

Appropriate Use of Information Technology Policy

I. POLICY STATEMENT

Any individual or group granted permission to use Auburn University 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 Auburn University policies.

II. POLICY PRINCIPLES

Auburn University 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 in a manner consistent with the goals of the university.

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

Auburn University 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

October 21, 2016

Revised October 26, 2018

IV. APPLICABILITY

This policy applies to all devices connected to the Auburn University network and to all persons using Auburn University IT resources.

V. POLICY MANAGEMENT

Responsible Office: Office of the CIO

Responsible Executive: Chief Information Officer (CIO)

Responsible Officer: Chief Information Security Officer

VI. DEFINITIONS

None.

VII. POLICY PROCEDURES

Appropriate use of Auburn University IT resources is guided by the same principles as appropriate behavior in other realms, namely responsibility, respect for others, and professional action.

Auburn University Information Technology Resources shall not be used for the creation or distribution of messages that violate the University's [Policy Regarding Prohibited Harassment of Student](#), [Policy Regarding Prohibited Harassment of Employees](#) and [Policy on Sexual and Gender-Based Misconduct](#).

Violations of these policies should be reported to the Office of AA/EEO & Title IX. An online complaint form can be completed here: [Discrimination or Harassment Complaint Form](#).

<http://auburn.edu/administration/aaeeo/Policies.php>

While it is not possible to specify a rule for every possible use or misuse of IT resources, persons to whom this policy applies are expected to act in accordance with the following examples:

Responsibility:

- Careful management and protection of your username and password; do not allow others to use your Auburn account;
- Accountability for all activity conducted under your username;
- Recognition that your access to Auburn University 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 Auburn University 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 intimidating, harassing or threatening.

Professional action:

- Compliance with State and Federal laws and Auburn University policy—this includes such laws as HIPAA, FERPA, Gramm Leach Bliley Act, DMCA (Digital Millennium Copyright 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.

Auburn University network connections may be monitored in accordance with the Auburn University Electronic Privacy Policy.

VIII. SANCTIONS

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

Failure or refusal to comply with this policy may result in discipline up to and including dismissal.

IX. EXCLUSIONS

None.

X. INTERPRETATION

The Auburn University Chief Information Officer has the authority to interpret this policy.