# The Division of Information Technology
# University Information Security Standards

**Information Security Standard – System Development & Acquisition (Legacy TAC 202)**
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

**Supplements University Rule 24.99.99.W1**

## 1. General

The purpose of the system development procedure is to describe the requirements for developing and/or implementing new application software in the University.

## 2. Applicability

This information security standard applies to University information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this information security standard is to provide a set of measures that will mitigate information security risks associated with system development and implementation of new application software. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided is based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

The intended audience includes, but is not limited to, all information resources data/owners, management personnel, and system administrators.

## 3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act.

3.2 Information Resources: 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.

3.3 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. 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, failure to comply with regulations or legal obligations, or closure of the University or department.

3.4 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

## 4. Procedures

4.1 Department Heads, information resource owners, and/or their designees, are responsible for developing, securing, maintaining, and participating in a System Development Life Cycle (SDLC) plan. All software developed that runs on production information systems shall be developed according to an SDLC plan. 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, tested, and secure before it is used in production.

4.2 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.

4.3 The department head or owner of an information resource shall ensure that all applicable information 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 should also be maintained.

4.4 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.

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.

**OFFICE OF RESPONSIBILITY:** Information Technology

**CONTACT:** Chief Information Officer