PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.01 Information Resources – Administrator/Special Access
Approved May 15, 2009
Revised May 10, 2011
Revised March 5, 2014
Revised May 14, 2019
Next Scheduled Review: May 2024

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for the creation, use, monitoring, control and removal of accounts with special access privileges.

Definitions

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 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.

Descriptive Data (e.g., logs) - information created by a computer system or information resource that is electronically captured and relates to the operation of the system and/or movement of files, regardless of format, across or between computer systems. Examples of captured information are dates, times, file size, and locations sent to and from.

User Data - user-generated electronic forms of information that may be found in the content of a message, document, file, or other form of electronically stored or transmitted information.

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 Technical support staff, security administrators, system administrators and others may have special access account privilege requirements compared to typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical users. Thus, the granting,

controlling and monitoring of these accounts is extremely important to an overall security program.

1.2 There may be additional measures that department managers/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 or ISO. 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) and the Senior Vice President for Business Affairs (SVPBA) prior to implementing alternate measures.

2. APPLICABILITY

2.1 This UAP applies to all Prairie View A&M University (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 AND RESPONSIBILITIES

3.1 The Information Security Officer (ISO) shall maintain a list(s) of personnel who have administrator, or special access, accounts for departmental information resources systems. The list(s) shall be reviewed at least annually by the appropriate department head, director, or their designee.

3.2 Each individual that uses Administrator and Special Access accounts must use the account with the least privileges for the work being performed (i.e., user account vs. administrator account) if two accounts are assigned.

3.3 Each account used for Administrator and Special Access must meet the guidelines established in UAP 29.01.03.P0.08 Password Authentication.

3.4 The information resource owner must change the password for a shared Administrator and Special Access account when an individual with the password leaves the department, PVAMU, or upon a change in the vendor or contractor personnel with access to a PVAMU information resource.

3.5 In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.

3.6 When Administrator and Special Access accounts are needed for internal or external audits, software development, software installation, or other defined needs, the need must be:

3.6.1 Authorized by the ISO;

3.6.2 Created with a specific expiration date;

3.6.3 Removed when the work is complete; and,

3.6.4 Documented within the department, or with a Special Purpose AD Account Request Form from the Forms Library.

Related Statutes, Policies, Regulations and Rules

System Policy 29.01 Information Resources

System Regulation 29.01.03 Electronic Information Services Access and Security

Tex. 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