

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.21	Data Classification	Responsibility:	Chief Information Security Officer

DATA CLASSIFICATION

Overview

Data classification is necessary to identify critical data that is essential for business operations. Security control measures are established and maintained based on data criticality and associated vulnerabilities.

Policy

Data is classified as follows:

Confidential/High Risk: Information protected by law and/or the disclosure is likely to result in significant adverse impact to the institution (embarrassment, financial loss, sanctions, etc.) The highest levels of protection are required for the protection of this information's confidentiality, integrity and availability including: administrative, technical, and physical safeguards. Classification examples include:

1. Protected Health Information: clinical patient records, identifiable patient research records.
 2. Student Identifiable Information: student demographic information, performance, financial, or health records, etc.
 3. Personnel Information: institutional and departmental personnel records that contain private information on an employee.
 4. Sensitive Digital Research Data: Electronic data requiring highest levels of protection due to the following circumstances:
 - a. data collected is subject to protection under federal or state law (HIPAA, FERPA, social security numbers).
 - b. data received or collected must be protected under specific requirements of externally-supported research agreements.
 - c. the project under which the data is being collected carries a security classification established by an authorized agency of the federal government.
 - d. information or data collected would violate the confidentiality of sources or subjects involved in the research.
-

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.21	Data Classification	Responsibility:	Chief Information Security Officer

-
- e. other instances where data collected warrants additional protection; designation of data subject to this circumstance will be made by the Vice President for Research.
5. Credit Card Information (Cardholder Data): At a minimum, cardholder data is the full credit card number (also known as the Primary Account Number or PAN). Cardholder data may also appear in the form of the full PAN plus any of the following:
- a. Cardholder name
 - b. Expiration date
 - c. Service code (the three- or four-digit security code on the back of the credit card; AMEX is on the front).
6. Other Sensitive Information: Other information that presents a significant competitive or regulatory disclosure risk including intellectual property subject to a confidentiality obligation, Homeland Security information, social security numbers, information described in University of Texas System Policy [UTS 165, "Information Resources Use and Security Policy"](#), data related to University Police, and Internal Audit investigations, etc.

Confidential: Confidential, sensitive and/or valuable data that warrants protection from unauthorized access, modification, and/or disclosure; without representing a significant exposure or financial loss should security measures fail. Examples include: personal data not protected by law, budget records, financial transactions, and other research data requiring integrity controls.

Internal: Routine operational information requiring no special measures to protect from unauthorized access, modifications or disclosure, but not widely available to the public.

Public: Information that is widely available to the public through publications, pamphlets, web content and other distribution methods.

It is the responsibility of the data owner to classify data and ensure that necessary security requirements comply with the Health Science Center

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.21	Data Classification	Responsibility:	Chief Information Security Officer

[Protection by Data Classification Security Standard](#), which includes but is not limited to the following forms of protection:

- Marking
- Transport/release
- Printing/displaying
- Storage
- Destruction
- Physical protection
- Access control
- Back-up and recovery
- Incident response

The [Protection by Data Classification Security Standard](#), as well as other security standards and guidelines pertaining to Information Security policies, may be found at the Information Security Web site (<http://ims.uthscsa.edu/policies.aspx>).

Accountability

Violations of this policy are subject to disciplinary action as described in the *Handbook of Operating Procedures* (HOP), [Section 2.1.2](#), "*Handbook of Operating Procedures*".
