THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

SECURITY OF IT RESOURCES

Number 06.01.02

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

Date April 2018

Purpose The purpose of this policy is to define the requirements and constraints to ensure the security of UAH IT resources.

Policy This policy establishes the requirements and constraints for securing The University of Alabama in Huntsville (UAH) owned information technology (IT) resources. These resources include but are not limited to computers, servers, applications, or network devices. This policy serves to ensure that all university-owned IT resources are maintained at appropriate levels of security while at the same time not impeding the ability of users to perform assigned functions.

This policy 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.

Procedure

1.0 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." This 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 Required Activities for Basic Users Without Administrative Privileges to IT Resources

(Users that do not administer any IT resources that contain UAH data.)

- 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 passwords and not sharing the passwords.
- Utilizing screen locks, requiring passwords to unlock the system, while not physically at the system.
- Contact 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
(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.
- Where possible 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 to reduce risk of system compromise.

1.3 Additional Required Activities for Local Support Providers
(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:
    - Administrative security to protect resources such as:
        - Fully implementing standard central authentication and authorization technologies available through OIT.
        - Using the most recently tested and approved software patches available.
        - Implementing the most effective current security configurations.
        - Using campus supported virus protection.

        - Configuring secure passwords and elimination of default and/or well-known usernames, such as root or administrator, where feasible.
- Be mindful of potential responsibilities such as being custodians of sensitive data transmitted or stored on IT resources under their control.
- Oversee compliance with all IT security regulations under federal, state, and local law.
- Participate in and support security risk assessments of IT resources, including, but not limited to, the following:
    - The degree of sensitivity or importance of the data transmitted or stored on those resources.
    - The criticality of connection of resources to the network and a continuity plan in the event that resources must be disconnected or blocked for security reasons.
    - The vulnerability of a particular resource to be used for illegal or destructive acts.
    - The vulnerability of a particular resource to be compromised by an attacker.
    - The plan to be followed in the event of disaster for recovery.
    - The measures to be taken routinely to ensure security for each device.
- Assist UAH OIT security personnel in investigations of security issues and incidents.
- Work 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.

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 delivers a service 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, preferably host-based and network-based, that limit access to services necessary for required functionality. These restrictions shall be based on IP address and port access requirements.

3.0 Virtual Private Networking (VPN)

To increase security, whenever possible, 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.

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. This may require installing patches, applying mitigating settings, and/or removal from the network.

5.0 Compliance with Policy

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.

5.1 Exceptions to Policy

Exceptions to this policy may be made by providing approval from unit head, brief description of IT resource, purpose, timeframe needed, and justification for exception. Documentation should be provided to UAH CIO, or direct reports, to approve the exception and maintain record. If updated documentation is not submitted, or is found to be unsuitable, network access to the facility may be revoked.

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