

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.26</b>	<b>Electronic Information Security Risk Management</b>	Responsibility:	Chief Information Security Officer

# ELECTRONIC INFORMATION SECURITY RISK MANAGEMENT

---

## Overview

Risk management serves to protect the integrity, confidentiality, and availability of electronic information at the level required based on data classification. This document establishes the risk management policy for all information resources (Executive Committee members shall designate the entity organizational level responsible for security management) in order to create the culture, processes, and structures that are directed towards the effective management of potential risks and adverse effects. The purpose of this policy is to require all designated entities (Schools, departments, or divisions, including UT Medicine) conduct, at minimum, annual self-assessments of security risks related to electronic information. The purpose is to determine areas of vulnerability, to initiate appropriate remediation, to increase awareness, and to communicate shared responsibility at all levels of the organization.

---

## Policy

The risk management process shall be conducted annually as a formalized and ongoing activity. It will involve monitoring and managing identified risks to ensure that such risks are minimized to a level deemed acceptable by the School, department, or division for its operation, understanding that such management must meet or exceed all Information Security policy requirements as set forth in [Section 5.8](#), "Information Security" and other applicable areas in the "*Handbook of Operating Procedures*" (HOP) as determined by the Information Security Office (ISO). Risk assessments will be conducted on any entity within the Health Science Center or on any organization providing third-party services. These assessments may be conducted on any electronic information system, including, but not limited to, applications, servers, appliances, networks, and any process or procedure by which these systems are administered and/or maintained. The risk management framework will include:

- Risk Assessment - The qualitative and quantitative result of risk analysis and risk evaluation which identifies:
  1. The nature and value of the electronic information assets or organizational assets.

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.26</b>	<b>Electronic Information Security Risk Management</b>	Responsibility:	Chief Information Security Officer

- 
2. The threats against those assets, both internal and external.
  3. The likelihood of those threats occurring.
  4. The impact upon the institution.
- Risk Analysis - A systematic use of available electronic information to determine how often specified events may occur and the magnitude of their consequences.
  - Risk Evaluation - The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels, or other criteria with the decision-making process of an acceptable level of risk.

The integrated risk management process is a formalized and ongoing iterative process used to assess changing electronic information security risks; it also engages management in making decisions concerning these risks, determines the success of efforts taken to date, and outlines which, if any, corrective actions should be taken. The formal risk management process involves risk assessments, configurations, vulnerability identification, and budget considerations, and then compares those results with desired outcomes. It also addresses project plans and status reports, internal audits, security audits, and the responses to these audits. Users are expected to cooperate fully with any risk assessment being conducted on electronic systems for which they are held accountable and to work with the ISO. The [Electronic Information Security Risk Assessment Security Standard](#), as well as other security standards and guidelines pertaining to Information Security policies may be found at the Information Management and Services Web site (<http://ims.uthscsa.edu/policies.aspx>).

This policy applies to all system users, at all Health Science Center locations, including UT Medicine, using departmentally-managed systems or privately-owned computers accessing University electronic information resources.

---

## **Monitoring**

The ISO is responsible for monitoring the decentralized process of electronic information security risk management implemented by this

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.26</b>	<b>Electronic Information Security Risk Management</b>	Responsibility:	Chief Information Security Officer

---

policy. To facilitate the monitoring function and support institution-level management, risk management reports shall be provided to the ISO. Additionally, the ISO reserves the right to require additional security efforts when minimum security standards have not been established, recommend additional security safeguards, initiate scans, perform periodic security audits or assessments, request documentation pertaining to the risk management efforts, direct those efforts, and/or assist with the development of remediation plans.

---

**Authority**

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

---