

10.6.a

Distance and Correspondence Education: Student Identity Verification

An institution that offers distance or correspondence education:

- a. ensures that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit.

Judgment

Compliant Non-Compliant Not Applicable

Narrative

The University of South Columbia has systems in place to verify that the student who registers for a distance education course or program is the same student who participates in and completes the course or program and receives the credit. The University of South Columbia utilizes the University of South Carolina system-wide login and pass-code security system to verify that the student who registers in a distance education course or program is the same student who participates in and completes the course or program. Unique eight-character usernames are assigned to each student when they are accepted to the university. For security reasons, network username passwords expire every six months and must be renewed by the student. (The University of South Carolina Columbia does not offer correspondence study courses.) These systems are utilized to verify the identify of students who register for distance education courses or programs through both the University of South Carolina Columbia and the regional Palmetto College campuses and off-campus sites.

Initial Verification Process

In order to set up an account with the University of South Carolina, students and employees must first know their University of South Carolina ID, which is provided upon acceptance to the university or employment by the university. Using the [account claiming process via the my.sc.edu portal](#), individuals must enter their University of South Carolina ID, legal last name, and date of birth. They must then provide a personal email address that is used as an additional measure to verify identity. The personal email address will be sent a verification code to be provided before accounts are set-up with the university.

The initial verification of identify of students enrolled in distance education courses follows the same process as that of on-campus courses. In addition, many courses require proctored exams and student identify is verified at on-campus and approved off-campus testing sites and or via online test proctoring by checking the student's government issued ID or Carolina Card.

Continued Verification

The University of South Carolina takes all reasonable and industry-standard measures to verify individuals are who they say they are. These include multiple stages of admission application that produce reasonably verifiable personal data elements, which are used throughout the [student account claiming process](#). In addition to the centrally-issued Network Username and password, USC uses [Multifactor Authentication \(MFA\)](#) on its core applications and systems. The University of South Carolina requires users update/change their password every 6 months; this process entails verification questions (e.g. what city were you born in) and the use of a verified personal email address in order to initiate the password change process.

Verification of identity is a shared responsibility of the Admissions offices, University Registrar, and Division of Information Technology. The student-facing offices facilitate the entry of the individual to the institution, including initial gathering of personally identifiable information (PII), and official maintenance of the individual's record, including contact information and other sensitive data. IT administers the technology components of identity management, account claiming, password change, user authentication services (CAS and Shibboleth), MFA, and technical support.

Verification via third-party platforms

Blackboard®, the platform for delivering all University of South Carolina system course content material, meets or exceeds standard mass notification security requirements. Specifically, Blackboard® course access requires a unique login and password for all users, and only students registered for the course can access the content. The "Course Statistics" feature tracks when items in Blackboard® are accessed. In 2020, the University of South Carolina will evaluate opportunities to place multifactor authentication in front of Blackboard to augment security and confirm identity of users.

The University of South Carolina Columbia provides optional test proctoring service for distance education courses. Course instructors can choose to use these services for any or all of their courses. The services provided through the Office of

Distributed Learning include one of the following three options: 1) a face-to-face test proctoring center with individual testing stations and observation camera-support proctoring, 2) coordination and certification of face-to-face test proctoring services throughout the state and nation, and 3) online test proctoring through ProctorU. In addition, the online test proctoring service Respondus Monitor is integrated into Blackboard. With each service, students are required to provide government-issued photo identification.

The university is [contracted with ProctorU](#), a leading company for online proctoring of exams and tests. A live proctor verifies the user's identity by comparing the student taking the exam to the student's government or university issued ID, ensures the exam environment is secure, and provides any technical assistance needed prior to the start of the quiz, test, or exam, and then the testing session is recorded and reviewed by a certified proctor. In courses where online proctoring is used, students have the ability to use their own webcam-equipped computer connected to the internet to connect with the ProctorU. The entire testing experience, including authentication, room security check, and execution of the test experience is recorded and reviewed by proctors employed by ProctorU. In the event of a potential cheating or exam procedure violation, faculty are sent links to time coded video of the potential incident for their review and action with the student. In courses where online proctoring is offered, it is not mandatory; therefore, students have the option to be proctored face-to-face at the Office of Distributed Learning's testing center or at one of the university's approved statewide or national testing centers. For students who choose to use ProctorU, a \$8-14 fee per exam (based on the length of the exam) is paid by the student directly to the vendor. The University of South Carolina Board of Trustees approved this fee in June 2018 and the University of South Carolina Columbia websites and course syllabi were updated to reflect the possible fee for proctored tests. The [Office of Distributed Learning](#) webpage provides information about test proctoring options and states:

"The secure online proctoring service, ProctorU, lets you schedule exam times and locations that fit your schedule. ProctorU verifies your identity and records your testing session. Each testing session is reviewed by a certified proctor to ensure integrity. You will be required to pay an \$8-14 fee for online proctoring, depending on the length of the exam, directly to ProctorU during your exam. You must also have access to a computer with a webcam and reliable internet connection to use ProctorU."






The University also [has a contract with Respondus for Monitor](#) for online test proctoring. Monitor provides automated exam proctoring and enables students to take assessments within Blackboard. After a one-time installation of a plugin, each student follows a startup sequence that guides them through completion of requirements set by the instructor (these requirements are entered when you set up your assessment in Blackboard). Monitor requires students to take a picture of a their government or university issued ID, records each student's session for later review, and applies monitoring algorithms to notify instructors of the timestamp of any suspicious activity for their review. This product is integrated in Blackboard, and available for use at no cost to students, instructors, or academic departments.

Data Management

The University of South Carolina Columbia's secure data management infrastructure is comprised of four main systems, each requiring independent login created and maintained by students. These systems consist of (a) network login (wired/wireless); (b) Banner® student intranet data system accessed through the [One Carolina portal](#); (c) Blackboard® course content management system; and (d) Microsoft® Outlook Live student email system. Each of these systems, working in tandem, provides assurance of network security including student identity. Students can view their IDs and [change passwords](#) via the One Carolina portal only if they know their current password or identifying information. Duo is a multifactor authentication (MFA) solution which is sometimes referred to as two-step or two-factor authentication. The university's license for Duo also [includes students](#). Duo adds an additional layer of protection to accounts and the data accessed through them.

The University Registrar is responsible for ensuring compliance with student identity security policies and procedures. [STAF 6.25 Academic Responsibility - The Honor Code](#) requires students to "adhere steadfastly to truthfulness and to avoid dishonesty, fraud, or deceit of any type in connection with any academic program". This honor code prohibits students from allowing another individual to access or complete their online coursework. University policy [UNIV 1.52 Responsible Use of Data, Technology, and User Credentials](#), stipulates that all individuals and organizational units that use or access data, technology, and user credentials must comply with state and federal laws. The policy defines what is considered university assets, policy statements that all employees must agree upon, and how consumable software and devices should be destroyed when they are retired from use.

Sources

-  [Homepage for my.sc.edu](#)
-  [MFA for Students](#)
-  [Mutifactor Authentication](#)
-  [Office of Distributed Learning - Proctoring](#)
-  [Password Changes via my.sc.edu](#)

-  ProctorU Contract
-  RESPONDUS Monitor Contract
-  STAF 6.25 Academic Responsibility - The Honor Code
-  Student Account Claiming Process
-  UNIV 1.52 Responsible Use of Data, Technology, and User Credentials