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. 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 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:

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

1) All users of Administrative/Special Access accounts must have account-management instructions, documentation, training, and authorization.
2) All users must sign the SHSU Non-Disclosure Agreement before access is given to an account.
3) Each individual who uses special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
4) Each account used for special access must comply with the “Passwords” guidelines stipulated in the SHSU User Accounts Password Policy (IT-02).
5) The password for a shared special access account must change when an individual with the password 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. (Shared accounts must be kept to an absolute minimum.)
6) In the case where a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
7) 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. (E.g., IT@Sam Client Services is the system owner for all SHSU desktops, laptops, and tablets.)
   b) Created with a specific expiration date or annual review date.
   c) Removed when work is complete.

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

**Related Policies, References and Attachments:**

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at [http://www.shsu.edu/intranet/policies/information_technology_policies/index.html](http://www.shsu.edu/intranet/policies/information_technology_policies/index.html). Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, January 19, 2012
Approved by: President’s Cabinet, February 6, 2012
Next Review: November 1, 2014