THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PROTECTION OF DATA POLICY

Number 06.01.01

Division Administration – Office of Information Technology

Date June 2018; Reviewed and Revised February 3, 2025

Purpose The purpose of this policy is to define the responsibilities of users for supporting and protecting electronic data at The University of Alabama in Huntsville (UAH).

Policy

This policy establishes the responsibilities of all users to support, secure, and protect all electronic data at UAH. UAH is responsible for properly securing data in all forms, including but not limited to its intellectual property, contracts, research, and Personally Identifiable Information (PII). This policy defines the responsibility of all users to support and protect the electronic data at UAH regardless of the user's affiliation or relation with UAH, irrespective of where the data is located, utilized, or accessed. All UAH community members are responsible for protecting electronic data's confidentiality, integrity, and availability.

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 does not apply 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 personal device.

However, students should note that other policies may cover such data. 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 UAH Information in electronic form.

Procedure

1.0 Responsibilities

UAH functional units operating or utilizing IT resources manage and maintain 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 and OIT directives supporting this and other policies. 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.

It shall be the responsibility of the data steward to classify the data, with input from appropriate university administrative units and the Office of Counsel. However, all individuals accessing data are responsible for protecting the data at the level determined by the data steward or as mandated by law. Therefore, the data steward is responsible for communicating the classification level to individuals granted access. Any data not yet classified by the data steward 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, or Restricted according to the following categories:

1. **Public data -** 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 are included in Appendix A).
2. **Private data -** data that derives 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 are included in Appendix A). All computing devices connecting to the UAH network in any way or owned by UAH that store or transmit Private data must meet a minimum set of security standards as published by OIT within the Knowledge Base.
3. **Restricted data -** data that, by law, is not to be publicly disclosed and whose access is restricted to authorized employees.

The recipients of Restricted data must not reveal the contents to any individual unless that person has a valid need to know and authorized permission from the appropriate authorization from the data steward to access the data. The person revealing such Restricted data must have specific authority to do so. Restricted data must not be copied without authorization from the identified custodian (examples of Restricted data include data that are regulated by federal regulations such as the 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), and Export Administration Regulations (EAR) and are included in Appendix A).

All computing devices connecting to the UAH network in any way or owned by UAH that store or transmit Restricted data must meet a minimum set of security standards as published by OIT within the Knowledge Base.

1.1 Roles

1. **Data Steward** - A Data Steward is an individual or group of people who have been officially designated as accountable for specific data transmitted, used, and stored on a system or systems within a department or an administrative unit of the university.

   UAH Data Stewards are defined in the UAH Data Roles and Responsibilities document located within the Knowledge Base.

   The Data Steward is responsible for ensuring that appropriate steps are taken to protect data and for implementing policies, guidelines, and memorandums of understanding (MOUs) that define the appropriate use of the data. Where appropriate, stewardship may be shared by managers of different departments.

   The Data Steward or their designated representatives are responsible for and authorized to:

   - Approve access and formally assign custody of an information asset
   - Specify appropriate controls, based on data classification, to protect the information resources from unauthorized modification, deletion, or disclosure. The steward will convey those requirements to administrators for implementation and educate users. Controls shall extend to information resources outsourced by the university
   - Confirm that applicable controls are in place to ensure appropriate level of confidentiality, integrity and availability
   - Confirm compliance with applicable policies and controls, including but not limited to FERPA, PCI, PII, and HIPAA
   - Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures
   - Ensure access rights are re-evaluated when a user's access requirements to the data change (e.g., job assignment change)
   - Understand and report all security risks and potential breaches to the UAH CIO and CISO.

2. **Data Administrator** - The Data Administrator is the university or outsourced service provider charged with implementing the controls specified by the Data Steward.

   The Data Administrator is responsible for the processing, storing, and recovering information. The administrator of information resources must:

   - Implement the controls specified by the Data Steward(s)
   - Provide physical and procedural safeguards appropriate for the classification of the data
   - Assist Data Stewards by identifying any potential security risks and evaluating the overall effectiveness of controls and monitoring
   - Reporting, and assisting with incident investigation in accordance with the IT Incident Reporting and Breach Notification Policy.

3. **Data User** - A Data User is any person who has been authorized by the Data Steward to read, enter, or update that information.

   All Data Users have the responsibility to:

   - Use the resource only for the purpose specified by the Data Steward
   - Comply with controls established by the Data Steward
   - Prevent disclosure of Private or Restricted information.

1.2 Storage of Data on Non-UAH Owned Systems

Data classified as Private or Restricted shall not be stored on devices that are not owned by UAH without the approval of the data steward(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 Restricted. This includes on-premise and cloud-based services. See the “Cloud Service and Information Technology Procurement” policy for the approval process.

1.4 Data Access Restrictions

All data access must be authorized under the principle of least privilege and configured to the minimum level of access required to accomplish the university’s mission and based on minimal need. Applying this principle limits the damage resulting from accident, error, or unauthorized use. The data steward or their designee must approve all permissions to access Restricted data, and a written or electronic record of all permissions must be maintained.

The data steward or their designee shall audit data access at least annually for Private or Restricted data. During data access audits, data stewards will be provided a list of users with access and their access rights. The data steward 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 steward’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 Restricted data shall not be provided to external parties or users without approval from the data steward. In cases where the data steward is unavailable, 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 granted access to Private or Restricted data changes responsibilities, all of their access rights shall be reevaluated by the data steward and any access to protected data outside of the scope of their new position or status shall be revoked.

1.5 Data Backup

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

1.6 Data in Transit

Data transmitted without encryption increases the possibility of eavesdropping attacks, where an attacker may intercept the data being transmitted. Private and Restricted data shall only be transferred through channels encrypted with CISO-approved algorithms whenever possible. This may include transport layer security (TLS), secure shell (SSH), virtual private networks (VPN), or other encrypted sessions

1.7 Data Encryption

IT Resources that store data classified as Private or Restricted shall utilize robust encryption mechanisms to maintain the confidentiality of the data and significantly reduce the risk of theft or loss of IT Resources. Examples of strong encryption vary over time and will be provided by OIT upon request. For more information about strong encryption, see the most recent revision of NIST Special Publication 800-57.

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 accordance with any applicable data retention schedule and/or policy in a manner that guarantees that the data is not recoverable. Destruction can be accomplished via disk wiping utilities or physically destroying the storage device.

1.9 Approved Data Storage Facilities for Servers Storing Private or Restricted Data

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

All units of UAH will deploy and use IT resources to mitigate cybersecurity risks, provide 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 cybersecurity risk mitigation is not practicable for achieving a unit’s work, the unit shall formally document its role, responsibilities, and ongoing controls to mitigate cybersecurity risks to UAH. The OIT cybersecurity team can assist with documentation for units supported by OIT.

Documentation should include approval from the unit head, a brief description of IT resources, purpose, timeframe needed, and justification for exception. Documentation should be provided to the UAH CIO, CISO, or direct reports to maintain records. Documentation shall be updated at least annually. If updated documentation is not submitted or found 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 UAH Chief Information Officer is responsible for the review of this policy every three years, or whenever circumstances require.

PROTECTION OF DATA

APPENDIX A

Protection Requirements Based on Classification:

The tables below define minimum protection requirements for each data category when 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 the 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 connect to the UAH network must comply with the Security of IT Resources policy, as well as applicable laws and standards.
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

Institutional Private Data **(hereafter "Private Data")**	
Collection and Use	Limited to authorized uses only. Units/Colleges that collect and/or use Private Data should participate in the Information Security Program by reporting systems and 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 Steward and tracked in a manner sufficient to be auditable. Before granting access to external third parties, contractual agreements that outline responsibilities for the security of the data shall be approved through the UAH contract process.
Disclosure, Public Posting, etc.	Private Data shall not be disclosed without the consent of the data steward. Private 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 private data with the third party/service provider.
Storing or Processing: Server Environment	Systems or servers that process and/or store private data must comply with the 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 Private Data must comply with the Security of IT Resources policy, as well as applicable laws and standards. In addition, any/all systems that process or store Private Data must require a PIN and/or password for access to the device.

Storing on Removable Media (e.g. USB or external disk, etc.)	Private Data shall only be stored on removable media in an encrypted file format or within an encrypted volume.
Electronic messaging Transmission	Private Data shall be transmitted in either an encrypted file format or over a secure protocol or connection. Messages shall only be sent to authorized individuals with a legitimate need to know. Private Data may only be shared through approved UAH services that meet all required standards and are approved by the CIO or their designee.
Printing, mailing, fax, etc.	Printed materials that include Private 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 Private 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 Private Data visible and unattended.
Disposal	Repurposed for University Use - Multiple pass overwrite. NOT Repurposed for University Use - Physically destroy.

Restricted Data	
Collection and Use	Limited to authorized uses only. Units/Colleges that collect and/or use Restricted Data should participate in the Information Security Program by reporting systems and servers to the Office of Information Technology. In addition, any/all systems and 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 UAH policies. All access shall be approved by an appropriate Data Steward 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 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 Data must comply with Security of IT Resources policy, as well as applicable laws and standards. Storing data protected by PCI or HIPAA requirements is not permitted on UAH systems or servers. If information protected by these requirements must be stored or processed, contact the UAH CIO or CISO for guidance.
Storing or Processing: Endpoint Environment (e.g. laptop, phone, desktop, tablet, etc.)	Systems that process and/or store Restricted Data must comply with Security of IT Resources policy, as well as applicable laws and standards. Storing Restricted Data on personally-owned devices is not permitted. Devices storing or processing Restricted data must be physically secure at all times. Avoid storing Restricted Data on portable devices, where possible.

Storing on Removable Media (e.g. thumb drives, CDs, tape, etc.)	Restricted Data shall only be stored on removable media in an encrypted file format or within an encrypted volume, unless such controls are denied by law, grant or contract.
Electronic Transmission	Secure, authenticated connections or secure protocols shall be used for transmission of Restricted Data.
Email and other electronic messaging	Transmission of Restricted Data is not permitted without express authorization of the data steward or unless required by law. Messages with Restricted Data shall be transmitted in either an encrypted file format or only through secure, authenticated connections or secure protocols. Restricted Data may be shared through approved UAH services.
Printing, mailing, fax, etc.	Printed materials that include Restricted 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 Restricted 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 Restricted Data visible and unattended.
Disposal	Assets which contain Restricted data that are repurposed for University Use must first have addressable locations overwritten via a process that supports a minimum of 3-time overwrite. Assets which contain Restricted Data, such as hard drives, that are not repurposed for University Use must be physically destroyed.