SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Administrator/Special Access on University Computer
SRSU Policy ID: APM 7.12
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: 8-16-2016
Next Review Date: 8-15-2021

PURPOSE:

The purpose of this policy is to provide a set of measures that will mitigate information security risks associated with IT Administrators/Special Access.

IT Administrators/Special Access is defined as users that have elevated account privileges. Therefore, these privileges must be restricted and granted only to those with an academic or business justification. Administrator accounts and other special-access accounts may have extended and overarching privileges. Thus, the granting, controlling and monitoring of these accounts is extremely important to the overall SRSU information security program. The extent of access privileges granted or used should not exceed that which is necessary.

SCOPE:

The SRSU IT Administrator/Special Access Policy applies equally to all individuals who have, or may require, special access privilege to a University computer.

POLICY STATEMENT:

Appropriate security levels and requirements must be determined for all special access accounts that utilize SRSU information technology resources. In order to safeguard information technology resources, the following controls are required:

1) All users of Administrative/Special Access accounts must complete the Local Administrator Access Form on the OIT website prior to authorization.

2) Each individual that has been granted an extended privilege account (e.g. –s, -a, -da) must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
3) Administrator access must not be used to remove administrator or system accounts from the administrator groups or add additional users as administrators.
4) When special access accounts are needed for audit, software development, software installation or other defined need, special access must be:

    a) Authorized by the system owner, Information Resource Manager, or Information Security Officer.

    b) Removed when no longer needed.

5) Periodic audits will be conducted by OIT security staffs for verification of

compliance.

6) Administrator access must not be used to install, freeware, open source, pirated/ unlicensed and file sharing software.

Related Policies, References and Attachments:

An index of approved policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available as part of Administrative Policy Manual.