

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.17 Server Hardening

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 Introduction

Servers are necessary to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

1.2 Audience

The Texas A&M University System Health Science Center (HSC) Server Hardening Policy applies to all individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resource security.

1.3 Ownership of Electronic Files

Electronic files created, sent, received, or stored on information resources owned, leased administered, or otherwise under the custody and control of the HSC are the property of the HSC.

1.4 Privacy

Electronic files created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the HSC are not private and may be accessed by HSC information system employees at any time without knowledge of the information resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Security Standards.

1.5 Definitions

- **Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the institution's information resources. The designation of an institution information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state institution's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the information resources of the institution. If an institution does not designate an IRM, the title defaults to the institution's President, and the President is responsible for adhering to the duties and requirements of an IRM.
- **Information Security Officer (ISO):** Responsible to the executive management for administering the information security functions within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Server:** A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server though it may also be running other client (and server) programs.
- **Vendor:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term

includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

2. SERVER HARDENING POLICY

2.1 A server must not be connected to the HSC network until it is in a HSC OIT accredited secure state and the network connection is approved by HSC OIT.

2.2 The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for HSC OIT accreditation. Some of the general steps included in the Server Hardening Procedure include:

- Installing the operating system from an OIT approved source,
- Applying vendor supplied patches,
- Removing unnecessary software, system services, and drivers,
- Setting security parameters, file protections and enabling audit logging, and
- Disabling or changing the password of default accounts.

2.3 HSC OIT will monitor security issues, both internal to HSC and externally, and will manage the release of security patches.

2.4 HSC OIT will test security patches against OIT core resources before release where practical.

2.5 HSC OIT may make hardware resources available for testing security patches in the case of special applications.

2.6 Security patches must be implemented within the HSC OIT specified timeframe.

3. DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY

Vice President for Information Technology and Chief Information Officer