

Procedure 29.01.03.T1.03 (Effective 5/4/2006)
(Supplements [Rule 29.01.03.T1](#))

Information Resources – Administrator/Special Access

1. APPLICABILITY

This Standard Administrative Procedure (SAP) applies to all information resources managed by the University.

The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with the administrator's special access. 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 are to 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 SAP 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 (ISO).

The intended audience is all University staff responsible for information resources.

2. DEFINITIONS

1. 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 a computer system or systems. Examples of captured information are dates, times, file size, and locations sent to and from.
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.
3. Information Security Officer (ISO): responsible for administering the information security functions within Tarleton State University and reports to the Information Resources Manager (IRM).
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.

3. PROCEDURES

1. Tarleton State 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.
2. All users of Administrator and Special Access accounts must have account management instructions, training, and authorization.
3. Each individual that uses Administrator and Special Access accounts must do investigations only under the direction of the ISO.

4. Each individual that uses Administrator and Special Access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
5. Each account used for Administrator and Special Access must meet the Tarleton State University Standard Administrator Procedure Password Authentication.
6. The password for a shared Administrator and Special Access account must change when an individual with the password leaves the department or Tarleton State University or upon a change in the vendor personnel assigned to the Tarleton State University contract.
7. 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.
8. When Special Access accounts are needed for internal or external audit, software development, software installation, or other defined need, they:
 - must be authorized,
 - must be created with a specific expiration date, and
 - must be removed when work is complete

OFFICE OF RESPONSIBILITY: Department of Information Resources

CONTACT: Executive Director of Information Resources