Sam Houston State University
A Member of The Texas State University System
Information Technology (IT)

IT Administrator/Special Access: IT-18

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. 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. The granting, controlling, and monitoring of these accounts is extremely important to the overall Sam Houston State University (SHSU) information security program. The extent of access privileges granted or used should not exceed that which is necessary.

SCOPE:

The SHSU IT Administrator/Special Access Policy applies equally to all individuals who have, or may require, special access privilege to any SHSU information technology resources.

POLICY STATEMENT:

1. Appropriate security levels and requirements must be determined for all special access accounts that utilize SHSU information technology resources. To safeguard information resources, the following controls are required:

    a. All users of Administrative/Special Access accounts must have account-management instructions, documentation, and authorization.
    b. All users must sign the SHSU Non-Disclosure Agreement and be current on their annual Cybersecurity Awareness Training before access is given to an account.
    c. Individuals who use special access accounts must use the account privilege most appropriate with the work being performed (i.e., user account vs. administrator account).
    d. Each account used for special access must comply with the “Passwords” guidelines stipulated in the SHSU User Accounts Password Policy (IT-02).
    e. Shared accounts are allowed only with Information Security Officer approval.
        i. The password for a shared special access account must change when an individual with the password has a role change, leaves the department or SHSU, or upon a change in the vendor personnel assigned to the SHSU contract. The account must also be re-evaluated as to whether it should remain a shared account

or not.

    ii. A password escrow procedure must be in place so that individuals can gain access to a shared account in an emergency.

f. When special access accounts are needed for audit, software development, software installation or other defined need, special access must be:

    i. Authorized by the system owner, Information Resource Manager, or Information Security Officer. (E.g., IT@Sam Client Services is the system owner for all SHSU desktops, laptops, and tablets.)
    ii. Created with a specific expiration date or annual review date.
    iii. Removed when work is complete.

g. All privileged commands issued in association with special access must be traceable to specific individuals via the use of comprehensive logs.

REFERENCE:

There are many individual laws, regulations, and policies that establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant are listed in the Texas State University System (TSUS) Rules and Regulations, Rule III Paragraph 19 and associated TSUS IT Policies.

Version 1.02
Approved by: President's Cabinet, September February 6, 2012
Reviewed by: Heather Thielemann, Information Resources Manager, May, 2023
Next Review: May, 2024