Texas A&M Health Science Center Guidelines

29.01.99.Z1.02 Guideline: System Development

Approved September 1, 2010
Revised February 13, 2013

Supplements System Regulation 29.01

Reason for the Guidelines

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

1. System Development

1.1 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.

1.2 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.

1.3 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.
1.4 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.

1.5 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.

1.6 All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

2. Violations

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 Finance and Administration