University of Alabama at Birmingham

ACCEPTABLE USE POLICY

July 1, 2017 (Target)

Related Policies, Procedures, and Resources

1.0 Introduction

The computing resources at the University of Alabama at Birmingham (UAB) support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the UAB community. As a consumer of these services and facilities, users have access to valuable University computing resources, to restricted and sensitive data, and to internal and external networks. Consequently, it is important for users to conduct themselves in a responsible, ethical, and legal manner.

2.0 Scope and Applicability of Policy

This policy applies to all users of UAB's computing resources and is intended to prohibit certain unacceptable uses of computers, mobile devices, and network resources and facilities, while also educating users about their individual responsibilities.

3.0 Policy Statement

3.1 No one shall use any University computer or network resource without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the University computing, network, and information technology resources.

3.2 No one shall knowingly endanger the security of any University computing, network, and information technology resources, nor willfully interfere with others' authorized computer usage.

3.3 No one shall use the University's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computing, network, and information technology resources anywhere.

3.4 No one shall connect any computer to any of the University's networks unless it meets technical and security standards set by the University administration.

3.5 All users shall share University computing resources in accordance with policies set by the University for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.

3.6 No one without specific authorization shall use any University computing, network, and information technology resources for non-University business.

3.7 No one shall give any password for any University computing, network, and information technology resources to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one, except the system administrator in charge of a computer, is authorized to issue passwords for that computer.

3.8 No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computing, network, and information technology resources privileges.

Proposed

3.9 No user will leverage unauthorized access to read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.

3.10 No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements, including, but not limited to, downloading and/or distribution of music, movies, or any other electronic media protected by said license agreements, copyrights, or other forms of legal protection.

3.11 No one shall create, install, or knowingly distribute malware, spyware, or other surreptitiously destructive or malicious programs on any University computer or network facility, regardless of whether any demonstrable harm results. Examples of such malicious software include, but are not limited to, computer viruses, Trojans, worms, key loggers, programs that provide unauthorized remote access, and ransomware.

3.12 Only authorized parties shall modify or reconfigure any University computing, network, and information technology resources.

3.13 No one shall store Restricted/PHI or Sensitive information in computers, portable devices or transmit Restricted/PHI or Sensitive information over University networks without protecting the information appropriately.

3.14 Users shall take full responsibility for data that they store in University computers, portable devices and transmit through network facilities. No one shall use University computers or network facilities to store or transmit data in ways that are prohibited by law or University policy, standards, and rules. Users shall not transmit any communications that are harassing or discriminatory as outlined in the UAB Equal Opportunity and Discriminatory Harassment Policy.

3.15 Those who publish web pages or similar information resources on behalf of the University shall take full responsibility for what they publish. Said parties shall respect the acceptable use conditions for the computer on which the material resides, and they shall obey all applicable laws and University policies, standards, and rules. They shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not allowed. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar information resources.

3.16 Users of University computers shall comply with the regulations and policies of mailing lists, social media sites, and other public forums through which they disseminate messages.

3.17 System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate University administration, University policies, and funding sources. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters and legal matters to appropriate authorities.

3.18 UAB email and other electronic messaging technologies are intended for communication between individuals and clearly identified groups of interested individuals, not for mass broadcasting. No one shall use University facilities to distribute spam messages without prior authorization. Such messages are defined as the same or substantially the same e-mail message sent to more than one person without prior evidence that they wish to receive it.

The University reserves the right to discard incoming mass mailings and spam without notifying the sender or intended recipient.

Proposed

3.19 For its own protection, the University reserves the right to block communications from sites or systems that are involved in extensive spamming or other disruptive practices, even though this may leave University computer users unable to communicate with those sites or systems.

3.20 Users are required to report suspected or actual security violations, compromises, or attacks (including phishing attempts) immediately to the UAB Information Security Office. Likewise, users are required to report suspected or actual suspicious or criminal activity immediately to the University Police Department. More information on incident reporting.

4.0 Exception

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs. To request a security exception, complete the Information Security Exception Request Form.

5.0 Non-Compliance

Confirmed violations of this policy will result in appropriate consequences with the offense, up to and including termination of employment, appointment, or other relationships with UAB.

6.0 Maintenance

This policy will be reviewed by UAB's Information Security Office periodically, or as deemed appropriate.

7.0 Implementation

The Vice President for Information Technology is responsible for the oversight and implementation of this policy, including the overall procedures related to its implementation and management.

Proposed