

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	November 2007
Section 5.8	Information Security	Revised:	January 2012
Policy 5.8.29	Web Application Security	Responsibility:	Chief Information Security Officer

WEB APPLICATION SECURITY

Overview

The Health Science Center's Internet web applications reflect the University's reputation and provide Internet users access to information. These applications must be developed in a manner that prevents the data from becoming vulnerable. For this reason, secure web application coding practices must be implemented to minimize risks to the University and information.

Policy

This policy is required for the Health Science Center's, and UT Medicine's Internet applications and is desired for Intranet applications. This policy applies to web applications that are developed by Health Science Center employees and contractors; and, those that are purchased from a vendor. Departments and data owners are accountable for ensuring proper controls are in place during the development lifecycle of web applications, including the design, development, testing, production, and maintenance. Web application developers are responsible for implementing these secure web applications.

Security administration of web applications must comply with the Health Science Center's [Web Application Security Standard](#), which includes, but is not limited to, the following requirements:

- User input data must first be validated before it is processed by the application.
- User input validation must include string length and meta character control.
- Verify user supplied data does not contain commands or queries.
- User content, such as articles, blogs, wiki's, commentaries, etc. must be reviewed for appropriateness by the data owner before it is posted or published.
- If allowing user file inclusions, such files must be virus scanned before they are stored or executed.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	November 2007
Section 5.8	Information Security	Revised:	January 2012
Policy 5.8.29	Web Application Security	Responsibility:	Chief Information Security Officer

-
- Application interfaces must be coded to prevent buffer overflows.
 - Applications must prevent users from directly accessing internal objects, API's, files, and databases. The application must interact on behalf of the user.
 - Account credentials and session tokens must be adequately secured.
 - Strong password requirements must be implemented.
 - Secure connections must be used to protect sensitive transactions, session cookies, and log-on processes.
 - Encrypting stored sensitive information should be considered.
 - Sensitive information must be stored on internal servers and not on Internet accessible servers.
 - Application leakage of information, such as configurations, logs, internal working, etc., must be avoided.
 - Access to sensitive information or information protected by law must be controlled at the log-on account level and restricted to only authorized users.
 - Access control must be implemented and constrained to the least privileged access required to complete transactions.

The [Web Application Security Standard](http://ims.uthscsa.edu/policies.aspx), 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>).

Accountability

Departmental

Deans, Chairs, and Directors are accountable for ensuring that their department remains in compliance with all applicable local, state, and federal information security policies as described in [Section 4.9.2](#) of the *Handbook of Operating Procedures* (HOP), "Management's

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	November 2007
Section 5.8	Information Security	Revised:	January 2012
Policy 5.8.29	Web Application Security	Responsibility:	Chief Information Security Officer

Responsibilities". If the Health Science Center's network, systems, data, or mission are placed at risk due to a willful or negligent lack of compliance with information security policies, Information Management Services (IMS) personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee for security remediation and/or reconnection of services. The service fee will be charged to the department's Project ID.

Individual

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