

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PROTECTION OF DATA

-INTERIM-

<u>Number</u>	02.01.42
<u>Division</u>	Office of Information Technology (OIT)
<u>Date</u>	August 2015
<u>Purpose</u>	The purpose of this policy is to define the responsibilities of users for supporting and protecting data at UAH.
<u>Policy</u>	<p>This policy establishes the responsibilities of all users to support, secure, and protect 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 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 data from unauthorized generation, access, modification, disclosure, transmission, or destruction.</p> <p>This policy applies to all faculty, staff, students, researchers, or other users of information technology (IT) resources that connect to UAH networks, and/or store or transmit UAH data, regardless of ownership of the device or system, including personally owned devices or systems.</p>

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

All electronic data of UAH shall be classified as public, private, or confidential 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. These data include information that the university is under legal or contractual obligation to protect. 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).
- **Confidential data** - 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. For student data, the data should only be provided to the student, to which the data are attributed. 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. 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)).

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.

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.

1.2 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. 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 of a particular unit, 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.

When an individual who has been granted access leaves the university, all of their access rights shall be revoked at the time of termination.

1.3 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).

In the interest of securing information protected under FERPA, HIPAA, FISMA, PCI, ITAR, EAR, other state and federal legislation, university policies, and reducing the risks to the university of fines and other penalties, all users of IT resources shall follow the "Security of IT Resources" policy. This includes all devices that store or transmit university data, regardless of ownership. Devices that have this potential include, but are not limited to, storage devices, including CDs/DVDs, flash drives, hard drives, external storage devices, laptops, desktops, servers, tablets, phones, and networking devices.

1.4 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.

1.4 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.

1.5 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.

1.6 Approved Data Storage Facilities

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 vigilantly mitigate cybersecurity risks, maximize 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 vigilance to mitigate cyber risks to UAH.

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.

1.7 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.

1.8 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.

2.0 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 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



Chief University Counsel



Provost and Executive Vice President for Academic Affairs

APPROVED:

Robert A. Altenkirch

President