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

Date June 2018

Purpose The purpose of this policy is to define the responsibilities of users for supporting and protecting electronic data at UAH.

Policy This policy establishes the responsibilities of all users to support, secure, and protect electronic data at The University of Alabama in Huntsville (UAH). UAH is responsible for properly securing its intellectual property, contracts, research and personally identifiable information. This policy evinces the responsibilities of all users in supporting and protecting the electronic data at UAH regardless of user's affiliation or relation with UAH, and irrespective of where the data are located, utilized, or accessed. All members of the UAH community have a responsibility to protect the confidentiality, integrity, and availability of electronic data.

This policy applies to all electronic data usage and storage by faculty, staff, students, researchers, or other users of information technology (IT) resources that connect to UAH networks, and/or store or transmit UAH data.

This policy is not applicable to electronic data in possession of students that is for a UAH class assignment and which is prepared by the student and maintained on the student's own device. Students should note that such data may be covered by other policies, however. Moreover, once submitted for a class assignment, such data shall be treated by the University faculty and staff under appropriate law, with their use governed by this policy.

All usage of the term data in this policy is in reference to electronic data.

Procedure

1.0 Responsible Units

UAH functional units operating or utilizing IT resources are responsible for managing and maintaining the security of the data, IT resources, and protected information. Functional units are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of data in compliance with this policy. This requirement is especially important for those IT resources that support or host critical business functions or protected information.

Protected information will not be disclosed except as provided by university oi a external users must be done in accordance with a Non-Disclosure Agreement (examples of private data include employment data).

Sensitive or Confidential data – Sensitive or Confidential data are data that by law are not to be publicly disclosed. This designation is used for highly sensitive information whose access is restricted to authorized employees. Student data restrictions are outlined in the UAH Student Records Policy (https://www.uah.edu/images/administrative/policies/03.01.01-VP_Student_Affairs_Student_Records_Policy.pdf).

The recipients of confidential data have an obligation not to reveal the contents to any individual unless that person has a valid need and authorized permission from the appropriate authority to access the data. The person revealing such confidential data must have specific authority to do so. Sensitive or confidential data must not be copied without authorization from the identified custodian (examples of confidential data include data that are regulated by federal regulations such as Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR)).

Research Data -

1.2 Storage of Data on Non-UAH Owned Systems

Data classified as private or confidential shall not be stored on non-UAH owned IT resources without approval of the data owner(s). IT resources storing this data shall be configured to secure the data properly. For further requirements see the “Security of IT Resources” policy.

1.3 Non-approved Locations for Data Storage

Storage systems that have not been approved by UAH Chief Information Security Officer (CISO), or direct reports, shall not be utilized to store data classified as private or turited tadee or U shar r06 Tc 0.006 Twt6

1.9 Approved Data Storage Facilities for Servers Storing Private or Sensitive or Confidential Data

OIT is responsible for operating IT facilities that maximize physical security, provide reasonable protections for IT systems from natural disasters, and minimize cybersecurity risks for UAH data and IT Resources.

OIT is also responsible for provisioning an evolving set of information technology infrastructure and services that meet the common, evolving needs of all units. This may include contracting for services via cloud and off-site service providers that offer desirable and secure common services of value to the UAH community.

All units of UAH will deploy and use IT an rable and sf246(an)10 (ev)14 (ol)6 (v)14

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).

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PROTECTION OF DATA

APPENDIX A:

Protection Requirements Based on Classification:

The tables below define minimum protection requirements for each category of data when being used or handled in a specific context. Please note that these protections are not intended to supersede any regulatory or contractual requirements for handling data.

Collection and Use	No protection requirements
Granting Access or Sharing	
Disclosure, Public Posting, etc.	

Private Data	
Collection and Use	Limited to authorized uses only. Units/Colleges that collect and/or use Sensitive Data should participate in the Information Security Program by reporting servers to the Office of Information Technology.
Granting Access or Sharing	Access shall be limited to authorized University officials or agents with a legitimate academic or business interest and a need to know as outlined by UAH policies. All access shall be approved by an appropriate data owner and tracked in a manner sufficient to be auditable. Before granting access to external third parties, contractual agreements which outline responsibilities for security of the data shall be approved through the UAH contract process.
Disclosure, Public Posting, etc.	Sensitive Data shall not be disclosed without consent of the data owner. Sensitive Data may not be posted publicly. Directory information can be disclosed without consent. However, per FERPA, individual students can opt out of directory information disclosure.
Electronic Display	Only to authorized and authenticated users of a system.
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	A contractual agreement (or MOU if governmental agency) outlining security responsibilities shall be in place and approved through the UAH contract process before exchanging data with the third party / service provider.
Storing or Processing: Server Environment	Servers that process and/or store sensitive institutional data must comply with Security of IT Resources policy, as well as applicable laws and standards.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	Systems that process and/or store sensitive institutional data must comply with Security of IT Resources policy, as well as applicable laws and standards. In addition, any/all systems that process or store Sensitive Data must require PIN and/or password for access to device.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	Sensitive Data shall only be stored on removable media in an encrypted file format or within an encrypted volume.
Electronic Transmission	Sensitive Data shall be transmitted in either an encrypted file format or over a secure protocol or connection.
Email and other electronic messaging	Messages shall only be sent to authorized individuals with a legitimate need to know.

	Sensitive Data may be shared through approved UAH services.
Printing, mailing, fax, etc.	Printed materials that include Sensitive Data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know.
	Access to any area where printed records with Sensitive Data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufo l4BTp9SefEMC /Arti3Tm[()4(e)-1(.)3(g)2

Providers, Cloud Services, etc.	approved through the UAB contract process before exchanging data with the third party / service provider.
Storing or Processing: Server Environment	at process and/or store sensitive institutional data must comply with Security of IT Resources policy, as well as applicable laws and standards.

Disposal	Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use -