PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.19 Information Resources - Account Management

Approved May 26, 2009
Revised January 15, 2015
Revised February 17, 2020
Next Scheduled Review: February 2025

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to provide procedures for the secure management of access authorization and associated credentials (e.g., User ID and password) for information technology resources.

Definitions

Confidential Information - information that is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g., The Texas Public Information Act.

Account – information resource users are typically assigned logon credentials which include, at a minimum, a unique user name and password.

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 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.

Information Security Administrator - individuals granting access to PVAMU information resources.

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.

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 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. Access to university information resources is normally controlled by a logon ID associated with an authorized account. Proper administration of these logon IDs is very important to ensure the security of confidential information and normal business operation of university managed and administered information resources.

1.2 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. 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.

3. PROCEDURES

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 holder's 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, or change of job duties (if access is deemed inappropriate). 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 UAP 29.01.03.P0.08 Password Authentication.

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; and,

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

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

Texas A&M System Data Classification Standard

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

UAP 29.01.03.P0.08 Password Authentication

Contact Office

Office of Information Resources Management	936-261-9350
