Texas A&M University System Standard - System Development and Acquisition

Standard Statement

The purpose of the system development standard is to describe the requirements for developing and/or implementing new application software at the System Office (SO).

Definitions

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements). Refer to System Regulation 29.01.03 and the related Data Classification standard for more information.

Examples of "Confidential" data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records

Information Resources (IR): The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Mission Critical Information: Information that is defined by the SO or information resource owner to be essential to the continued performance of the mission of the SO. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, and failure to comply with regulations or legal obligations, or closure of the department.

Major Application**:** An information technology application at SO will be considered a major application if it meets one, or more, of the following criteria:

- The application cost $1 million, or more, to design and develop.
- The application requires ten, or more, person years of effort to design and develop.

- The application is used at a department-wide level for an on-going function, and manages confidential information (as defined by Texas Administrative Code [TAC] 202) such as credit card information, or personnel records.

- The application alters the work methods of enterprise mission critical administrative and business procedures, and supports financial, personnel, or strategic decision processes.

- The application is used by multiple system members at institution-wide level.

Owner of an Information Resource: an entity responsible for:

- A business function; and,

- Determining controls and access to information resources supporting that business function.

Official Standard

This Standard Administrative Procedure (standard) applies to SO Major Applications that store or process mission critical and/or confidential information.

The purpose of the implementation of this standard is to provide a set of measures that will mitigate information security risks associated with system development and implementation of new application software, including systems acquired from vendors. There may also be other or additional measures that will provide appropriate mitigation of the risks. The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

The intended audience is SO owners and custodians that manage SO Major Applications that store or process mission critical and/or confidential information.

1. STANDARDS

1.1 Department information resource owners, or their designees, are responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) plan. All software developed in-house that runs on production systems shall be developed according to an SDLC plan. Additionally, where applicable, the SDLC plan should also be followed for systems acquired from vendors. At a minimum, this plan shall 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. The requirement for such

methodology ensures the software will be adequately documented and tested before it is used for critical departmental or SO information.

1.2 All applicable systems shall have designated owners and custodians. Owners, and/or their designees, shall perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

1.3 The department head or owner of an information resource shall ensure that all applicable systems have a documented access control process to restrict who can access the system, as well as restrict the privileges available to system users. A log of permission(s) granted shall also be maintained.

1.4 Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. 1.5 Per State of Texas Department of Information Resources Security Controls Catalog v1.3, "Copies of production data are not used for testing unless the data has been authorized for public release or unless all custodians involved in testing are otherwise authorized access to the data."

At least two people will review and approve a change before it is moved into production. For emergencies, where this is not possible, a timely management review process shall be established.

Related Statutes, Policies, or Requirements

Regulation 29.01.04 and related standards

Guidelines and Forms

Guidelines, forms and templates relating to Systems Development Life Cycle SDLC may be found at http://opensdlc.org.

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer