

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

**29.01.03.P0.01 Information Resources – Administrator/Special Access**

Approved: (May 2009)

Revised: (May 10, 2011)

Next Scheduled Review (May - 2012)

**1. PURPOSE**

- 1.1 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. 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 the University's overall security program.
- 1.2 This procedure applies to all university information resources managed by the University.
- 1.3 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 approved by the Information Security Officer and the Senior Vice President for Business Affairs prior to implementing alternate measures.

**2. DEFINITIONS**

- 2.1 Information Security Officer (ISO): The individual responsible for administering the information security functions within the University.
- 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 Descriptive data (e.g., logs): Information created by a computer system or information resource that is electronically captured and which 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.
- 2.4 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.
- 2.5 Information Resource Owner: An entity responsible for:
  - 2.5.1 a business function; and,

- 2.5.2 determining controls and access to information resources supporting that business function.

### **3. PROCEDURES AND RESPONSIBILITIES**

- 3.1 Prairie View A&M University departments shall maintain a list or lists 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 All users of Administrator and Special Access accounts must have account management instructions, training and authorization.
- 3.3 Each individual that uses Administrator and Special Access accounts must use the account privilege most appropriate for the work being performed (i.e., user account vs. administrator account) if two accounts are assigned.
- 3.4 Each account used for Administrator and Special Access must meet the Prairie View A&M University Administrative Procedure for Password Authentication.
- 3.5 The password for a shared Administrator and Special Access account must change when an individual with the password leaves the department, Prairie View A&M University, or upon a change in the vendor or contractor personnel with access to a Prairie View A&M University information resource.
- 3.6 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.
- 3.7 When Special Access accounts are needed for internal or external audit, software development, software installation, or other defined needs, they:
  - 3.7.1 must be authorized by the Information Security Officer and the Senior Vice President for Business Affairs;
  - 3.7.2 must be created with a specific expiration date;
  - 3.7.3 must be removed when work is complete; and,
  - 3.7.4 must be documented within the department, or with a Special Purpose AD Account Request Form from the Forms Library.

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