

UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM

SECTION: Information Technology

Number: 07.A.08

AREA: Computing Services

SUBJECT: Data Classification and Protection

1.- PURPOSE

The purpose of this policy is to direct information owners and information custodians in the assessment of information and information systems to determine the appropriate data classification level, which then prescribes the necessary security measures which must be in place.

For guidelines related to the disclosure of information, refer to [SAM 01.D.06, Protection of Confidential Information](#) and the Office of General Counsel.

2.- POLICY

It is the policy of the University of Houston System (UHS) to ensure data is appropriately classified and technical and physical security safeguards are implemented to protect the data. Appropriate protection measures must be applied to UHS information, no matter the location where the information is stored or accessed.

3. DEFINITIONS

3.1. Critical information resource: - An information resource housing confidential, sensitive personal or mission critical information. Critical information resources must have the following physical and technical safeguards implemented:

- A. Physical access granted only to authorized personnel via access cards, keys or other control mechanisms.
- B. Protection from environmental hazards.
- C. Regularly completed backups of all files. If the ~~component~~ university backup system is not used, the backup data must be stored in a separate, secure area.
- D. Uninterrupted power supply (UPS).
- E. [Supported operating system with all relevant updates installed.](#)
- ~~F.~~ Relevant security patches installed.
- ~~G.~~ Anti-virus software installed and appropriately configured.

- G.H. Unnecessary and/or inactive accounts must be disabled or deleted.
- H.I. Vendor-supplied system passwords must be replaced with strong passwords.
- J. Audit/security logs enabled on the critical information resource.
- J.K. Prior to the disposal of the critical information resource, a secure destruction method must be used to ensure the resource is sanitized rendering the data unrecoverable.

- 3.2. Information cCustodian: - ~~An information custodian is a~~ person, ~~(or department, /or unit)~~ providing operational support for an information resource (e.g., server administrators) and implementing iInformation oOwner defined controls and access to an information resource.
- 3.3. Information oOwner: - ~~An information owner is t~~The person responsible for the business use of a collection of information or the business function supported by a system (e.g., the Registrar is the information owner of student records) and for establishing the controls for the generation, collection, processing, dissemination, and disposal of the information. The information owner may also be responsible for other information resources including personnel, equipment, and information technology that support their business function. The head of a respective college, division or department may be the information owner, and ownership may be shared by managers of different departments.
- 3.4. Information resource: - As defined by Texas Government Code Section 2054.003(7), Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

4. DATA DEFINITIONS

- 4.1. Confidential information (Level 1 data): - Information, as defined by SAM 01.D.06 – Protection of Confidential Information, that includes, but is not limited to, social security numbers, educational records as defined by the Family Educational Rights and Privacy Act (“FERPA”), health care information as defined by the Health Insurance Portability and Accountability Act (“HIPAA”) and other applicable law, and customer information as defined by the Gramm-Leach-Bliley Act (“GLB Act”).
- 4.2. Sensitive personal information (Level 1 data) - ~~As defined by the~~ Texas Business and Commerce Code Section 521.002(a)2),
 - A. An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- social security number;
- driver's license number or government-issued identification number; or
- account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

B. Information that identifies an individual and ~~related~~relates to:

- ~~The~~the physical or mental health or condition of the individual;
- ~~The~~the provision of health care ~~of~~to the individual; or
- ~~Payment~~payment for the provision of health care to the individual.

4.3. Mission-critical information (Level 1 data): - Information defined by UHS, the each university, or information owners to be essential to the continued performance of the mission of UHS, each the U university or a university department or/ unit. Mission-critical information includes all research data obtained from third parties pursuant to an agreement or grant and/or other data necessary to substantiate research results or to satisfy grant-funding requirements, regardless of whether such data was developed by the university or obtained from third parties. An event causing the unavailability of mission-critical information has the potential to cause significant financial loss, including loss of future funding, institutional embarrassment, non-compliance with legal obligations, or closure of UHS, any of the its University universities or a university department or/ unit.

4.4. Protected information (Level 2 data): - Information that may be subject to disclosure or release under the Texas Public Information Act as requested.

4.5. Public information (Level 3 data) -: Information readily available in the public domain, such as information posted on the UHS public website, each UHS component-university's public web-site, and any other information not classified as Level 1 or 2.

5. CLASSIFYING DATA

5.1. It is the responsibility of the information owner to classify information for which they are responsible into one of the types listed in Section 4.

5.2. It is the responsibility of the information custodian to ensure the appropriate technical and physical security safeguards are implemented as directed by the information owner.

5.3. If the information owner cannot classify data based on the definitions in Section 4, the data should be classified according to the requirements ~~of~~for confidentiality, integrity, or availability of the information. These requirements

may be defined by documents such as non-disclosure agreements, memoranda of understanding, service-level agreements, etc. Data must be classified by the highest level identified for any one of the criteria.

- Confidentiality – Data must be limited to individuals with sufficient privileges and demonstrated need.
- Integrity – Data must be whole, complete, and uncorrupted.
- Availability – Data must be able to be accessed in a timely manner and usable format.

Criteria	Information Protection Level		
	Required	Recommended	Optional
Confidentiality	Level 1	Level 2	Level 3
Integrity	Level 1	Level 2	Level 3
Availability	Level 1	Level 2	Level 3

6. DATA PROTECTION REQUIREMENTS

6.1. Level 1 – Data classified as Level 1 must be protected in the following manner:

- A. Must be stored on a critical information resource [as defined in Section 3.1](#).
- B. Must have appropriate data access controls in place [such as a unique identifier and password for electronic information and storage in a locked location for hard copy information](#).
 - ~~If electronic information, access must be granted only through the use of a user ID and complex password.~~
 - ~~If hard copy information, must be stored in a locked location (such as a locked file cabinet).~~
- C. Must ~~not~~ be [encrypted when](#) transmitted via wireless network devices ~~unless encrypted~~.
- D. Must ~~not~~ be [encrypted when](#) transmitted by e-mail ~~unless encrypted~~.
- ~~E. Should be encrypted at rest when technically and feasibly possible.~~
- ~~EG. Should~~ [Must not be stored on non-university devices or non-university managed cloud storage without approval from UHS Information Security to ensure appropriate agreements, security controls and compliance requirements are in place. If a valid business need requires level 1 data to be stored on a non university device, specific permission must be obtained](#)

~~in advance from the department/unit head or component university Information Security Officer.~~

F. ~~Should~~ Must not be stored on a removable device (e.g., USB flash drive or external hard drive) or portable device (~~such as a e.g., flash drive or~~ laptop or tablet), but rather accessed directly from the critical information resources where the data is stored. If ~~a valid business need requires level 1 data to be stored on~~ a removable or portable device must be used, the information must be encrypted.

~~G. Should not be stored on non-university devices. If a valid business need requires level 1 data to be stored on a non-university device, specific permission must be obtained in advance from the department/unit head or component university Information Security Officer.~~

GE. Should be encrypted at rest when technically and feasibly possible.

6.2. Level 2 – Data classified as Level 2 does not require specific protection measures, but the following safeguards are recommended to ensure the confidentiality, integrity, and availability of the information.

- A. Should be stored on a critical information resource.
- B. Should have appropriate access controls in place (e.g., user ID and password).

6.3. Level 3 – Data classified as Level 3 has no requirement for confidentiality, integrity, or availability. As such, no specific protection measures are required.

7. REVIEW AND RESPONSIBILITIES:

Responsible Party: Senior Associate Vice Chancellor for Information Technology and Chief Information Officer

Review: Every ~~three~~ five years ~~on or before June 1~~

8. APPROVAL

Approved: Jim McShan
Senior Vice Chancellor for Administration and Finance

Renu Khator
Chancellor

Date: December 15, 2017

9. ASSOCIATED POLICIES

System Administrative Memoranda (SAM) 07.A.11 – Information Security Incident Reporting and Investigation

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	09/06/2011	Initial version (MAPP 10.05.03)
2	06/12/2015	Converted from MAPP 10.05.03 to SAM 07.A.08
3	12/15/2017	Added research data in the definition of mission-critical information in Section 4.3. Included encryption of data at rest when technically and feasibly possible to Data Protection Requirements (Level 1) in Section 6.1.E