Information Technology Services Administrator/Special Access Standard

Approved: February 11, 2020

Standard Statement

This standard applies to all information resources managed by Tarleton State University. The purpose of this standard 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.

Reason for Standard

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 standard 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.

Standards and Responsibilities

1. University departments shall maintain a list or lists of personnel who have administrator or special access accounts for departmental information resources systems. The appropriate department head, director, or their designee shall review the list at least annually.

2. All users of Administrator and Special Access accounts shall have account management instructions, training, and authorization.

3. Each individual who uses Administrator and Special Access accounts must do investigations only under the direction of the ISO.

4. Each individual who uses Administrator and Special Access accounts will use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).

5. Each individual who uses Administrator and Special Access accounts will use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).

6. The password for a shared Administrator and Special Access account must change when an individual with the password leaves the department or the university or upon a change in the vendor personnel assigned to the Tarleton contract.

7. When a system has only one administrator, there shall be a password escrow standard in place so that someone other than the administrator can gain access to the administrator account in an emergency.

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.

Definitions

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.

Information Resources: the standards, 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: responsible for administering Tarleton's information security functions and reports to the information resources manager (IRM.

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.

Contact Office

Information Technology Services
CIO of Information Technology Service
254.968.939