditions of any and all software and database licensing agreements. Any form of original expression fixed in a tangible medium is subject to copyright, even if there is no copyright notice. Examples include music, movies, graphics, text, photographs, artwork, and software, distributed in any medium—including online. The use of a copyrighted work (such as copying, downloading, file sharing, distribution, public performance, etc.) requires either (a) the copyright owner's permission, or (b) an exemption under the Copyright Act. The law also makes it unlawful to circumvent technological measures used by copyright owners to protect their works. Copyright infringement exposes the user, and possibly the University, to heavy fines and potential criminal liability. Therefore, without limitation of other possible sanctions, the University may refuse, suspend, and/or terminate computer and network access with respect to any user who violates the copyright law or who uses the University's computer or network resources contrary to the terms of the University's software or database license agreements.

See the following related documents for more information:
- U.S. Copyright Office [13]
- Copyright and Fair Use [14]
- Copyright FAQs, including Peer-to-Peer File Sharing [15]
- UA Library's Copyright Guide [16]

8. **Respect University property.** Misuse of University property includes, but is not limited to, stealing or damaging equipment or software, knowingly running or installing computer viruses or password-cracking programs, attempting to circumvent installed data protection methods that are designed and constructed to provide secure data and information, in any way attempting to interfere with the physical computer network/hardware, or attempting to degrade the performance or integrity of any campus network or computer system.

See the following related policy for more information:
- Misuse of University Assets [5]

9. **Make only appropriate use of data to which you have access.** Authorized University personnel (e.g., system, network, and database administrators, among others) may have access to data beyond what is generally available. Privileged access to data may only be used in a way consistent with applicable laws, University policies, and accepted standards of professional conduct. Those who have access to databases that include personal information shall respect individual privacy and confidentiality, consistent with applicable laws and University policies regarding the collection, use, and disclosure of personal information. Users should be aware however that state laws and University policies, guidelines, and regulations may prevent the protection of certain aspects of individual privacy. Both the nature of electronic communications and the public character of the University's business make certain uses less private than users may anticipate. For example, in certain circumstances, the
University may permit the inspection, monitoring, or disclosure of e-mail, consistent with applicable laws and with the University's Electronic Mail Policy.

See the following related policies/documents for more information:
  - UA Electronic Privacy Statement (IS-1000) [8]
  - Family Educational Rights and Privacy Act (FERPA) Compliance [9]

10. **Respect and adhere to other departmental/college/Internet Service Provider’s acceptable use policies.** When using a University computer system and/or network to connect to a non-University of Arizona system or network, adhere to the prevailing policies governing that system or network. This does not in any way release your obligation to abide by the established policies governing the use of University of Arizona computer systems and networks.

**Recourse for Misuse and/or Noncompliance**

Aforementioned policies in this document include action steps to be taken to determine whether or not an individual has, in fact, misused University computing and/or network resources. Protections of the rights of individuals accused of policy violations afforded by those policies also apply.

Users who misuse University computing and network resources or who fail to comply with the University's written usage policies, regulations, and guidelines are subject to one or more of the following consequences:

- Temporary deactivation of computer/network access
- Permanent deactivation of computer/network access
- Disciplinary actions taken by the department or Dean of Students Office up to and including expulsion from school or termination of employment
- Subpoena of data files
- Legal prosecution under applicable federal and state laws
- Possible penalties under the law, including fines and imprisonment

**Compliance and Responsibilities**

Violations, complaints and questions should be reported to the University Information Security Office by e-mail (infosec@email.arizona.edu [1]) or by phone (520-626-8324).

**Revision History**

Revised February 22, 2010

**Source URL:**
http://policy.arizona.edu/information-technology/acceptable-use-computers-and-networks

**Links**
[1] mailto:infosec@email.arizona.edu