PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.17 Information Resources – Change Management
Approved May 26, 2009
Revised September 16, 2013
Revised March 28, 2018
Next Scheduled Review: March 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to describe the requirements for the appropriate management of changes to information resources. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code 202.75 Information Resources Security Safeguards.

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. (TAMUS Data Classification Standard).

Information Security Breach Notification Matrix – advises readers of their responsibilities in notifying the correct personnel in the event of a breach of information. (TAMUS Notification Matrix).

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.

Information Resources Manager (IRM) – person responsible to the State of Texas for management of the University's information resources. The designation of an IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the University's information activities, and ensure greater visibility of such activities within the University. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the University. If an IRM is not designated, the title defaults to the University's executive director who then will be responsible for adhering to the duties and requirements of an IRM.

Information Security Officer (ISO) - person responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

Custodian - the person responsible for implementing owner-defined controls and access to an information resource. The custodian is responsible for the processing and storage of information and is normally a provider of services.

Change - any implementation of new functionality, interruption of service, repair of existing functionality or removal of existing functionality.

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.

Official Procedures and Responsibilities

---

1. GENERAL

1.1 The information resources infrastructure at Prairie View A&M University (PVAMU) is expanding and continuously becoming more complex. There are more people dependent on information resources being interconnected, upgraded and expanded (e.g., administrative systems and application programs). As the interdependency among information resources grows, the need for an effective change management process is essential.

1.2 From time to time, information resources require a service disruption for planned upgrades, maintenance or fine-tuning. Additionally, such activities may result in unplanned service disruptions. Managing these changes is a critical part of providing a robust and valuable information resource infrastructure.

1.3 The goal of change management is to ensure that the intended purpose of the change is successfully accomplished, while eliminating or minimizing any negative impact to the users of the resources as a result of the change. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the user community.

1.4 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 202.75 Information Resources Security Safeguards, 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 systems storing or processing mission critical and/or confidential information. The intended audience for this UAP includes, but is not

limited to, all individuals that install, operate or maintain PVAMU information resources.

3. PROCEDURES AND RESPONSIBILITIES

3.1 A consistent process is to be used for the implementation of information resource changes. The degree to which change management activities and processes are employed is dependent on the projected inherent risk of the change (e.g. potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation) and the complexity of the information resources (e.g. number of users, interconnections with other systems, or number of components or subsystems). Where appropriate, the process should include: preparation, review/approval, notification, implementation, post-implementation review, and documentation.

3.2 Every change to a PVAMU information resource such as: operating systems, computing hardware, networks, and applications is subject to this UAP and should follow the procedures, unless special circumstances exist.

3.3 Facilities Services should report/coordinate all changes affecting computing environmental facilities (e.g. air conditioning, water, heat, plumbing, electricity, and alarms) to all impacted departments, the ISO, Information Resources Manager (IRM), and the Chief Information Officer (CIO).

3.4 A formal change request must be submitted for all changes prior to changes being made. Change requests are to be submitted to the Change Request Distribution Group (informationsecurity@pvamu.edu) by completing a Change Management Request Form and must be approved by the ISO, IRM, and CIO. Changes must be sufficiently prepared in order to minimize outages.

3.5 Preparation may include:

3.5.1 Review of previous similar changes and results in an attempt to avoid any repetition of mistakes or negative impact;

3.5.2 Determination of the following:

3.5.2.1 Best date/time for implementation (to minimize the impact to users) and the length of time required;

3.5.2.2 Net impact to other systems or to normal operations during and following the change implementation (inherent risk); and,

3.5.2.3 Risk associated with the change implementation (to minimize the risk of disruption of service caused by the change).

3.5.3 Ensuring that the changes will not negatively impact the overall system security.

3.6 Notification must be given to users in a timely manner, including relevant details that would not negatively impact the security of the information resource, such as time and date, nature of the change (e.g., projected net effect), and time needed

for implementation. The method of notification should be appropriate to the environment and the user base, but should include, at a minimum, email.

3.7 All change implementations should be performed in the approved manner.

3.8 All formal, documented approvals or rejections of change implementations must be maintained by the ISO until the next review cycle.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

Texas Administrative Code 202.75 Information Resources Security Safeguards

Contact Office

Office of Information Resources Management	936-261-9350