THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

SECURITY OF IT RESOURCES

-INTERIM-

Number 02.01.49

Division Office of Information Technology (OIT)

Date August 2015

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 faculty, staff, students, researchers, or other users of IT resources that connect to the UAH networks, and/or store or transmit UAH data, regardless of ownership of the device or system, including personally owned devices or systems.

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 required activities are documented below.

1.1 Required Activities for Basic Users

- 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, and locking the systems while not physically at the terminal.
- 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

- Update all software packages on the system, including antivirus, anti-malware and operating system, in a timely fashion.
- 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

- 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:
  - Physical security to protect resources such as keys, doors, and/or rooms maintained to the level of security commensurate with the value of the resources stored in those locations
  - 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 Accessible from Outside the UAH Network

In addition to the requirements listed above, any 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

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

Robert W. Richr

Chief University Counsel

Christine W. Curtis

Provost and Executive Vice President for Academic Affairs

APPROVED:

Robert A. Altenkirch

President