University Policy 5.1: Responsible Use of University Computing and Electronic Communications Resources

I. Purpose

The computing and electronic communication resources that Alabama A&M University provides for faculty, staff, and students are essential to carrying out the University's primary mission of education, service, and research. Protecting and preserving University computing and electronic communication resources is a cooperative effort that requires each member of the University community to act responsibly and guard against abuses. Any other uses that jeopardize the integrity of the University Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited. The use of any University electronic communication systems or the University network is a revocable privilege.

The University Network incorporates all electronic communication systems and equipment at Alabama A&M University (the "University"). This policy sets forth the standards by which all Users may use the shared University Network. Electronic communication systems and equipment refers to all computers owned or operated by the University and includes hardware, software, data, and communication networks, printers, network-attached devices, and any other peripherals associated with these systems.

This policy applies to all users of Alabama A&M University computing and electronic communication resources, including faculty, staff, students, guests, individuals not otherwise affiliated with the University, and external organizations and individuals accessing external network services, such as the Internet, through University facilities. By using or accessing the University Network, Users agree to comply with this policy and other applicable University policies and procedures which may be implemented from time to time, as well as all federal, state, and local laws and regulations. Only authorized Users are permitted to use and/or access the University Network.

II. Rights and Responsibilities

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So too, however, do the responsibilities and limitations associated with those rights. The university supports a campus and computing environment open to the free expression of ideas, including unpopular points of view. However, the use of university computing resources, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible.

III. Standards of Responsible Use

Users of university computing resources must comply with federal and state laws, university rules, policies and procedures, and the terms of applicable contracts including software licenses while using university computing resources. Examples of applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark , obscenity and child pornography; the Alabama Computer Crime Act, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities; the university's Student Code of Conduct; the university's Sexual Harassment Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and resolutions may apply to

a particular use of university computing resources should contact the Office of the General Counsel for more information.

Use of University computing and electronic communication resources is conditioned upon the obligation of each user to adhere to the following standards of responsible use:

1. Each User is required to behave responsibly with respect to the University Network and other Users at all times.
2. Each User is required to respect the integrity and the security of the University Network.
3. Each User is required to behave in a manner consistent with University's mission and comply with all applicable laws, regulations, and University policies and procedures.
4. Each User is required to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the University Network and show restraint in the consumption of shared resources.
5. Each User is required to respect the rights and property of others, including privacy, confidentiality and intellectual property.
6. Each User is required to cooperate with the University to investigate potential unauthorized and/or illegal use of the University Network.
7. Each User is required to respect the security and integrity of university computer systems and data.
8. Privately-owned computer systems or those owned by collaborative research projects, when attached to, or connected via, the campus data network and/or other campus resources are subject to the same responsibilities and regulations as pertain to University-owned systems. University account holders who use computers belonging to others to connect to the campus network either directly or via Virtual Private Network (VPN) must assure that the computers are in compliance with University regulations before making such connections.

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.

IV. Authorization

The University provides authorization to use University computing resources with the creation of a user ID and password. Students, faculty, and staff obtain a user ID when they commence enrollment or employment at the University. The user ID will provide access to basic computing services such as use of email, access to office automation software, the Internet, and access to systems and information that are provided based on the group the person belongs to or the position he or she holds at the University. Applicable departments or units will provide access to additional resources as appropriate.

V. Appropriate Uses

Examples of computer and network uses that are encouraged, with the appropriate authorization if necessary, include, but are not limited to, the following:

- Use of microcomputers in student labs for class assignments;
- Instructor preparation;
- Thesis and dissertation research support;

- Publishable research;
- Personal computing to improve computing literacy, or to learn new computer hardware and software;
- Use of public computers for review of generally available individual or campus information;
- Use of computers provided by the university to faculty and staff in support of their work;
- Approved use of the university's information and administrative systems; and
- Use of Internet resources to promote collegial interaction and research.

VI. Violation of Policy

Violations of responsible use of University computing and electronic communication resources include, but are not limited to the following:

1. **Prohibited Behavior:** Storing, transmitting or printing any of the following types of Electronic Communications on the Computer System is prohibited: material that infringes upon the rights of another person; material that is obscene; material that consists of any advertisements for commercial enterprises; material or behaviors that violate the Alabama A&M University Code of Student Conduct or other University Policies or Procedures; or material that may injure someone else and/or lead to a lawsuit or criminal charges.
2. **Identity Fraud:** Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate the University's name, network names, or network address spaces.
3. **Privacy Infringement:** Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.
4. **Hacking or Spamming:** Users may not use the University Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the University Network or any network that the University connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by the University, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information (i.e., non business-related information) on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others.
5. **Harassment:** Harassing others by sending annoying, abusive, profane, threatening, defamatory or offensive messages is prohibited. Users may not distribute or send unlawful communications of any kind, including but not limited to cyberstalking, cyberbullying, threats of violence, obscenity, child pornography, or other illegal communications (as defined by law). This provision applies to any electronic communication distributed or sent within the University Network or to other networks while using the University Network.
6. **Use of Pornography:** Intentional access to or dissemination of pornography by University employees, temporary staff, contractors, or vendors is prohibited unless (1) such use is specific to work-related functions and has been approved by the respective manager or (2) such use is specifically related to an academic discipline or grant/research project. This provision applies to any

electronic communication distributed or sent within the University Network or to other networks while using the University Network.

7. **Network Security Infringement:** Users may not attempt to bypass network security mechanisms, including those present on the University Network, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of the University Network is also prohibited. For permission to perform network scans, user must receive prior approval by calling 372-HELP (4357) and submitting a ticket to the Information Security Office.
8. **Unauthorized use of data:** Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law. Information on the Digital Millennium Copyright Act can be found at: http://www.copyright.gov/legislation/dmca.pdf and the Copyright Act at: http://www.copyright.gov/title17/.
9. **Non University Business/Commercial Use:** Users may not use the University Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-University organizations, unlawful activities, or uses that violate other University policies.
10. **Illegal access or connecting to the University Network:** Users may not extend or share with public or other users the University Network beyond what has been configured accordingly by Information Technology Services. Users are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the University Network without advance notice to and consultation with Information Technology Services.
11. **Destruction, Sabotage:** Intentionally destroying anything stored on the Computer System. Deliberately performing any act that will seriously impact the operation of the Computer System. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer or peripheral.
12. **E-Mail Forgery:** Forging e-Mail, including concealment of the sender's identity, is prohibited.
13. **Program/Software Theft:** Unless specifically authorized, copying computer program(s) from the Computer System or from University purchased media for personal use is prohibited.
14. **Violation of Laws or Ordinances:** Users may not violate any laws or ordinances, including, but not limited to, laws related to copyright, discrimination, harassment, threats of violence and/or export controls.
15. **Recreational Use:** Recreational use of the Computer System that interferes with the ability of other users to complete their work is prohibited. In particular, if you are using a machine in a Public Computer Lab for recreational purposes, and others are waiting to use a machine for academic purposes, you are expected to give up your seat.

VII. Review and Penalties

A. Users should have no expectation of privacy as to any communication on or information stored on the University network or University computers. The University reserves the right to review and/or monitor any transmissions sent or received through the University Network (including e-Mail and voicemail). This includes access without notice, where warranted. Non-intrusive monitoring of campus network traffic occurs routinely, to assure acceptable performance and to identify and

resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified. Access to other transmissions sent or received through the University Network may occur in the following circumstances:

1. In accordance with generally accepted, network-administration practices;
2. To prevent or investigate any actual or potential information security incidents and system misuse, if deemed necessary by authorized personnel;
3. To investigate reports of violation of University policy or local, state, or federal law;
4. To comply with legal requests for information (such as subpoenas and public records requests); and
5. To retrieve information in emergency circumstances where there is a threat to health, safety, or University property involved

B. Penalties for violating this policy may include:

1. Restricted access or loss of access to the University Network;
2. Disciplinary actions against personnel and students associated with the University,
3. Termination and/or expulsion from the University, and
4. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

The University, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

VIII. Policy Updates

The University reserves the right to update or revise this policy or implement additional policies or procedures in the future. Users are responsible for staying informed about University policies and procedures regarding the use of computer and network resources and complying with all applicable policies. Changes required by university contractual commitments shall be effective and binding to users upon execution of any such contract by the university. A user shall be deemed to have accepted and be bound by any change in University policies, information, requirements or procedures if such user uses computer or network resources at any time following announcement or publication of such change. The current version of this policy can be found at http://www.aamu.edu/administrativeoffices/information-technology/ITpolicies/Pages/default.aspx

IX. Compliance

Failure to comply with this Policy and/or regulations promulgated hereunder will be deemed a violation of University Policy and subject to disciplinary action in accordance with the disciplinary guidelines as outlined in the Faculty or Staff Handbook, whichever one is applicable to the individual.

Revision History

- Initially approved: December 2011 (Procedure)
- Policy Approved December 2012 (Board Approval)

Authority: President

Responsible Office: Information Technology Services