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

User Accounts Management Policy: IT-01

PURPOSE:

The purpose of this policy is to establish standards for the administration of user accounts that access Sam Houston State University information technology resources. These resources must be protected from unauthorized access, loss, corruption, or destruction, thus ensuring the confidentiality, integrity and availability of these resources. Proper management of accounts provides a means of assuring accountability and protecting SHSU resources. The standards established in this policy include issuing accounts, granting access to approved resources, account maintenance and deactivation processes.

Scope:

The SHSU User Accounts Management policy applies to those responsible for the management of user accounts on Sam Houston State University information technology resources.

Policy Statement:

Creating unique domain user accounts is an automated process utilizing the current approved SHSU account naming convention and is based on assigned roles within the Banner system (e.g. faculty, staff, student worker, student, visitor, alumni, etc.) The level of authorized access will be based on the principle of least privilege (PoLP), but if a user is assigned multiple roles, the most privileged role will take precedence.

1. The creation of a user account issues a unique, non-transferable electronic identity known as the "username". Usernames will remain in effect throughout the individual's official affiliation with SHSU. (IT-S04 User Account Eligibility)
2. Usernames are not reused.
3. When an individual changes roles or ends their affiliation, IT@Sam has an automated process for deactivating user accounts that no longer meet SHSU's eligibility requirements (IT-S04 User Account Eligibility) and removing non-standard access.
4. Upon user activation, account holders are authorized to access the resources dictated by their role membership.
5. IT@Sam requires users to change passwords per IT-02 User Accounts Password Policy.
6. Requests for exceptions to this policy must be submitted in writing (IT@Sam Policy Exception Form) to the Information Security Officer (ISO) or Chief Information

Officer (CIO) and will be reviewed on a case by case basis. Requests shall be justified, documented, and communicated as part of the risk assessment process.

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. 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, VP for Information Technology, May 31, 2013
Approved by: President's Cabinet, September 16, 2013
Next Review: November 1, 2017