THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PROTECTION OF DATA

Number 06.01.01

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 policy and procedures, or as required by law or court order.

1.1 Data Classification

It shall be the responsibility of the data owner to classify the data, with input from appropriate university administrative units and the Office of Counsel. However, all individuals accessing data are responsible for the protection of the data at the level determined by the data owner, or as mandated by law. Therefore, the data owner is responsible for communicating the level of classification to individuals granted access. Any data not yet classified by the data owner shall be deemed confidential. Access to data items may be further restricted by law, beyond the classification systems of UAH.

All electronic data of UAH shall be classified as public, private, sensitive or confidential, or research according to the following categories:

- **Public data** - Public data are defined as data that any person or entity either internal or external to the university can access. The disclosure, use, or destruction of public data should have no adverse effects on the university nor carry any liability (examples of public data include readily available news and information posted on the university's website).

- **Private data** - Private data are defined as any data that derive value from not being publicly disclosed. The value of private data to the university and/or the custodian of such data would be destroyed or diminished if such data were improperly disclosed to others. Private data may be copied and distributed within the university only to authorized users. Private data disclosed to authorized, 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** - Research data are defined as: "the recorded factual material commonly accepted in the scientific community as necessary to validate research findings." (OMB Circular 110). Research data cover a broad range of types of information and privacy will vary widely depending on compliance with the particular funding agency such as National Institutes of Health (NIH) or National Science Foundation (NSF).

  Although some protected information, private data, and confidential data the university maintains may ultimately be determined to be “public records” subject to public disclosure, such status as public records shall not determine how the university classifies and protects data until such a determination is made. Often public records are intermingled with confidential data and protected information, so that all the information and data should be protected as confidential until it is necessary to segregate any public records.

  All data determined to be public data by the data owner and released to the public is considered public data, not 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 confidential. This includes cloud-based services such as Dropbox. See the “Cloud Service and Information Technology Procurement” policy for approval process.

1.4 Data Access Restrictions

All data access must be authorized under the principle of least privilege, and based on minimal need. The application of this principle limits the damage that can result from accident, error, or unauthorized use. All permissions to access confidential data must be approved by the data owner or their designee, and written or electronic record of all permissions must be maintained. For private or sensitive or confidential data, the approving authority for the data shall audit data access at least annually.

During data access audits, data owners will be provided a list of users with access and their access rights. The data owner must respond with appropriate changes, updates, terminations or concurrence, within 20 business days. Failure to do so will result in notification to the vice president responsible for the data owner’s unit and the access rights being audited may be revoked. A written response to the data access audit is required, even if there are no changes to the access list and/or the rights detailed in the list.

Private or confidential data shall not be provided to external parties or users without approval from the data owner. In cases where the data owner is not available, approval may be obtained by the Director or Department Head of the unit in which the data are maintained, or by an official request from a senior executive officer of the university.

When an individual who has been granted access changes responsibilities, all of their access rights should be reevaluated and any access to protected data outside of the scope of their new position or status should be revoked.

1.5 Data Backup

Data that are critical to the mission of the university shall be located, or backed up, on centralized servers or other campus-wide approved backup solutions, unless otherwise authorized by the data owner of that data, or Chief Information Officer (CIO).

1.6 Data in Transit

Data that is transmitted without encryption has increased possibility of eaves dropping attacks, where an attacker may intercept the data being transmitted. Whenever possible, private and confidential data shall only be transferred through encrypted channels. This may include secure socket layer (SSL), secure shell (SSH), virtual private networks (VPN) or other encrypted sessions. Encryption is the process of converting the information into a form that is unintelligible except when converted back to original form utilizing a cryptographic key.

1.7 Data Encryption

IT Resources that store data classified as private or confidential shall utilize strong encryption mechanisms to maintain confidentiality of the data and greatly reduce the risk of theft or loss of IT Resources. Examples of strong encryption include RSA (2048 bits and higher), AES (128 bits and higher), ECC (224 bits and higher), TDES/TDEA (triple-length keys), DSA/D-H (2048/224 bits and higher). For more information about strong encryption, see NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/).

1.8 Destruction of Data

Once the data or IT resource is no longer needed or is being repurposed, the data shall be destroyed in a manner that guarantees that the data are not recoverable. Destruction can be done through wipe utilities or physical destruction of the storage device.

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 resources in ways that mitigate cybersecurity risks, providing physical security for IT systems, and minimize unacceptable risks to IT resources and data from natural disasters.

The primary means of reducing and mitigating cyber risks at UAH is for units to use the secure facilities, common information technology infrastructure, and services provided by OIT to the greatest extent practicable for achieving their work.

To the extent that the primary means of cyber risk mitigation is not practicable for achieving a unit’s work, the unit shall formally document their role, responsibilities, and ongoing mitigation of cyber risks to UAH. The OIT cybersecurity team can assist with documentation for units supported by OIT.

Documentation should include 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 maintain record. Documentation shall be updated at least annually. If updated documentation is not submitted, or is found to be unsuitable, network access to the facility may be revoked.

2.0 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.

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.

Public Data	
Collection and Use	No protection requirements
Granting Access or Sharing	No protection requirements
Disclosure, Public Posting, etc.	No protection requirements
Electronic Display	No protection requirements
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	No protection requirements
Storing or Processing: Server Environment	Servers that connect to the UAH network must comply with Security of IT Resources policy.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	Systems that connect to the UAH network must comply with Security of IT Resources policy.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	No protection requirements
Electronic Transmission	No protection requirements
Email and other electronic messaging	No protection requirements
Printing, mailing, fax, etc.	No protection requirements
Disposal	No protection requirements

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.) sufficient to prevent unauthorized entry. Do not leave printed materials that contain Sensitive Data visible and unattended.
Disposal	Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy.

Sensitive or Confidential 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. In addition, any/all servers that process or store Restricted Data must meet all requirements associated with applicable laws and/or standards.
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 UAB 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.	Not permitted unless required by law.
Electronic Display	Restricted data shall be displayed only to authorized and authenticated users of a system. Identifying numbers or account number shall be, at least partially, masked or redacted.
Exchanging with Third Parties, Service	A contractual agreement (or MOU if governmental agency) and/or Business Associate Agreement (BAA) outlining security responsibilities shall be in place and

Providers, Cloud Services, etc.	approved through the UAB 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 Credit/Debit card PAN data is not permitted.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	Any/all systems that process or store Sensitive or Confidential Data must be encrypted volume and endpoint must require PIN and/or password for access to device. Systems that process and/or store sensitive institutional data must comply with Security of IT Resources policy, as well as applicable laws and standards. Storing Sensitive of Confidential Data on personally-owned devices is not permitted. Devices storing or processing Sensitive or Confidential data must be physically secure at all times. Avoid storing Sensitive or Confidential Data on portable devices, where possible.
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, unless denied by law, grant or contract.
Electronic Transmission	Secure, authenticated connections or secure protocols shall be used for transmission of Sensitive or Confidential Data.
Email and other electronic messaging	Not permitted without express authorization or unless required by law. Messages with Sensitive or Confidential Data shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols. Sensitive or Confidential Data may be shared through approved UAH services.
Printing, mailing, fax, etc.	Printed materials that include Sensitive or Confidential 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 or Confidential Data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry. Do not leave printed materials that contain Sensitive or Confidential Data visible and unattended.

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

Research Data	
Collection and Use	Requirements commensurate with sensitivity and/or grant or contract requirements.
Granting Access or Sharing	Requirements commensurate with sensitivity and/or grant or contract requirements.
Disclosure, Public Posting, etc.	Requirements commensurate with sensitivity and/or grant or contract requirements.
Electronic Display	Requirements commensurate with sensitivity and/or grant or contract requirements.
Exchanging with Third Parties, Service Providers, Cloud Services, etc.	Requirements commensurate with sensitivity and/or grant or contract requirements.
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.
Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	Requirements commensurate with sensitivity and/or grant or contract requirements.
Electronic Transmission	Requirements commensurate with sensitivity and/or grant or contract requirements.
Email and other electronic messaging	Requirements commensurate with sensitivity and/or grant or contract requirements.
Printing, mailing, fax, etc.	Requirements commensurate with sensitivity and/or grant or contract requirements.
Disposal	Requirements commensurate with sensitivity and/or grant or contract requirements.