

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

|                      |                                   |                 |                                    |
|----------------------|-----------------------------------|-----------------|------------------------------------|
| Chapter 5            | Information Management & Services | Effective:      | October 2004                       |
| Section 5.8          | Information Security              | Revised:        | May 2011                           |
| <b>Policy 5.8.23</b> | <b>Data Back-up Policy</b>        | Responsibility: | Chief Information Security Officer |

# DATA BACK-UP POLICY

---

## Overview

Creating a back-up of data on magnetic tape, CD ROM, or other removable media that can be safely stored in another location is essential to the data recovery operation in the event of loss of the computer system or media on which the data resides. A clear, defined and documented back-up strategy is an industry best practice, and each department should ensure that routine data back-up processes and procedures are in place whether using central services or local resources.

---

## Policy

Appropriate security measures shall be taken to ensure the protection of and continued availability of all Health Science Center, including UT Medicine, information resources. To ensure the continued availability of critical information, the following data backup procedures should be implemented:

- The data owner must establish the criticality of the data and the risk associated with its loss.
- Data back-up procedures must be established and implemented to create and maintain retrievable copies commensurate with data criticality and associated risk to the institution.
- Data back-up procedures must be tested on a periodic basis to ensure that exact copies of the data can be restored and placed into production use.
- Back-up media must be stored in a physically secure environment, such as a secure, off-site storage facility. If back-up media remains on site, it must be stored in a separate, physically secure location.
- If using an off-site storage facility or backup service and if the information is “confidential/high risk”, a Business Associate Agreement must be used to ensure that the service will safeguard such data in an appropriate manner.

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

|                      |                                   |                 |                                    |
|----------------------|-----------------------------------|-----------------|------------------------------------|
| Chapter 5            | Information Management & Services | Effective:      | October 2004                       |
| Section 5.8          | Information Security              | Revised:        | May 2011                           |
| <b>Policy 5.8.23</b> | <b>Data Back-up Policy</b>        | Responsibility: | Chief Information Security Officer |

---

This policy includes, but is not limited to, back-ups for all files, records, images, voice or video files that may contain Health Science Center and UT Medicine critical information.

**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*".

---