

**ADMINISTRATIVE PROCEDURES**

|  |  |
| --- | --- |
| **50.10 Information Resources Project Management** | **Revised: December 21, 2012** |

1. GOVERNING REGULATIONS

This procedure is governed by the Texas Administrative Code, Title 1, Part 10, [Chapter 216, Subchapter C](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=216&sch=C&rl=Y), Rules §216.20 - §216.22, and [Chapter 202](http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202), Information Security Standards.

1. DEFINITIONS

2.1 Major Information System – See Administrative Procedure 50.01, Section 7.

2.2 Mission Critical – See Administrative Procedure 50.01, Section 6.

2.3 Project – An information resources project that meets the following criteria:

a. Has a purposeful assignment or an undertaking that is either performed internally (by a department or the agency) or outsourced to create a customized information system solution.

b. Includes an initiative that provides information resources technologies and creates products, services or results within or among elements of a state agency.

c. Is characterized by well-defined parameters, specific objectives, common benefits, planned activities, a scheduled completion date and an established budget with a specified source of funding.

2.4 Requestor – A department head or program leader (or designee) who is responsible for funding and approving a project.

2.5 Sensitive Information – See Administrative Procedure 50.01, Section 5.

2.6 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.

2.7 Owner of an Information Resource – A designated department or person responsible for determining controls over and access to an information resource supporting a business function. An owner is responsible and authorized for several tasks:

a. Assigning custody of information resources and providing appropriate authority to implement security controls and procedures.

b. Ensuring accuracy, authenticity and integrity of data.

c. Ensuring compliance with applicable controls.

d. Specifying data control requirements and conveying them to users and custodians.

2.8 Custodian of an Information Resource – A designated department or person responsible for guarding or taking care of an information resource supporting a business function. A custodian is responsible for several tasks:

a. Implementing owner-specified controls and access guidelines.

b. Providing physical and procedural safeguards.

c. Implementing monitoring techniques and procedures for detecting, reporting and investigating security incidents.

2.9 Production System – The hardware, software, physical, procedural and organizational issues that need to be considered when addressing the security of an application or group of applications.

1. PURPOSE

The purpose of this procedure is to describe project management practices for Texas A&M Forest Service.

1. PROJECT SIZE CLASSIFICATION

4.1 If a project is mission critical, routinely houses or processes sensitive information or is a major information system, the requestor shall submit a statement of work (SOW) to the Information Resources (IR) Department Head for review and further handling.

4.2 Other projects are classified as either departmental or agency-wide, based upon the following criteria:

a. Departmental projects affect only department or division operations and are intended for departmental or division use.

(1) The Associate Director of the division shall approve and prioritize departmental projects that will be performed by department staff or outsourced.

(2) For departmental projects that will be performed in part by the IR Department, the requestor will submit a description outlining the project scope and requirements to the IR Department Head for further handling.

b. Agency-wide projects affect agency-wide operations and are intended for use by the entire agency or the public.

The requestor will work with the IR Department Head to document the project purpose, scope, specific objectives, technical requirements, planned activities and scheduled completion date.

4.3 Web-based projects performed in part or completely by the IR Department shall be managed according to the Administrative Procedure 50.08 Web Project Priority Planning Committee.

5. OUTSOURCING OF PROJECTS

5.1 For projects that will be outsourced in part or completely, the requestor shall prepare a detailed SOW that follows the [Texas Project Delivery Framework](https://dir.texas.gov/View-Resources/Pages/Content.aspx?id=16) guidelines.

5.2 The requestor shall submit the SOW for projects to be outsourced to the IR Department Head for review. The IR Department Head may suggest changes to the SOW and work with the requestor to finalize the SOW.

5.3 The IR Department Head will consult with the Purchasing Department Head for guidance on the appropriate procurement method and provide the approved SOW and a timeline for completion.

6. INTERNAL SYSTEM DEVELOPMENT

6.1 Department heads, information resource owners and their designees are responsible for developing, securing, 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, tested and secure before it is used in production.

6.2 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.

6.3 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 permissions granted shall also be maintained.

6.4 Where resources permit, there shall be a separation among 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.  
  
For projects that are developed by the IR Department, at least two IR Department members will review and approve a change before it is moved into production.   
  
Projects developed outside the IR Department shall, at a minimum, be reviewed by the Information Technology Administrator before being moved into production.

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

6.6 Detailed technical specifications, security requirements and a template SDLC plan for software application development will be provided by the IR Department upon request.

CONTACT: [Information Resources Department Head](mailto:cbryan@tfs.tamu.edu), 979/458-6607