THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

APPROPRIATE USE OF IT RESOURCES

Number 06.01.03

Division Finance and Administration - Office of Information Technology (OIT)

Date June 2018

Purpose The purpose of this policy is to establish required and prohibited activities to ensure the security and integrity of UAH IT resources.

Policy The University of Alabama in Huntsville (UAH) is committed to providing a wide range of high quality information technology (IT) services to students, faculty, and staff, in support of the mission of the university. However, access to IT resources is a privilege, not a right, and all users must act honestly and responsibly.

This policy establishes the required and prohibited activities to ensure the security and integrity of the university's IT resources as well as fair and equitable access to those resources by all the members of the university community. This policy applies to all IT usage by faculty, staff, students, researchers, or other users of IT resources that connect to UAH networks, and/or store or transmit UAH data.

Procedure

1.0 Required Activities

All users of UAH IT resources as described above must:

- Be accountable for using IT resources in an ethical and lawful manner, abiding by local, state, and federal law, as well as all applicable university policies.
- Report suspicious activities or any discoveries of excessive access rights.
- Use only IT resources that access has been authorized.
- Maintain individual responsibility for the safekeeping of assigned access codes, account identifiers, and passwords, and refrain from sharing these with any other party or other individuals.
- Properly identify oneself in any electronic correspondence and provide valid, traceable identification if required by applications

or servers within the UAH IT resources or in establishing connections from the UAH IT resources.
- Use IT resources in a manner consistent with the “Security of IT Resources” policy.

2.0 Prohibited Activities

All users of UAH IT resources as described above must refrain from:

- Excessive and/or disruptive use of IT resources including, but not limited to, creating excessive wired or wireless network traffic, system resource usage, or any activity that diminishes the quality of IT resources for others.
- Activities that negatively impact the performance or security of the UAH network.
- Network mapping, port scanning, vulnerability scanning, or any other security testing of systems or networks which the user does not own or administer, without prior written approval from UAH Chief Information Security Officer (CISO). Networks or systems that do not connect to the UAH network and are setup for these types of activities are exempt from needing approval.
- Sharing of university accounts or passwords.
- Accessing any UAH e-mail, files, data, or transmissions owned by others without authorization.
- Extending UAH data network either through wired or wireless means without approval from UAH CISO.
- Using UAH IT resources to conduct commercial activities, other than those authorized by the Academic Affairs Office or Office of the Vice President of Research and Economic Development.
- Any actions deemed illegal by local, state, or federal law, shall not be permitted on UAH IT resources. Such acts include, but are not limited to:
    - accessing, destroying of, or altering data owned by others
    - modification of computer system configuration
    - installation of unauthorized software
    - interference with access to computing facilities or harassment of users of such facilities at UAH or harassment of users of such facilities elsewhere
    - unauthorized disruption of UAH IT resources
    - attempts to discover or alter passwords or to subvert security systems in any IT resource

3.0 Administration and Compliance

OIT personnel may take immediate action to abate identified issues impacting network or system operations.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, the Staff Handbook, or University policy, will be referred to appropriate university authorities.

Review The IT Investment Advisory Council is responsible for the review of this policy every five years (or whenever circumstances require).