

# STANDARD ADMINISTRATIVE PROCEDURE

## 29.01.99.M1.21 Information Resources – System Development and Acquisition

*Approved July 18, 2005*

*Next Scheduled Review: Currently Under Review*

*Supplements [University Rule 29.01.99.M1](#)*

### 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 Standard Administrative Procedure (SAP) applies to University information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this SAP 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 will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. 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 in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual ISAAC report (See [University Rule 29.01.99.M1](#)).

The intended audience is University owners and custodians that manage University information resources that store or process mission critical and/or confidential information.

### 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 (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.

- 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 for:
- 3.4.1 a business function; and,
  - 3.4.2 determining controls and access to information resources supporting that business function.

#### 4. PROCEDURES

- 4.1 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. 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 University information.
- 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 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.
- 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.

CONTACT: [Information Technology Issues Management of CIS](#)

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)