



ASU Data Classification Standard

Version 0.1
November 2008

Table of Contents

1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL	3
2 DOCUMENT REVISION	3
3 PURPOSE	4
4 SCOPE	4
5 RESPONSIBILITY FOR DATA MANAGEMENT	4
6 DATA CLASSIFICATION STANDARD	4
6.1 Public Data	4
6.2 Confidential Data	5
6.3 High Risk Data	6
7 DATA CLASSIFICATION ROLES AND RESPONSIBILITIES	8
8 ENFORCEMENT	9

1 DOCUMENT CLASSIFICATION: UNIVERSITY CONFIDENTIAL

Physical and Administrative Controls	Reproduction	Distribution	Destruction/Disposal
Each employee is responsible for controlling usage and access on a need-to-know basis. This policy also applies to contractors.	Limited copies may be made only to employees or contractors who have signed a non-disclosure agreement.	Internal: Use University envelope whenever possible. External: Use sealed envelope.	Use document destruction bins. Shred or erase magnetically recorded documents if unable to recycle.

2 DOCUMENT REVISION

Date	Revision	Revised By	Basis for Revision & Description

Document Change/Correction Request

Your feedback is valuable. Anyone who uses this document is invited to use this form to submit requests for changes or corrections to this document. Please complete all of the sections and mail to:

Document Identification

Document title
Date of Document
Master File Location

Requester Identification

Name	
Department	
Phone Number	() -
Email Address	

Request

The following Change is requested:

Please describe the change and reason(s) why the change is requested.

Correction

Section ____, page ____ contains the following erroneous information:

This information should be changed to:

Attach additional sheets if necessary to fully describe the change or correction.

3 PURPOSE

To educate the ASU community about the importance of protecting data generated, accessed, transmitted and stored by the University; to identify procedures that should be in place to protect the confidentiality, integrity and availability of University data; and to comply with local and federal regulations regarding privacy and confidentiality of information.

4 SCOPE

This standard is designed to protect all data that is protected by federal, State and local law, regulation and compliances.

5 RESPONSIBILITY FOR DATA MANAGEMENT

Data is a critical asset of the University. All members of the ASU community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form).

Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of University data in compliance with this standard.

Data owned, used, created or maintained by the University is classified into the following three categories:

- Public
- Confidential
- High Risk

Departments should carefully evaluate the appropriate data classification category for their information. Examples provided in this Standard are illustrative only and serve as identification of implementation practices rather than specific requirements. Nothing in this standard is intended to identify a restriction on the right of departments to require policies and/or procedures in addition to the ones identified in this document.

6 DATA CLASSIFICATIONS STANDARD

6.1 Public Data

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all members of the University community and to all individuals and entities external to the University community.

By way of illustration only, some examples of Public Data include:

- Publicly posted press releases
- Publicly posted schedules of classes
- Publicly posted interactive University maps, newsletters, newspapers and magazines

6.2 Confidential Data

Confidential (Internal Use Only) Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Confidential (IUO) Data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of Confidential Data include:

- Employment data
- University partner or sponsor information where no more restrictive confidentiality agreement exists
- Internal telephone books and directories????
- Research Data/ Intellectual Property (Non- National Security)

Confidential Data:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure and should be zoned in network with like data
- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use
- Must not be posted on public websites
- Must be destroyed when no longer needed subject to the University Record Retention Policy. Destruction may be accomplished by:
 - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
 - Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal.
 - Thumb drives and laptops should employ encryption when utilized. Laptops should utilize disk encryption and utilize AES standard

encryptions. Thumb drives should utilize password and username for entry. Locking cables should be utilized when laptop is left alone.

	Physical and Administrative Controls	Reproduction	Distribution /Transmission	Storage	Destruction See Data Sanitation Standard.
Hard Copies	Must be under lock and Key	Limited Copies : Labeling "Internal Use Only" or Confidential <Dept>	Internal: User University Envelope External: Use Sealed Envelope	Locked Filing Cabinets/Draws or hanging files	Use Document Bins or shred
Electronic	Restricted Access to Need-to-know	Restrict copy function access rights:	Utilize SSL within network	Must be in a encrypted system utilizing OS level EFS and NTFS	Magnetically wipe or destroy media
Responsibilities	All Employees	These fall on Administrative and System Administrative.	Falls on administrative staff and system/network administrators	All administrative staff and system administrators	All Staff and system administrators
3 rd Party Requirements	Must sign a Non-Disclosure 3 rd Party Agreement	Will not reproduce	Utilize SSL and or IPSEC	Storage should be done in a 3 rd party encryption 3DES 256 key or higher	Utilize shredding if hardcopy and magnetically wipe and destroy media

6.3 High Risk Data

High Risk Data is information protected by statutes, regulations, University policies or contractual language. Managers may also designate data as High Risk.

High Risk Data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside the University should be authorized by executive management and/or the Vice President and General Counsel.

By way of illustration only, some examples of High Risk Data include:

- Medical records (HIPAA)
- Student records and other non-public student data (FERPA)
- Social Security Numbers (PII)
- Personnel and/or payroll or records (PII)
- Any data identified by government regulation to be treated as confidential or sealed by order of a court of competent jurisdiction (Legal)
- Intellectual Property/Research Data (Government Classified: Confidential and above)

High Risk data:

- When stored in an electronic format, must be protected with strong passwords and stored on servers that have protection and encryption measures provided by AES in order to protect against loss, theft, unauthorized access and unauthorized disclosure. High Risk Data should be placed in a network zone of like departmental data.
- Must not be disclosed to parties without explicit management authorization.
- Must be stored only in a locked drawer, room or area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know basis.
- When sent via fax must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on public websites.
- Must be destroyed when no longer needed subject to the University Record Retention Policy. Destruction may be accomplished by:
 - "Hard Copy" materials must be destroyed by shredding or another process that destroys the data beyond either recognition or reconstruction. After destruction, materials may be disposed of with normal waste.
 - Electronic storage media shall be sanitized appropriately by degaussing 3 times prior to disposal.
 - Thumb drives and laptops must employ encryption when utilized. Laptops should utilize biometric technology that locks down to the bios and provides no way to gain access to command prompts. Thumb drives should leverage AES standard encryptions and leverage FIPS-2 compliance for wiping data. Locking cables should be utilized when laptops are left alone.

	Physical and Administrative Controls	Reproduction	Distribution /Transmission	Storage	Destruction <i>See Data Sanitation Standard</i>
Hard Copies	Must be under lock and Key	Limited Copies : Labeling "HRI" or HRI<HIPAA/FERPA/PII PCI and National Security Intellectual Property>	Internal: User University Envelope External: Use Certified mail Sealed Envelope	Locked Filing Cabinets/Draws or hanging files	Use Document Bins or shred
Electronic	Restricted Access to Need-to-know	Restrict copy function access rights:	Utilize SSL within network	Must be in a encrypted system utilizing AES longest key available/	Magnetically wipe or destroy media.
Responsibilities	All Employees	These fall on Administrative and System Administrative	Falls on administrative staff and system/network administrators	All administrative staff and system administrators	All Staff and system administrators
3 rd Party Requirements	Must sign a Non-Disclosure 3 rd party Connection Agreement	Will not reproduce	Utilize SSL and or IPSEC	Storage should be done in a 3 rd party encryption AES longest key available	Utilize shredding if hardcopy and magnetically wipe and destroy media

The Office of the Information Security Officer must be notified in a timely manner if data classified as High Risk is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place or is suspected of taking place.

7 DATA CLASSIFICATION ROLES AND RESPONSIBILITIES

UTO and IT University entities are primarily charged with developing processes and procedures subordinate to and in support of this standard.

The Office of the Information Security Officer within UTO is charged with the promotion of security awareness within the University community as well as responsibility for the creation, maintenance, enforcement and design of training on relevant security processes and procedures in support of this standard.

The Information Security Officer will receive and maintain reports of incidents, threats and malfunctions that may have a security impact on the University's information systems and will receive and maintain records of actions taken or standards and procedures developed in response to such reports.

The HIPAA Privacy Officer will receive and maintain reports of incidents, threats and malfunctions that may have a privacy impact on the University's HIPAA policies and will receive and maintain records of action taken or standards and procedures developed in response to such reports.

The Information Security Officer/ HIPAA Privacy Officer will assist the Internal Audit Department, as appropriate, in conducting periodic audits to determine University compliance with this standard.

The University Internal Audit Office will facilitate the distribution of this standard; they will assist in the investigation of policy breaches, and method for reporting instances of suspected misconduct and violations of law or University policies.

The Office of the General Counsel will review procedures issued under authority of this standard for compliance with applicable regulations. General Counsel will also respond to court ordered releases of information.

The Data Trustee will provide oversight in their perspective areas and ensure enforcement of this Standard.

The Data Steward will provide access within their general area and ensure accuracy, privacy, and security.

The Data Custodian will provide physical data management and manage access rights.

The Security Administrator will provide application security within general area and authorized users based on approval processes and procedures.

The Authorized User will be responsible for protection of data from disclosure, loss and theft and will report its loss immediately to the Information Security Officer and/or HIPAA Privacy Officer. The Authorized User will only disclose information to authorized personnel.

The Information Security Oversight will be the initial forum for discussion of questions arising out of or in response to this Standard.

8 ENFORCEMENT

Any employee found to have violated this Standard may be subject to disciplinary action up to and including termination of employment.