Sul Ross State University
A Member of the Texas State University System
Office of Information Technology
May 2019

User Account Eligibility Statement:

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

SRSU automatically authorizes an SRSU user account for any individual with an official affiliation as an employee (including faculty, staff and retiree) and student. Accounts for other affiliations such as contractors, auditors, visiting faculty and other officials are created on an as-needed basis. The following defines user account eligibility for Sul Ross State University. Exceptions may be requested by contacting the Chief Information Officer.

Upon activation, account holders are authorized access to resources based on their role as determined by the appropriate data owner or the data custodian. General guidelines for what resources are available are as follows:

a. Faculty (permanent, adjunct and emeritus), staff, and students have access to appropriate campus file shares (designated network shares), email and calendaring with designated quotas, appropriate file servers, personal website, wireless access, specific applications, and self-service functionality, so long as access to these services are appropriate to the needs of the university.
b. Retiree have access to email with designated quotas and personal websites.
c. Visitors to the campus are granted internet access through a wired or wireless access point via a guest SSID only.
d. Access to services by any other groups, including contractors, auditors, visiting faculty and other officials, is evaluated on a case-by-case basis.

All inactive accounts will either be disabled or deleted (depending on the account type) based on the following account retention schedule:

<u>Account Retention:</u>

Accounts for individuals that no longer have an association with SRSU are subject to the following retention schedule:

a. Employees – Employee accounts are created automatically once the employment record indicates the individual is “hired.” The account is deleted from the system 30 days from day of termination, unless the appropriate “retiree” designation is set in Banner, and all data associated with the account is no longer available to the terminated employee. Even if the retiree designation in Banner is set at termination of employment, access to institutionally-owned data is not allowed, unless requested by the affected department or Data Owner.

b. Retirees – Retiree accounts are created on an as requested basis based on information supplied by Human Resources in the Banner system. The PEAEMPL employee class is set to one of the Retiree values (typically, an RR) and will remain valid until the retiree requests the account be closed or the individual is deceased.
c. Students – Student accounts are created at the point of application to the university and remain valid for as long as the student has a record of enrollment in Banner. If a student has no such Banner activity during one long semester (fall or spring semesters), the account is deleted and all associated data is removed from SRSU systems and storage.
d. Others – on date specified by the sponsor

When an account is deactivated or removed from the system, all data associated with that account is also removed.

a. All data stored on SRSU information technology resources remains the property of the university after an account is terminated.
b. It is the responsibility of the affected department to ensure that all SRSU departmental data is not stored on an individual's drive, but is stored on a shared drive or directory.
c. All information is the property of SRSU and must not be removed unless specific permission has been given to do so and the data classification for that information has been considered before removing the data from SRSU. SRSU data that is classified as Sensitive or Confidential must not be removed from SRSU owned devices and should not be migrated to or stored on other systems. See the Data Classification Guide on the OIT website for more information on how to determine classification for data and who has the authority to do so.
d. SRSU cannot guarantee recovery of individual files. Retrieval is dependent on management approval and storage capacity.
e. Users may contact the Helpdesk at (432) 837-8888 or email techassist@sulross.edu for help on removing or deleting data from SRSU property.

<u>Third-party accounts:</u>

Third-party accounts, including contractors, auditors, visiting faculty and other officials, 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. Sponsors must request that third-party accounts be deactivated when the account holder no longer requires account privileges or has completed the SRSU work for which an account was required.
b. The sponsor requests a third-party account by submitting a request through LTAC on behalf of the individual seeking an account. The sponsor's eligibility is verified (i.e. their status as current SRSU staff or faculty).
c. The sponsor is expected to remain in contact with the account holder to assess whether the account should be extended or not.

d. Without a request from the sponsor to extend the account beyond the expiration date, the account is automatically deactivated upon expiration.
e. The sponsor is responsible for taking reasonable steps to ensure that the user account holder uses their account in accordance with SRSU policies. If there are any problems with a third-party account, OIT will contact the sponsor.

Requests for exceptions to this policy must be submitted in writing to the Assistant Vice President for Information Technology/Chief Information Officer and are reviewed on a case by case basis. Requests shall be justified, documented, and communicated as part of the risk assessment process.