SIU Minimum Information Technology Security Guidelines

All users will be issued unique user-id(s). SIU does not condone the sharing of user-ids and passwords among faculty, staff or students.

The following are required for passwords with regular change intervals:

- Passwords must be a minimum of six characters in length.
- Passwords must contain at least two character classes (uppercase letters, lowercase letters, numbers or special characters).
- Password change history for University wide identifiers (user-ids) will be tracked for 6 iterations before allowing the same password to be utilized again by the respective user.
- Passwords will be changed at least every 60 days unless the additional password requirements for extended change intervals are followed.
- The following are prohibited as passwords:
    - User-id or reversal of the user-id
    - Name or reversal of the name
    - Words found in the dictionary or reversal of words found in the dictionary
- The number of invalid attempts an individual user is allowed to log into a secure service will be limited to ten (10) before access is denied. The user must request corrective action by the respective Information Technology Department or wait 20 minutes to attempt access.

The following are ***additional*** requirements for passwords with extended change intervals (i.e., those that are permitted to extend between 61 and 180 days.)

- Passwords must contain at least three character classes (uppercase letters, lowercase letters, numbers or special characters).
- Password change history for University wide identifiers (user-ids) will be tracked for 10 iterations before allowing the same password to be utilized again by the respective user.
- The following are prohibited as passwords:
    - Sequential keyboard patterns
    - Foreign words
    - Slang
    - Use of case change to disguise a word

- Any program(s) or script(s) utilized to validate University wide identifiers (user-ids) will be executed at least monthly.

- If there is no activity from the user's work station during the last thirty (30) minutes, the access authorization will automatically, if application/system controls are available, be revoked and the user must re-authenticate to access the system(s).

- Any access to information and resources should be limited based on the user's job function and duties.

    - Student, faculty and staff will, in general, be allowed access to appropriate secure services, based on job function, twenty-four (24) hours per day as long as they authenticate with the proper credentials.

    - Users will be allowed to log on to a single system multiple times or to multiple systems from the same work station as long as they authenticate each time and to each system using proper credentials.

- Account privileges, based on criticality and sensitivity, should be reviewed on a minimum of a monthly basis. Some accounts for non-critical resources, such as e-mail, may be reviewed less frequently (semester basis).

Approved:

Duane Stucky 11.24.09

Duane Stucky
Senior Vice President for Financial and
Administrative Affairs and Board Treasurer

Date