

Auburn University at Montgomery

Policies and Procedures

Title: Information Technology Appropriate Use Policy

Responsible Office: Office of Technology

I. PURPOSE

Any individual or group granted permission to use Auburn University at Montgomery (AUM) Information Technology (IT) resources is responsible for using those resources in an appropriate manner, consistent with the mission of the University, and in compliance with Federal, State, and local statutes and AUM policies.

II. POLICY

AUM grants permission to use IT resources to support the University's mission of instruction, research, and outreach and the administrative functions of the University. Therefore, it is critical to protect the interests of the University and the user by attending to legal, contractual, security, and policy requirements and to insist the use of the resources is consistent with the goals of the University.

In addition, because AUM IT resources are shared resources, all users are expected to use these resources in a manner that does not abridge the rights or requirements of others.

AUM reserves the right to regulate individual resource usage to promote optimum system wide performance, optimum performance for critical and priority functions and to enforce system and data security.

College, school, or departmental policies and guidelines that further define the use of IT resources and services must not conflict with this policy.

III. EFFECTIVE DATE

June 2001

REVISED DATE

December 1, 2017

IV. APPLICABILITY

This policy applies to all devices connected to the AUM network and to all AUM users who use IT resources.

V. RESPONSIBILITY

The Office of Technology implements and administers the policy/procedure in detail.

Policy Responsible Office: Office of Technology

Policy Responsible Executive: Chief Information Officer (CIO)

VI. DEFINITIONS

User refers to any person using any of AUM's IT resources or facilities, including, but not limited to:

- Faculty
- Staff
- Students
- Clinical and adjunct title holders
- Associates, honoraries, and visiting staff
- Alumni
- Consultants
- Third parties (e.g., vendors, contractors, etc.)
- Other users authorized by the University to access its systems and/or network
- Anyone connecting non-AUM owned equipment (e.g., laptop computers) to the University network

AUM IT resources refers to any AUM resources or facilities operated by the University – whether owned, leased, used under license or by agreement – including, but not limited to:

- Telephones (including mobile devices) and telephone equipment, voice mail, SMS
- Mobile data devices
- Desktop, laptop, and tablet computers
- Email, chat, facsimiles, mail
- Any connection to the University's network, or use of any part of the University's network to access other networks
- Connections to the Internet that are intended to fulfill information processing and communications functions
- Communication services
- Hardware, including printers, scanners, facsimile machines
- Laboratories or other facilities
- Any off-campus computers and associated peripherals and equipment used for the purpose of University work or associated activities

VII. PROCEDURES

Appropriate Use:

Appropriate use of AUM IT resources is guided by the same principles as appropriate behavior in other realms, namely responsibility, respect for others, and professional action. Users to whom this policy applies are expected to assess the appropriateness of their use by reference to these principles. It is not possible to specify a rule for every possible use or misuse of IT resources, but some examples of appropriate use include:

- **Responsibility:**
 - Careful management and protection of your username and password; do not allow others to use your AUM account;
 - Accountability for all activity conducted under your username;

- Recognition that your access to AUM IT resources is for your individual activities that support the University's mission, not for commercial purposes or personal gain;
- Observation of standard security practices.
- **Respect for others:**
 - Protection of other users' privacy;
 - Recognition that AUM IT resources are shared resources;
 - Avoidance of activities that could degrade or disrupt others' usage of IT resources;
 - Care to obtain explicit permission before accessing or using files or data that belong to another user;
 - Special care to avoid activity that is or could be perceived as demeaning, harassing, or threatening.
- **Professional action:**
 - Compliance with State and Federal laws and AUM policy—this includes such laws as HIPAA, FERPA, Gramm Leach Bliley Act, US copyright laws, and policies regarding the protection of data;
 - Accurate presentation of your identity in electronic communications and other network traffic;
 - Use of IT resources to support the University's mission;
 - Maintenance of current security updates and software patches on devices for which you are responsible.

AUM reserves the right to monitor and regulate individual resource usage to promote optimum system-wide performance and/or optimum performance for critical or priority functions. Users should note that there should be no expectation of privacy in electronic files stored on the resident memory of a computer available for general public access, and such files are subject to unannounced deletion.

Unacceptable Use:

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing AUM-owned resources.

The list below is by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AUM.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AUM or the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an AUM IT resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any AUM account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to AUM is made.
- Circumventing user authentication or security of any host, network or account.
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.

VIII. SANCTIONS

Violations of this policy may result in actions ranging from warnings to loss of access to AUM IT resources.

Deliberate disregard of this policy or the protection standards created to implement this policy will be considered a Group I infraction under the University Personnel Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

NONE.

X. INTERPRETATION

The Office of Technology CIO has the authority to interpret this policy.

APPROVAL TO PROCEED: 

DATE: 12-1-17

APPENDICES

NONE.