

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

APPROPRIATE USE OF IT RESOURCES

-INTERIM-

Number 02.01.48

Division Office of Information Technology (OIT)

Date August 2015

Purpose The purpose of this policy is to establish proper user practices 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 rules and practices 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 faculty, staff, students, researchers, or other users of IT resources that connect to UAH networks, and/or store or transmit UAH data, regardless of the device used to access UAH IT resources or ownership of the device.

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.
- Use only those resources for which the IT resource owner has authorized use, whether resources are at UAH or at any other location accessible through a network.
- 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.
- Maintain adequate security posture of devices connecting to UAH IT resources as required in 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 which the user does not own or administer, without prior written approval from UAH Chief Information Security Officer (CISO).
- Sharing of university accounts or passwords.
- Accessing any 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 Office of Sponsored Programs, Academic Affairs Office, Office of the Vice President of Research and Economic Development or Professional and Continuing Studies.
- 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, destruction of, or alteration of 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

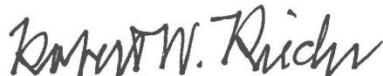
The connection of a device to the UAH network requires the registration of that IT resource with the Office of Information Technology. This registration occurs through either the use of the network client authentication or electronic form available at: <https://narf.uah.edu/>.

Failure to abide by this policy may result in the loss or suspension of IT privileges, claims for reimbursement of damages, disciplinary action, and/or referral to appropriate state/federal law enforcement authorities.

Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, or the Staff Handbook, will be referred to appropriate university authorities. OIT personnel may take immediate action as needed to abate ongoing interference with system or network operations, or to ensure integrity of university systems or data.

Review The UAH Cybersecurity and Policy Advisory Council is responsible for the review of this policy every three years (or whenever circumstances require).

Approval

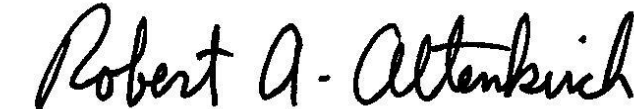


Chief University Counsel



Provost and Executive Vice President for Academic Affairs

APPROVED:



President