THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

SECURITY OF IT RESOURCES POLICY

Number	06.01.02
Division	Administration – Office of Information Technology
Date	April 2018; Reviewed and Revised February 3, 2025
Purpose	This policy defines acceptable use of information technology resources owned by The University of Alabama in Huntsville (“UAH” or “University”) including electronic accounts, devices, networks, applications, data, information systems, and all information composed, transmitted, accessed, received, or stored by these resources.
Policy	This policy establishes the requirements and constraints for securing UAH-owned information technology (IT) resources, and applies to all IT usage by faculty, staff, students, researchers, or other users of IT resources that connect to the UAH networks, and/or store or transmit UAH data.

1.0 User Responsibility for Securing UAH IT Resources

When securing UAH IT resources, the system criticality, data classification and support, encryption and regulatory requirements shall be considered. For more guidance on data classification, refer to the Protection of Data Policy.

UAH Information Security has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as the basis for the university-wide set of security standards and guidelines. All computing devices connecting to the UAH network are expected to comply with the minimum cybersecurity standards as set forth in published in the UAH OIT Knowledge Base.

This Security of IT Resources Policy requires different activities from individuals depending on their level of interaction with IT resources and respective roles within the university community. These roles and required activities are documented below

1.1 Requirements for All Users of UAH IT Resources

All users of UAH IT resources are required to comply with the following requirements:

- Protect and maintain confidentiality of user account credential information for all IT system resources. The University grants each account holder specific levels of access to technology resources required by an individual to fulfill their University-assigned roles and responsibilities. In all cases, an electronic account is for the exclusive use of the individual to whom it is assigned.

- Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the university's IT resources.
  - Keep university systems and data secure by choosing strong authenticators (such as passwords) and not sharing the authenticators or storing them in an unsecured manner.
  - Utilizing screen locks, requiring that require authenticators to unlock the system, while not physically at the system.
  - Contact OIT or their local support provider whenever a questionable situation arises regarding the security of any UAH IT resource.
  - Report all security events involving UAH IT resources following the process outlined in the "Incident Reporting and Breach Notification" policy.

1.2 Additional Required Activities for Users with Administrative Privileges to IT Resources

This includes users that administer IT resources that are used by themselves only and contain UAH data

- Update all software packages on the system, including antivirus, anti-malware and operating system, in a timely fashion.
- Unless not technically feasible, utilize the university-wide Trusted Identity Management System to provide user authentication.
- Protect the resources under control with the responsible use of secure passwords.
- Assist in the performance of remediation steps in the event of a detected vulnerability or compromise.
- Comply with industry best practices and UAH policy and procedures to reduce risk of system compromise or unauthorized data disclosure.

1.3 Additional Required Activities for Local Support Providers

This includes users that administer IT resources that are used by other users and contain UAH data

- Maintain and document a thorough understanding of the supported IT resources to be able to respond to emerging threats and to support security event mitigation efforts.
- Understand and recommend the appropriate measures to properly secure the supported IT resources, including, but not limited to the following:
  - Fully implementing OIT-standard university-wide Trusted Identity Management System for authentication unless not technically possible.
  - Using the most recently tested and approved software patches available.
  - Implementing the most effective current security configurations as directed by OIT.
  - Installing and enabling campus-supported endpoint and virus protection solutions.

  - Configuring secure password protection measures and eliminating default and/or well-known usernames, such as root or administrator, where feasible.
  - Being mindful of potential responsibilities such as being custodians of UAH data transmitted or stored on IT resources under their control.
  - Overseeing compliance with all IT security regulations under federal, state, and local law, UAH policies and procedures and OIT requirements.
  - Participating in and supporting security risk assessments of IT resources.
  - Assisting UAH OIT security personnel in investigations of security issues and incidents.
  - Working with the unit head, the unit IT manager, director and/or other relevant personnel to address critical security notices issued by UAH OIT security personnel.
  - Complying with and helping enforce university-wide cybersecurity requirements

1.4 Additional Required Activities for Third-Party Service Providers

This includes any vendor or service provider that will have access to UAH IT systems, networks, and/or data, or that otherwise provide an IT-related solution or service

- Conduct Vendor Assessments: Prior to engaging a third-party service provider, requesting units are required to work with OIT to perform a thorough assessment of the vendor's security practices and controls.
- Include Security-related Contractual Requirements. All contracts for IT-related services must include adequate contract provisions to ensure compliance with applicable federal and state data security laws and regulations, data security standards, and university policy. Contractual requirements to be addressed should include, but are not limited to:
  - Compliance with federal regulations (e.g., FERPA, HIPAA, GLBA, etc.)
  - Breach notification requirements as required under federal and/or state law
  - Compliance with relevant data security standards (e.g., PCI-DSS)
- Conduct Annual Contract / Vendor Reviews and Assessments. Each unit head is responsible for the annual review of, and updating as necessary, any contracts and agreements for IT-related services under that unit's control. Annual reviews must include the following minimum components:
  - Review of business need for service
  - Review of vendor security assessments, to include the most recent vendor disclosures

2.0 Requirements for Systems Allowing Remote Network Access from The Internet to Systems On The UAH Network

In addition to the requirements listed above, any UAH network-connected system that is accessible from outside of UAH's network shall be configured to provide a copy of the log events to OIT logging solutions.

These systems shall also have firewall restrictions, both host-based and network-based, that limit access to services necessary for required functionality. These restrictions shall be based on IP address, port, and/or protocol access requirements.

Access to UAH systems from the Internet requires the approval of and coordination with UAH OIT.

3.0 Virtual Private Networking (VPN)

Unless not technically feasible, access to UAH IT resources shall be restricted to on campus and VPN access only. Non-VPN outside access shall only be provided when VPN access is not feasible, and such non-VPN access requires the prior approval of and coordination with UAH OIT.

4.0 Vulnerability Scanning and IT Audits

Security of IT resources will be audited through vulnerability scanning, spot checks and security audits, authorized by UAH Chief Information Security Officer (CISO).

Where vulnerabilities are discovered, appropriate action will be taken to mitigate the issue in accordance with OIT-published vulnerability management procedures and requirements on the UAH Knowledge Base. This may require installing patches, applying mitigating controls, and/or removal from the network

5.0 Compliance with Policy

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

Violations that constitute a breach of the Code of Student Conduct, the Faculty Handbook, the Staff Handbook, University policy, or local, state, federal, or international laws will be referred to appropriate university and/or other authorities.

5.1 Exceptions to Policy

Exceptions to this policy may be requested by the appropriate unit head by providing a brief description of the IT resource, purpose, timeframe needed, and justification for the exception request. Documentation should be provided to UAH CIO, or designee, to approve the exception and maintain a record thereof. Exception requests must be renewed annually. If updated documentation is not submitted, or is found to be unsuitable, network access to the IT resource may be revoked

6.0 Actions to Protect UAH Assets

All computing devices connecting to the UAH network in any way or owned by UAH along with devices that store or transmit private, sensitive, or confidential data must meet a minimum set of security standards as published by OIT on the UAH Knowledge Base. To protect university data and systems, as well as to protect threatened systems external to the university, the University Chief Information Security Officer, Chief Information Officer, or University Chief Risk and Compliance Officer may place limits or restrictions on technology services provided on or from any university-owned or -managed system and network.

Limitations may be implemented through policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.

Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on university functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the University Chief Information Security Officer, Chief Risk and Compliance Officer, or Chief Information Officer.

To protect university data and systems, as well as to protect threatened systems external to the university, OIT Directors or the UAH Chief Information Security Officer may unilaterally choose to virtually isolate a specific university system from university, campus, or external networks, given:

- Advance consultation with the UAH Chief Information Officer or their designee, where practical and where circumstances warrant.
- Information in hand reasonably suggests that the system has been compromised or presents a security threat to other UAH assets.
- There is ongoing activity associated with the system that is causing or will cause damage to other university systems or data or to assets of other internal or external agencies, or there is a medium to high risk of such damage occurring.
- All reasonable attempts have been made to contact the responsible technicians or department management, or such contact has been made and the technician or department managers are unable to or choose not to resolve the problem in a reasonable time.

Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the Chief Information Officer or Chief Information Security Officer.

Review The UAH Chief Information Officer is responsible for the review of this policy every three years, or whenever circumstances require.