Policies of the University of North Texas Health Science Center	Chapter 04 - Administration
04.304 Data Integrity and Classification	

Policy Statement.
The purpose of this policy is to provide a standardized classification system for data owners and managers to classify data in a consistent way so as to maintain data integrity and appropriate security levels of the University's data resources in the central computing facility.

Application of Policy.
Deans, Department Heads, and Supervisors

Definitions.
None

Procedures and Responsibilities.

Procedure / Duty	Responsible Party
1. Classification: Data should be classified into the following categories. Most data will fall into more than one category, but should be managed in accordance with its most restrictive classification.	Director of Infrastructure and Security

Availability: Data should be analyzed for operational dependency. How long can you operate without the data? Then use the table below to classify its criticality.

Class	A	B	C	D	E
Maximum allowed Server downtime, per event	> 1 Week	1 Week	1 Day	1 Hour	1 Hour
On which Days?	Any	Mon-Fri	Mon-Fri	Mon-Fri	7 Days
During what hours?				07:00-18:00	24h
Expected availability percentage	70%	80%	95%	99.5%	99.9%
==> expected max. downtime	= 1 week/ month	= 1 day/week	= 2 hours/ Week	= 20min./ Week	= 12min./ month

2. Sensitivity

Director of Infrastructure and Security

A classification system is proposed which classes information / processes into three levels. The lowest 1 is the least sensitive and the highest 3 is for the most important information / processes. The following concepts are needed:

- All data has an owner.
- The data or process owner must classify the information into one of the security levels- depending on legal obligations, costs, corporate into policy and business needs.
- If the owner is not sure at what level data should be classified, use level 3.
- The owner must declare who is allowed access to the data.
- The owner is responsible for this data and must secure it or have it secured (e.g. via a security administrator) according to its classification.
- All documents should be classified and the classification level should be written on at least the title page.

Once the data on a system have been classified to one of the following levels, then that system should be installed to conform to all directives for that class and classes below.

If a system contains data of more than one sensitivity class, it must be classified at the most confidential level for data on the system. The data names listed in each class below are not intended to be exhaustive but are only examples. There are many other data at the UNTHSC-FW that need to classified as well.

Class 1: Public / non classified information
This data could be made public without any implications for the UNTHSC-FW (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger.

Examples: Test services without confidential data, certain public information services, news releases, news letters, items classified as public by State law, and data already available in the public domain, etc.

Class 2: Internal information
External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the UNTHSC-FW may be publicly embarrassed). Internal access is

	selective. Data integrity is important but not vital. Examples of this type of data are found in development groups (where no live data are present), certain production public services, certain Customer Data, "normal" working documents and project/meeting protocols, Telephone books, budgets, purchasing information, and fund raising information, etc.	
3.	Confidential information Data in this class are confidential within the UNTHSC-FW and protected from external access. If such data were to be accessed by unauthorized persons, it could influence the institution's operational effectiveness, cause an important financial loss, or unauthorized access would prove to be a violation of the law. Data integrity is vital. Examples: Data centers normally maintain this level of security. Such data are personnel data, Accounting data, passwords, data protected by law, patient health information, student records, intellectual property, and data that will cause damage to the institution, etc.	Director of Infrastructure and Security

References and Cross-references.
None

Forms and Tools. (optional)

Approved: 5/1/2004
Effective: 5/1/2004
Revised: 4/24/2009