29.01.03.H0.23 System Development and Acquisition

Approved: April, 2014
Next Scheduled Review: April, 2019

Procedure Statement

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.

Reason for Procedure

The purpose of this procedure is to describe the requirements for developing and/or implementing new software on Texas A&M University-Texarkana (TAMUT) Information Resources. It applies to all individuals who use TAMUT Information Resources.

Definitions

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.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, 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, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes 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): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency'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 agency. At TAMUT, the IRM is the CIO.

Information Technology: The name of the TAMUT department responsible for computers, networking and data management.

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.

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.

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.

Procedures and Responsibilities

1. SYSTEM DEVELOPMENT

1.1 INFORMATION TECHNOLOGY is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for TAMUT 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. This methodology ensures that the software will be adequately documented and tested before it is used for critical TAMUT information.

1.2 All production systems must have designated Owners and Custodians for the critical information they process. INFORMATION TECHNOLOGY must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

1.3 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. A designated access control administrator (who is not a regular user 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.

2. DISCIPLINARY ACTIONS

Violation of this procedure may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of TAMUT Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rule § 202.75, Information Resources Security Safeguards
System Policy 07.01, Ethics
System Regulation 29.01.02, Use of Licensed Commercial Software

References

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Information Security Officer
903-886-5425