PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.26 Information Resources – System Development and Acquisition
Approved October 21, 2013
Revised December 7, 2018
Next Scheduled Review: December 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to identify the requirements for developing and/or implementing new application software at Prairie View A&M University (PVAMU). In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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 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.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Custodian of an Information Resource - a person who is responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity.

Official Procedures and Responsibilities

1. GENERAL

1.1 There may be additional measures that department heads or deans will implement 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 Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP 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).

2. APPLICABILITY

2.1 This UAP applies to all PVAMU information resources that develop in-house software. The intended audience for this UAP includes, but is not limited to, all information resources data/owners, management personnel, and system administrators who develop in-house software.

3. PROCEDURES AND RESPONSIBILITIES

3.1 Information resource owners, and/or their designees, who develop in-house software, 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 should address the areas of requirements analysis; general design and detailed specifications for solutions; development; testing and quality assurance; user acceptance; production implementation; and, post-implementation support and maintenance. The requirement for such methodology ensures the locally developed software solutions will be adequately documented, tested, and secured before they are used for production operations.

3.2 The Information Security Officer (ISO) shall keep a list of all applicable systems and their designated owners and custodians. The ISO shall perform periodic risk assessments of systems to determine whether the controls employed are adequate.

3.3 The ISO shall ensure that all information resource owners, or their designees, have a documented access control process for all applicable systems. In addition, the information resource owners, or their designees, will maintain a log of permission(s) granted, which will be periodically reviewed by the ISO.

3.4 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. The ISO should ensure that the information resource owners establish procedures for approving software changes before they are moved into production. At a minimum, the procedures should include details on tests conducted to ensure the code performs according to requirements; plans for removing the code from production in case it does not perform according to requirements; and, two separate reviews and approvals. Also, the procedures should include a process

for the emergency migration of code into production to prevent or resolve damage to the information resource.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Forms

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

Contact Office

Office of Information Resources Management	936-261-9350