>

University of North Alabama Information Technologies Acceptable Use Statement

INTRODUCTION

This acceptable use statement governs the use of computers, networks, and other information technologies at the University of North Alabama. This statement applies to all students and employees of the University, and to all other persons who may legally or illegally use or attempt to use a computer resource owned by the University, and/or is connected by any means to the campus computing network. As a user of these resources, you are responsible for reading and understanding this document.

Information technologies at the University of North Alabama are to be used in a manner that supports the educational mission of the University, and is conducive to the overall academic climate. Information technologies at the University of North Alabama refers to all computers owned or operated by the University and includes hardware, software, data, and communication networks, modems, phone lines, etc. associated with these systems. The systems range from multi-user systems to single-user terminals, personal computers and mobile devices, whether free-standing or connected to networks.

ACCESS PRIVILEGES

Access to hardware, software and networks is provided to members of the University for the primary purpose of enhancing the academic experience. Members of the University community may apply for the right to use computer resources through authorized computer accounts. To be granted the use of a computer account, users must agree to abide by certain rules and regulations related to appropriate, legal and ethical use of University computing systems.

Users do not own accounts on University computers, but are granted the privilege of their use. Information technology resources are the property of the University. Rules prohibiting misuse, theft, or vandalism apply to all software, data, and physical equipment. This includes University

owned data, as well as data stored by individuals on University computing resources. All existing laws (federal and state) and university regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct and state owned property.

UNACCEPTABLE USE

Misuse of computing, network or information resources can result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users will be held accountable for their conduct under any applicable university policies or procedures, or state or federal laws and regulations.

EXAMPLES OF UNACCEPTABLE USE

Conduct which involves the misuse of computer facilities and data networks, includes but is not limited to, the following:

- Violating university security or damaging university systems
- Attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses and worms.
- Attempted use, or possession in one's university account, of programs intended to crash the system, fraudulently imitate system responses, "sniff" secure or encrypted information, or gain unauthorized access to privileges, accounts, data, software, computers, or networks.
- Deliberately wasting/overloading computing resources, such as printing too many copies of a document.
- Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or regulations.
- Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be viewed by others.
- Violating copyright and software agreements, including but not limited to, copying university owned or licensed software or data to another computer system.

- Attempting to make unauthorized modifications to university owned or licensed software or data.
- Storing excessively large files or amounts of data on university owned computer systems. The University reserves the right to periodically purge excessively large files.
- Installing or running any software that the University has not granted you express permission to install or run.
- Knowingly accepting or using software or data obtained by illegal means or by methods violating university policy.
- Accessing data belonging to another individual or university department, even if access was inadvertently given to such information. For example, if a person fails to logoff the computer system and another individual comes along and uses the account that was accidentally left open, this statement has been violated by the second person. In this situation, the person finding the open account should report it so the account can be safely logged out.
- Failure to remove files, including e-mail, from university owned systems in a prompt and timely fashion. The University reserves the right to periodically purge files and e-mail which have not been removed in a timely manner.
- Misrepresenting your identity or affiliation, or the falsification of information.
- Disrupting or monitoring the activity or communications of other users. This includes, but is not limited to, electronic "stalking" and harassment of others, sending electronic chain letters, or using information technology resources for unauthorized commercial or profit-making purposes.
- Allowing another person the use of your computer password(s). Computer accounts are to be used only by the person to whom they are issued. The individual to whom an account is issued will be held responsible for all activity on that account.
- Using computers and/or network facilities in ways that impede the computing activities of others. For example, in a student laboratory, an individual who attempts to use several computing stations at the same time is preventing other students from reasonable use of the computing lab. This also includes using computers for games or recreational use while other students require access for course assignments.
- Defacing or removing hardware, software, manuals, supplies, etc. from computing sites.
- Disobeying lab and system policies, procedures, and protocol (e.g., time limits on workstation usage).
- Destroying or damaging equipment, software, or data that belongs to the University or to other users.

DISCIPLINARY ACTIONS

Access to the information technology resources at the University of North Alabama is a privilege and must be treated as such by all users of these systems. Like any other campus facility, abuse of these privileges can be a matter of legal action or official campus disciplinary procedures.

Minor infractions of this statement, when accidental, are generally resolved informally by electronic mail, or in-person discussion and education. Repeated minor infractions, or misconduct which is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources; attempts to steal passwords, data, or hardware; unauthorized use or copying of licensed software; repeated harassment; or threatening behavior.

Any offense that violates local, state or federal laws will result in the immediate loss of all university computing privileges and will be referred to appropriate university officials and/or law enforcement authorities.

SECURITY

Except for personally owned computers, the University owns, or has responsibility for, all of the computers and the internal computer networks used on campus. The University also has various rights to the software and information residing on, developed on, or licensed for these computers or networks. The University has the responsibility to administer, protect, and monitor this aggregation of computers, software, and networks.

The University reserves the right to require users to refrain from using any program. All users must also note that computer activity will be monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of computer usage the contents of user files, including electronic mail, may also be inspected. The University has the right to use information gained in this way in disciplinary or criminal proceedings. Users are expected to cooperate with investigations either of technical problems or possible unauthorized or irresponsible use as defined in these guidelines; failure to do so may be grounds for suspension or termination of access privileges. It should be noted that the University accepts no responsibility for damage to personal data or hardware caused by any university computer system. This includes, but is not limited to, malfunctions of hardware and software, computer viruses, Trojan Horses, and worms.

ACCESS ELIGIBILITY

Information technology resources, including laboratories and computer account privileges, are available to students, staff and faculty at the University of North Alabama. Staff and faculty should contact the Coordinator of Academic Technology for information or application materials. Access will normally be granted for the length of the individual's employment with the University.

As a general rule, student accounts remain active as long as the student is enrolled in the University. Questions should be addressed to UNA's Information Technology Services department at infosec@una.edu.

Failure to abide by this statement may result in temporary or permanent denial of access to information technologies.

Questions regarding this statement should be addressed to:

UNA Information Technology Services
Box 5061
University of North Alabama
Florence, AL 35632-0001
(256) 765-4865