

UTMB INFORMATION RESOURCES PRACTICE STANDARD

Section 1	Security Management	07/03/2008	-Effective
Subject 0	Governance and Dictionaries	07/03/2008	-Revised
Practice Standard 1.0.4 Data Classification		Information Security Officer-Author	

Data Classification

Introduction

Confidentiality, Integrity, Availability (CIA) are three words to be considered when protecting data.

Data classification is something that institutions have been struggling with for many years. While some data, such as PHI (Protected Health Information), financial, student and certain elements of personal information are clearly defined and regulated by statutes, laws and policy, other types of data classification are not so clear. It is up to the data owner to review and apply the necessary classification to ensure that sensitivity (integrity) and confidentiality are adequately maintained.

Purpose

The purpose of this standard is to set minimum requirements for properly and consistently classifying and adequately protecting data throughout UTMB.

Audience

This standard applies to all owners of data created, manipulated and stored on any UTMB Information Resource.

Implications

- The responsibility for data classification, as defined in this standard, is uniquely that of the data owner. This responsibility cannot be delegated to a system custodians or data users.
- The relative classification of data should be reviewed, and if necessary modified, periodically to ensure appropriate protections and control are applied.
- Data owners need to document the classification of data to facilitate appropriate review and audit functions.
- Data owners need to inform system custodians and data users of data classifications to ensure necessary protections and controls are applied and adhered to.

UTMB INFORMATION RESOURCES PRACTICE STANDARD

Section 1	Security Management	07/03/2008	-Effective
Subject 0	Governance and Dictionaries	07/03/2008	-Revised
Practice Standard 1.0.4 Data Classification		Information Security Officer-Author	

Data Classification, continued

Sensitive Digital Data Management

UTMB Information Resource users are required to protect “Sensitive Digital Data” in accordance with UTMB Practice Standard 1.2.10 – Managing Sensitive Digital Data.

Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).

Practice Standards

Data owners are required to classify all data stored and processed within their respective UTMB information resources and to apply the appropriate [technical and administrative safeguards to adequately protect the data](#) from unauthorized disclosure, access or alteration. Data owners will also ensure that data is available when needed.

All UTMB data must be classified into one of the three categories:

- Confidential
 - Sensitive
 - Public
1. Confidential - Any data that UTMB is legally or ethically obligated to protect and where the unauthorized disclosure or alteration would have a negative impact to UTMB, either financially, legally, or through the loss of professional reputation. Access to confidential data will be limited to authorized users. Examples of confidential information include but are not limited to the following:
- a) Patient Medical/Health Information (HIPAA)
 - b) Student Records (FERPA)
 - c) Donor/Alumni information (UTS, Texas Identity Theft Enforcement and Protection Act, HIPAA)
 - d) Research information (Granting Agency Agreements, Other IRB Governance)
 - e) Employee personal Information
 - f) Access credentials (information resources and physical security)
 - g) Human Resources related data
-

UTMB INFORMATION RESOURCES PRACTICE STANDARD

Section 1	Security Management	07/03/2008	-Effective
Subject 0	Governance and Dictionaries	07/03/2008	-Revised
Practice Standard 1.0.4 Data Classification		Information Security Officer-Author	

Data Classification, continued

Practice Standards (cont)

-
- h) Business/Vendor data (Gramm-Leach-Bliley Act, Non-Disclosure agreement)
 - i) Proprietary Information, i.e. data network maps, certain management information critical infrastructure detail.
 - j) Any data classified as confidential by the data owner.
2. Sensitive – Any data which requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. The controlling factor for sensitive data is that of integrity.
- a) Publicly accessible directory entries
 - b) Library Catalog
 - c) Official web-site postings
 - d) Research data
 - e) Any data classified as sensitive by the data owner
3. Public – Any data that, if disclosed or manipulated, would not negatively impact UTMB and does not meet the requirements of the confidential or sensitive categories. Examples of public information include but are not limited to the following:
- a) Blogs
 - b) News group posting
 - c) Chat room posting
 - d) Public domain data
 - e) Any data classified as public by the data owner
4. The below matrix is designed to assist data owners with classification requirements and to provide them the appropriate controls to adequately protect sensitive and confidential data.

UTMB INFORMATION RESOURCES PRACTICE STANDARD

Section 1	Security Management	07/03/2008	-Effective
Subject 0	Governance and Dictionaries	07/03/2008	-Revised
Practice Standard 1.0.4 Data Classification		Information Security Officer-Author	

Data Classification, continued

Practice Standards (cont)

Data Classification and Security Matrix				
Need for Confidentiality	Need for Data Integrity	Need for Availability	Category	Required Technical Controls
Yes	No	No	Confidential	Restrict access to authorized users.
Yes	Yes	No	Confidential	Restrict access and modify/write permissions to authorized users.
Yes	Yes	Yes	Confidential	Restrict access and modify/write permissions to authorized users. Host data on an institutional server; backup as required.
Yes	No	Yes	Confidential	Restrict access to authorized users. Host data on an institutional server; backup as required.
No	Yes	No	Sensitive	Restrict Modify/write permissions to authorized users.
No	Yes	Yes	Sensitive	Restrict modify/write permissions to authorized users. Host data on an institutional server
No	No	Yes	Public/ Sensitive	Host data on an institutional server.
No	No	No	Public	None

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.

UTMB INFORMATION RESOURCES PRACTICE STANDARD

Section 1	Security Management	07/03/2008	-Effective
Subject 0	Governance and Dictionaries	07/03/2008	-Revised
Practice Standard 1.0.4 Data Classification		Information Security Officer-Author	

Data Classification, continued

References

-
- UTS 165 – Information Resources Use and Security Policy
 - Texas Administrative Code, Ch. 202 – Information Security Standards