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

User Account Eligibility Statement: IT-S04

Sam Houston State University has created this User Account Eligibility Statement in order to clarify who can and will be granted rights and access privileges to SHSU information technology resources.

SHSU automatically authorizes an SHSU user account for any individual with an official affiliation as an employee (including faculty and staff as identified by Human Resources), retiree, alumni, and admitted or registered student (as determined by the Registrar). The following defines user account eligibility for Sam Houston State University. Exceptions may be requested by contacting the Information Resource Manager or Information Security Officer.

Definition of Affiliation:

    a. Student - A person who is attending classes, either online or classroom study, at Sam Houston State University. Student accounts will have access to appropriate campus file shares and email.
    b. Faculty - The academic staff, teaching either online or classroom classes, at Sam Houston State University.
    c. Alumni - A graduate or former student of Sam Houston State University that has completed greater than 15 credit hours.

Upon user activation, account holders are authorized to access the resources dictated by their role membership, for example:

    a. Faculty, staff, student workers, approved visitors, and student accounts will have access to appropriate campus file shares and email with designated quotas, appropriate file servers, personal website, wireless access, specific applications, and self-service functionality.
    b. Alumni accounts will have access to email with designated quotas and self-service functionality. File shares, file servers and personal websites are not available to accounts in this role.
    c. Retiree and limited visitor accounts will have access to email with designated quotas, personal websites and self-service functionality.   File shares other than the home drive (s:\) and file servers are not available to this role.
    d. Authorized custom accounts will be created according to specific needs.

All inactive accounts (accounts not being accessed, such as not logging in to a workstation or checking e-mail) will either be disabled or deleted (depending on the account type) after 180 days of inactivity.

Faculty, staff and student employee user accounts may change or be completely deleted due to, but not limited to, separation of employment, retirement, or extended leave. This can result in the deletion of data, such as e-mail or home drive (S:\) contents.

    a.   All data stored on SHSU information technology resources remains the property of the university.

    b.   It is the responsibility of the affected department to ensure that all SHSU department data is not stored on an individual's drive, but is stored on the T:\ drive or a shared directory.

    c.   It is the responsibility of the individual employee to archive incidental/personal data to removable media prior to separation.

    d.   Employee's individual email boxes and home drive (S:\) data will be retained for 5 months after account deletion and may be available for retrieval.

    e.   Users may contact the service desk at (936) 294-1950 or email HelpDesk@shsu.edu to initiate recovery services.

    f.   SHSU cannot guarantee recovery of individual files. Retrieval is dependent on management approval and storage capacity.

<u>Visitor and third-party accounts:</u>

A person who is not entitled to an account through SHSU affiliation but who is otherwise affiliated with the university through activities sponsored by a current SHSU faculty or staff member may obtain a visitor or third-party (vendor, contractor, support services) account.

Visitor and third-party accounts are termed accounts that must be requested and sponsored by a current faculty or staff member. The sponsor specifies an initial desired expiration date of one year or less as part of the request. Specifics pertaining to these accounts are:

    a.   Regular accounts (e.g., faculty, staff, and student) can be migrated to visitor account status if the sponsorship requirements are met.

    b.   Sponsors must request that visitor or third-party accounts be deactivated when the account holder no longer requires account privileges, or has completed the SHSU work for which an account was required.

    c.   The sponsor requests a visitor or third-party account by submitting an Account Request form on behalf of the individual seeking a visitor account. The sponsor's eligibility is verified (i.e. their status as current SHSU staff or faculty). The sponsor will receive an automated notification that the account will be deactivated unless the sponsor requests that it be renewed before the expiration date.

    d.   The sponsor is expected to remain in contact with the account holder to be able to respond to such reminders with an assessment of whether the account should be extended or not.

    e.   Without a request from the sponsor to extend the account beyond the expiration date it will automatically be deactivated upon expiration.

f. The sponsor is responsible for taking reasonable steps to ensure that the user account holder uses their account in accordance with IT@SAM policies.   If there are any problems with a visitor or third-party account, IT@SAM will contact the sponsor.

g. One or more limited visitor accounts are also available upon request by a current faculty or staff member via the IT@Sam Service Desk. These are numbered accounts that are reset per each checkout request and useful for conferences and seminars where attendees need computer access.

By default, only specific accounts will be listed in the SHSU directory and on the website.

a. Faculty/staff accounts are listed in the SHSU directory on the public website with information provided by Human Resources or the Registrar. This information will include email address, professional title, phone number, department, and room number.

b. Students have the option of suppressing their directory listing through the Registrar's Office.

c. Visitor accounts may appear in the directory at the sponsor's request with name and email information only.

To access restricted systems, services, or facilities, the account holder or sponsor must request authorization from the relevant data owner and/or data custodian.

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
Next Review: November 1, 2016