



**THE UNIVERSITY OF
ALABAMA AT BIRMINGHAM**

Acceptable Use Policy

Release 1.0



Reviewed: September 2008



Acceptable Use Policy (AUP)

UAB Policy for Acceptable Use of Computer and Network Resources

August 27, 2004

UAB computer and network resources are allocated only for activities that support UAB's mission of instruction, research, and service or other approved activities. These resources may not be used for any activity which is destructive, disruptive, or illegal. Further, these resources may not be used for activities which interfere with the ability of UAB to support its mission, compromise the character and reputation of UAB by association, or violate the UAB Conflicts of Interest Policy. UAB students, faculty, employees, and other users are responsible for adhering to this policy.

UAB secures its computers, systems, servers, campus network, and external connectivity to a reasonable and economically feasible degree against unauthorized access and/or abuse, while at the same time making these resources accessible for authorized and legitimate users. Any activity which attempts to circumvent, defeat, disable, manipulate, or compromise such security is prohibited.

The right to use UAB computer and network resources may be revoked if misused or abused, even if unintentionally. Any attempt to violate the provisions of this policy may result in disciplinary action in the form of revocation of user accounts, revocation of access to the network, and/or progressive disciplinary actions, regardless of the success or failure of the attempt. Severe or continued violations will be reported to UAB authorities. Permanent revocation of access may be part of the disciplinary actions taken by those authorities. Actions which are in violation of applicable laws and statutes will be referred to appropriate law enforcement agencies and authorities.

This policy is applicable to all computing or networked devices present on UAB premises, regardless of whether they are UAB or private property. This policy also is applicable to all computing or networked devices which are UAB property, whether or not physically present in, or connected through, UAB facilities. This policy also is applicable to all devices connected through UAB's network infrastructure including, but not limited to, wired data ports, campus wireless access points, virtual private networks (VPN's), dial-up modems, and any other physical or virtual communication medium in which the device transmits or receives data via a UAB computer or network. This policy is applicable to all computing or networked devices regardless of their typical designation (or not) as a "computer" including, but not limited to, servers; desktop personal computers; workstations; laptops; printers; kiosks; personal digital assistants (PDA's); cellular telephones using data services; and network-capable cameras, game-playing units, appliances, digital



video recorders, and multimedia storage.

This policy is meant to supplement, not replace, existing UAB policies and guidelines including, but not limited to, the following:

- [Computer Software Policy](#)
- [Computer Software Copying and Use Policy](#)
- [Data Protection and Security Policy](#)
- [Information Disclosure and Confidentiality Policy](#)
- [Policy for Connecting Devices to the UAB Voice, Data, and Video Network](#)
- [Cellular Telephones Policy](#)
- [World Wide Web Pages Policy](#)
- [Best Practices for Local Area Network Administrators](#)
- [Policies in the *You and UAB Handbook for Administrative, Professional, and Support Personnel*](#)
- [Policies in student handbooks and catalogs](#)
- [Policies in the *Faculty Handbook and Policies*](#)
- [University of Alabama Board of Trustees Rules](#)

UAB will publish this policy on its World Wide Web (WWW) site and will provide periodic reminders to users of the expected standards of conduct and the disciplinary actions for not adhering to them. In addition, this policy and its implementation may be included as a WWW hyperlink in online forms in which authorization to use UAB computer and network resources is requested.

EXAMPLES OF POLICY VIOLATIONS

While it is impossible to anticipate every possible violation, examples are provided below to assist in defining what is considered to be responsible and ethical behavior. This list is not intended to be exhaustive; in general, any activity which does not directly contribute to UAB's mission may be considered inappropriate use.

Commercial activities, advertising, or any other "for-profit" ventures not specifically approved by the UAB administration.



University of Alabama at Birmingham
Office of Information Technology

Sustained promotion of any non-UAB activity or venture, profit or non-profit, public or private, personal or commercial, without approval of the UAB administration.

Creating, displaying, or transmitting threatening, racist, sexist, or harassing language and/or materials.

Creating, displaying, transmitting, or obtaining obscene or pornographic materials or any form of content which violates state and/or federal statutes and/or local standards of decency.

Copyright and licensing violations including, but not limited to, providing or obtaining illegal copies of software or digital media (movies, videos, music, etc.) for which legal permission to distribute or possess has not been granted.

Vandalism or mischief intended to incapacitate, compromise, or destroy UAB or other facilities, resources, or services.

Forgery or attempted forgery of electronic mail or posts to electronic forums or any other act of deceptive labeling of the originator of an electronic communication.

Obtaining goods, services, or funds of any form via electronic means by using the name and/or credentials of another person or entity without their consent and knowledge.

Deliberately sending un-welcomed or off-topic messages to an individual or discussion forum. This includes continuing to send such messages after being asked by the individual or forum's owner/moderator to stop doing so even though the originator does not consider the material offensive or inappropriate.

Transmitting unreasonable quantities of data or messages to persons or groups without their consent or request.

Spamming or transmitting unsolicited material to a large number of individual persons and/or discussion lists, newsgroups, or other forums even though the material itself may not otherwise violate these guidelines.

Being a continued impediment to other users through mass consumption of computing or network resources after receipt of a request to cease such activity, even if the activity is not otherwise disallowed.

Transmitting without permission private information such as grades, medical records, financial data, or any other information that is protected by the Public

Records Law or by legislation such as HIPAA, FERPA, etc.



University of Alabama at Birmingham
Office of Information Technology

Attempts to compromise computer and/or network security measures or providing information/instructions for how to do so.

Unauthorized, deliberate action which damages or disrupts a computing system or network, alters its normal performance, or causes it to malfunction. This includes intentional attempts to "crash" network systems or programs.

Attempts to gain unauthorized access to other systems on the UAB campus or the Internet.

Sharing of secure access credentials, such as passwords or private keys.

Attempts to guess, capture, "hack", or decrypt the secure access credentials of other users.

Attempts to possess, decrypt, or distribute data to which access has not been authorized.

Attempts to elevate system privileges or access without consent.

Unauthorized access of internal or external services through the use of stolen, guessed, hacked, copied, or discovered secure access credentials or other private data obtained without consent.

The willful or negligent introduction of computer "viruses" or other disruptive/destructive programs into the UAB network or into external networks.