PASSWORD GUIDE

Sul Ross systems that employ passwords for authenticating user identities shall comply with the following minimum password acceptability standards (complex password):

a. passwords must be case-sensitive;
b. passwords must be at least eight characters in length; longer passwords and passphrases are strongly encouraged;
c. passwords must include at least one character from each of the following four character sets:

    1. uppercase characters (A, B, C … Z);
    2. lowercase characters (a, b, c … z);
    3. numeric characters (0, 1, 2 … 9); and
    4. special characters or symbols (e.g., #, $, %, ^, &, -);

d. passwords may not include the associated LoboID or the LoboID owner's first or last name; and
e. The previous 4 passwords cannot be reused.
f. After 3 unsuccessful attempts to log in with an ID and password, the account must remain locked for a period of 5 minutes before accepting any further attempts to log in.

Password repositories must utilize one-way encryption and, once assigned, the password must not be retrievable by anyone. Thus, when a password is lost or forgotten, the existing password will not be retrieved but rather, a new password will be assigned.

Passwords must be changed at least once every 180 days. System owners and custodians may require more frequent password changes based upon risk assessment results.

OIT recommends that "Strong Passwords" be used on all systems that allow them. A strong password:

- Has at least 10 characters (phrases rather than words)
- Has uppercase characters, lower case characters, numeric characters and special characters or symbols (as noted above)
- Is not like your previous passwords
- Is not your name or login
- Is not a keyboard pattern, such as qwerty, asdfghjkl, or 12345678
- Is changed frequently
- Is never shared
- Is not used on another system
- Is easy to remember but difficult to guess