

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

29.01.99.Z1.02 System Development

Approved September 1, 2010

Supplements System Policy 29.01

1. GENERAL

1.1 Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

1.2 Purpose

The purpose of the Texas A&M University System Health Science Center (HSC) System Development Policy is to describe the requirements for developing and/or implementing new software in the HSC information resources.

1.3 Audience

The HSC System Development Policy applies equally to all individuals who use any HSC information resource.

1.4 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 assistant (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.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **System Development Life Cycle (SDLC):** A set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.
- **Owner:** The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.
- **Custodian:** Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications, OIT is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.
- **User:** Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.
- **Production System:** The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

2. SYSTEM DEVELOPMENT

- 2.1 OIT is responsible for developing, maintaining, and participating in a SDLC for HSC system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review or implementation via continuous integration. This methodology ensures that the software will be adequately documented and tested before it is used for critical HSC information.
- 2.2 All production systems must have designated owners and custodians for the critical information they process. OIT must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- 2.3 If applicable, all production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. One or more designated access control administrators (who are not regular users on the system in question) must be assigned for all production systems.
- 2.4 Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.
- 2.5 When applicable, access to manipulate an application's production installation will be limited to the application's custodian, plus designated backups. Production database access will be limited to each application's custodian, plus designated backups, and any appropriate database administrators.
- 2.6 All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

3. DISCIPLINARY ACTIONS

Violation 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