

**PRAIRIE VIEW A&M UNIVERSITY  
UNIVERSITY ADMINISTRATIVE PROCEDURE**

**29.01.03.P0.17 Information Resources – Change Management**

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

**1. PURPOSE**

- 1.1 The information resource infrastructure at PVAMU is expanding. As the interdependency among information resources grows, the need for an effective change management process is essential.

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.

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.

- 1.2 This University Administrative Procedure (UAP) applies to multi-user systems storing or processing mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this UAP are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this UAP.

The intended audience is information resource owners and system administrators of University information resources that store or process mission critical and/or confidential information.

**2. DEFINITIONS**

- 2.1 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.
- 2.2 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.
- 2.3 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.

- 2.4 Change:
  - 2.4.1 Any implementation of new functionality
  - 2.4.2 Any interruption of service
  - 2.4.3 Any repair of existing functionality; and
  - 2.4.4 Any removal of existing functionality
  
- 2.5 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.
  
- 2.6 Owner of an Information Resource - an entity responsible for:
  - 2.6.1 a business function; and,
  - 2.6.2 determining controls and access to information resources supporting that business function.

### **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 (i.e., potential for unplanned disruption of service, corruption/loss of data, or disclosure of confidential information resulting from the change implementation). Where appropriate, the process should include: preparation, notification/awareness, approval and documentation.
  
- 3.2 Preparation includes:
  - 3.2.1 Review results of previously implemented changes to prevent repetitive mistakes or negative impacts.
  
  - 3.2.2 Determine the following:
    - 3.2.2.1 the best time/date for implementation (to minimize the impact to users);
    - 3.2.2.2 the net impact to other systems or impact to normal operation during and following the change implementation (inherent risk);
    - 3.2.2.3 the risk associated with the change implementation (to minimize the risk of disruption of service caused by the change); and,
    - 3.2.2.4 the concurrence of the resource owner for implementation of the change.
  
  - 3.2.3 Ensure that the changes do not negatively impact the overall system security
  
- 3.3 Notification includes a forum or notification process that informs users of changes planned for implementation. Typically, user notification may include e-mail in addition to an announcement posted on the web. Notification should include relevant details indicated in the documentation section (see 3.4 below).

- 3.4 Approval and audit of application/software changes includes:
  - 3.4.1 Review of the code revision to be implemented which shall be performed by someone other than the developer;
  - 3.4.1 Approval of the implementation of code revision performed by someone other than the developer; and,
  - 3.4.2 Review of logs for previous change implementations.
- 3.5 Documentation and change include:
  - 3.5.1 Documentation: any issues identified during the preparation phase that require special considerations or a revision to the implementation plan.
  - 3.5.2 Change details for documentation include:
    - 3.5.2.1 date/time of change;
    - 3.5.2.2 expected duration or length of time required to implement the change;
    - 3.5.2.3 nature of the change (a brief description of the net effect);
    - 3.5.2.4 developer's name for the modification if newly developed or modified code is involved;
    - 3.5.2.5 implementer's name of the modification;
    - 3.5.2.6 an indication of successful or unsuccessful completion of the change; and,
    - 3.5.2.7 an analysis and "lessons learned" (corrective/preventative actions) for changes that deviated unexpectedly from the plan, resulted in an unplanned disruption of service, corruption of data, or disclosure of confidential information.

**Contact Office:** Information Security Officer; 936-261-2126