

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

29.01.03.P0.19 Information Resources – Account Management

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

1. PURPOSE

- 1.1 Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

The purpose of the implementation of this UAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. 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 will 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 UAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.

- 1.2 The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

2. DEFINITIONS

- 2.1 Confidential Information - information that is accepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act.
- 2.2 Account information - resource users are typically assigned logon credentials, which include, at the minimum, a unique user name and password.
- 2.3 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.
- 2.4 Information Security Officer (ISO) - responsible for administering the information security functions within Prairie View A&M University and reports to the Information Resources Manager (IRM).

- 2.5 Information Security Administrator - individuals granting access to university information resources
- 2.6 Logon ID - a user name that is required as the first step to logging into a secure system. Generally, a logon ID must be associated with a password to be of any use.
- 2.7 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, and failure to comply with regulations or legal obligations, or closure of the University or department.
- 2.8 Owner of an Information Resource - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 An approval process is required prior to granting access authorization to an information resource. The approval process shall document the acknowledgement of the account holder to follow all terms of use and the granting of authorization by the resource owner or their designee.
- 3.2 Each person is to have a unique Logon ID and associated account for accountability purposes. Role accounts (e.g., guest or visitor) are to be used in very limited situations, and must provide individual accountability when used to access mission critical and/or confidential information.
- 3.3 Access authorization controls are to be modified appropriately as an account holders employment or job responsibilities change.
- 3.4 Account creation processes are required to ensure that only authorized individuals receive access to information resources.
- 3.5 Processes are required to disable Logon IDs that are associated with individuals that are no longer employed by, or associated with the University. In the event that the access privilege is to remain active, the department (e.g., owner, department head) shall document that a benefit to the University exists.
- 3.6 All access privileges to information resources must be reviewed at least biannually by the owners (department heads or administrators), and documented as such.
- 3.7 Passwords associated with Logon IDs shall comply with the University Password.
- 3.8 Information Security Administrators or other designated staff:
 - 3.8.1 Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

- 3.8.2 Shall have a documented process for periodically reviewing existing accounts for validity.

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