SOUTHERN WESLEYAN UNIVERSITY
P O L I C Y

Policy Title: Student Identity & Privacy in Distance Education	**Policy Number:** 13.17
Authority: Information Technology; SWU Global	**See Also:** • Authentication and Authorization Policy • Web Use Policy • Email Policy • SACSCOC Standard 10.6
Submitted: 8/14/2025 **Adopted:** 8/19/2025	

I. PURPOSE

Southern Wesleyan University (SWU) is committed to protecting the integrity of educational credentials awarded via distance education. The purpose of this policy is to outline SWU's procedures for verifying student identity and protecting student privacy in the digital/online learning environment, inclusive of all distance education programs and courses.

II. POLICY STATEMENT

In this policy, the term "distance education" refers to courses offered in a 100% online modality. The policy applies to all students participating in courses offered in a fully digital/online learning environment.

Access to network resources (including the Learning Management System) will be achieved by individual and unique logins and will require authentication. All student accounts are required to use Multi-Factor Authentication (MFA) when accessing university systems. This requirement is meant to strengthen identity verification and reduce the risk of unauthorized access. The privacy of student emails, usernames, and passwords are protected through a secured directory service.

III. PROCEDURES

SWU issues each student with a unique, six-digit identification number (ID) at the time of acceptance to the university. University employees also receive a unique, six-digit ID at the date of employment. Persons retain their unique ID number throughout their association with the institution (students who may later be employed by the university maintain the same ID number).

A SWU email account is issued to all students. A secure login that is unique to each user will be required to access the email. A login consists of a username and password combination. The school issues email is to be used as the primary method of communication among students, faculty, and staff.

This unique and persistent identifier is used by anyone who may have an educational or business need to access a service that requires Authentication. Authorization for services provided by the University depends on the individual's relationship(s) to the University and requirements associated with that role. In all cases, only the minimum privileges necessary to complete required tasks are assigned to a role. Privileges assigned to each role will be reviewed on a periodic basis and modified or revoked upon change in status with the university.

All students, regardless of their learning format, are assigned usernames and passwords. Unique usernames are created for each student. Separate unique and complex passwords are created for each student for (a) domain/email access; and (b) access to the Learning Management System (LMS), Canvas. The domain/email password and the LMS passwords may be the same for a given student but are typically different from each other.

Passwords must be changed by new users upon their first login. Passwords must be set according to the following history, length, and complexity rules:

- May not be any of the four (4) previous passwords
- Must be between 12 and 16 characters long
- Must contain at least three (3) of the following character types:
    - Uppercase letter
    - Lowercase letter
    - Numeric character
    - Special character (e.g. @, #, %, etc.)
- Cannot contain any of the following items associated with the email account:
    - Username
    - First Name
    - Preferred Name
    - Last Name

Once a password has been changed, it cannot be changed again within 24 hours.

Following four (4) consecutive unsuccessful network or email login attempts, the user account will be locked and will automatically unlock after fifteen (15) minutes. Users who are unable to recall their password may utilize the password reset links provided beneath the login fields.

All parties accept personal responsibility for the security of their passwords. Passwords must not be inserted into email messages or other forms of electronic communication without the use of encryption. Passwords should never be written down and left in plain

sight or stored in plain text online. Passwords should never be shared with anyone. Account owners will be held responsible for any actions performed using their accounts.

SWU protects the privacy of user passwords and usernames. Domain/email credentials are maintained in Microsoft Active Directory. LMS credentials are stored in a one-way hashed/encrypted format in the vendor database in the vendor's cloud environment. Passwords in Active Directory are stored using the NT hash (NTLM) algorithm and never saved in plain text. Similarly, student portal and LMS passwords are securely encrypted and hidden from view. All credential data is transmitted over HTTPS to ensure secure communication during login and password resets.

To access the LMS (Canvas), users use the secure login credentials (username and password) by which they access SWU's other digital resources. The combination of the user's username and password identifies students and faculty members to the system upon each visit. Student and faculty information is protected and separated from other users within the Canvas learning/teaching environment and from outside intruders. SWU considers all account login information, grades, and other student information as confidential.

Faculty members teaching in the digital/online learning environment will promote the security of students' personal data and course grades by utilizing the course management system grade book that (1) contains only students enrolled through the Student Information System (SIS) and (2) prohibits students from accessing other students' grades. Grades should not be posted in any manner that identifies students.

Many security features, such as those listed below, are provided within the LMS. Instructors are encouraged to utilize as many of these as necessary to ensure the safety, security, and integrity of student coursework.

- Question groups that randomize the selection of quiz questions for each student.
- Instructor-provided passwords for quizzes, tests, and other graded assignments.
- Time limits for quizzes and tests.
- Specified limit to number of quiz/test attempts.
- Automatic shuffling of questions and shuffling of multiple-choice responses between student quiz/test attempts.
- Browser security settings (lockdown browser) prohibiting access to other online sites and/or prohibiting printing during quizzes and tests.
- Limiting student access to quiz/test grades or to review of graded quizzes/tests until all submissions have been graded.
- Quiz/test item presentation options (one question per page, no returning to previous questions, etc.).
- Time delays between subsequent attempts of quizzes or tests that allow multiple attempts.

This policy will be widely available to university stakeholders through publication in SWU's policy manual and academic catalog. Distance education students will have consistent and regular access to this policy through their course syllabi.

The procedures contained in this policy will be regularly reviewed for accuracy and effectiveness.