Southern Association of Colleges and Schools
Commission on Colleges
1866 Southern Lane
Decatur, Georgia 30033-4097

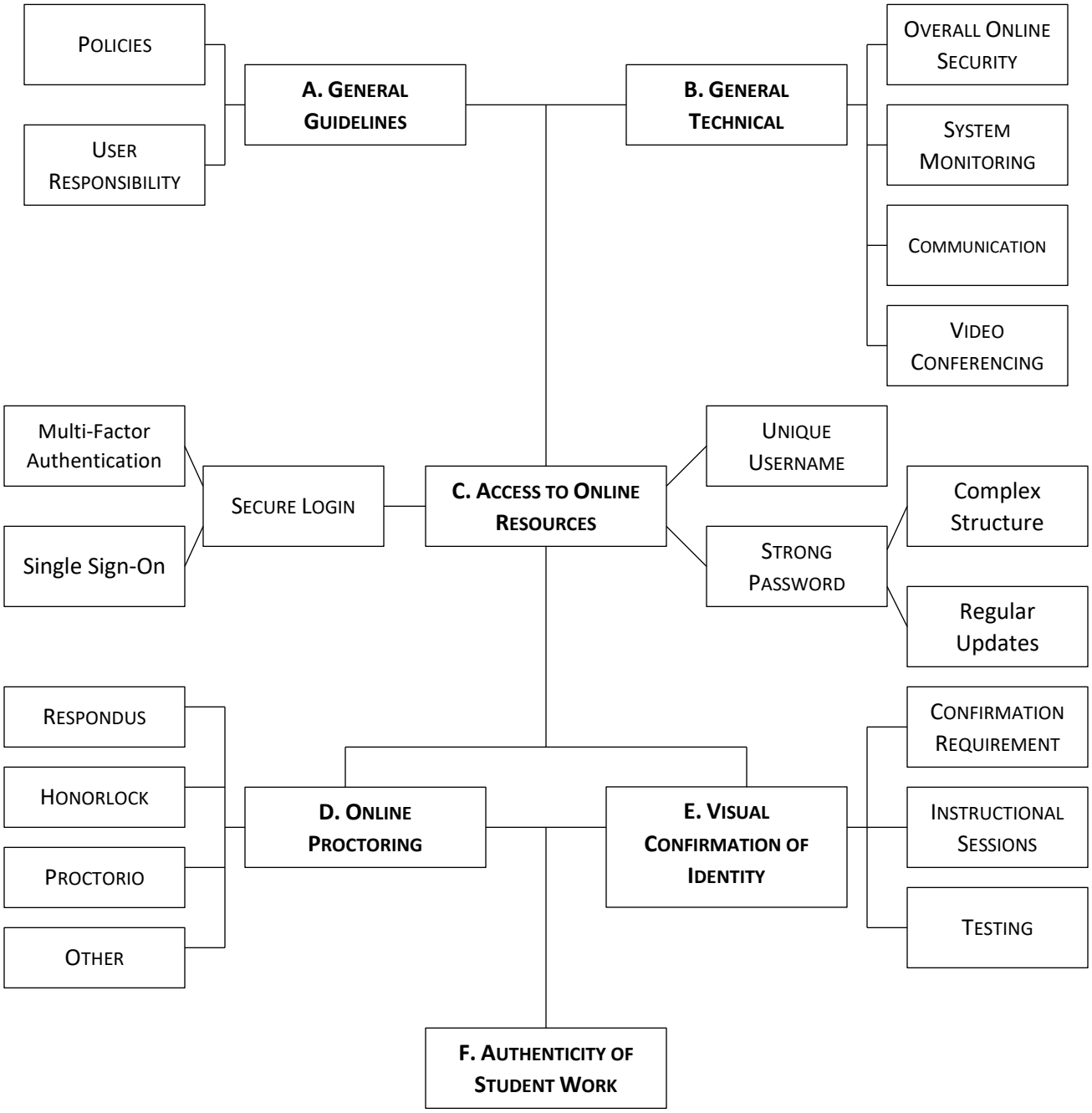
STUDENT AUTHENTICATION IN ONLINE LEARNING

Good Practices

In Fall 2020, SACSCOC developed and administered a comprehensive survey to understand how member institutions address complex challenges associated with the advent of the COVID-19 pandemic. Responses were received from more than **490** colleges and universities, which account for approximately 63% of the overall SACSCOC institutional membership.

Since the initiation or significant expansion of distance learning was an immediate and very common response to the pandemic, one of the survey questions asked respondents to **outline key approaches that their institutions take to ensure student authentication in online and/or hybrid education environments** (re: SACSCOC standard 10.6 (a).)

This document provides a visual summary of the preliminary content analysis of survey responses on the student authentication question as well as selected *sample* direct quotes to illustrate multiple and varied approaches that SACSCOC member institutions developed and implemented to ensure that students are properly authenticated in the distance education contexts.


Policies
User Responsibility
A. General Guidelines
B. General Technical
Overall Online Security
System Monitoring
Communication
Video Conferencing
Multi-Factor Authentication
Single Sign-On
Secure Login
C. Access to Online Resources
Unique Username
Strong Password
Complex Structure
Regular Updates
Respondus
Honorlock
Proctorio
Other
D. Online Proctoring
E. Visual Confirmation of Identity
Confirmation Requirement
Instructional Sessions
Testing
F. Authenticity of Student Work

A. General Guidelines

Policies

- The institution's Password Management and Use policy sets clear standards for protection of passwords used to access any of the systems used by the University.
- The University's Responsible Computing Policy addresses the privacy and security of electronic correspondence and data and provides guidelines on choosing and maintaining a secure password.
- Students sign a computer use policy that prohibits sharing of their ID and password.
- Students receive the IT Security Policy, which requires "protection from unauthorized, inappropriate, and/or accidental access" of information. As part of their application to any online program, students must acknowledge that they have read and reviewed the technology requirements of the university and program. Students check a radio button in the application to signify agreement.
- The University's distance learning policy defines expectations for maintaining academic integrity, including requiring secure logins and passwords for the learning management system, proctoring for examinations, and appropriate steps to verify the identity of the student participating in the distance learning course.
- [Institution's] "Policy on Identity Authentication in Online Classes" requires that every online course include a clear and actionable plan for verifying the identity of every student enrolled in the course, a plan which must be approved by the Vice President of Academic Affairs (VPAA) and the Director of Online Education. The purpose of this policy is to ensure that the person who receives the credit for the course is the same person who did the work for the course.

User Responsibility

- Each online student is required to take an online orientation course through Moodle, the institution's learning management system. One part of this orientation educates students on the institution's Honor Code, and each online student is required to check that they have read and agree to abide by this Honor Code.
- Through the [Institution] website, new student orientation, and the [Institution] Distance Education LMS, [Institution] informs students of the secure login method and instructs students not to share their login and password information with others for security and student privacy reasons.
- Policy requires that users do not share their account credentials, so by policy whomever has the account should be the owner. The account holder is also made responsible for protecting and reporting compromises of their account by policy as well.
- [Institution's] Identity Access Management Policy indicates the responsibility of users to secure their passwords. If students are found to have shared their password, the academic integrity policy … is then used to address the students' failure to abide by the Identity Access Policy.
- All faculty, staff, and students, must agree to our user account terms and are susceptible to severe penalties and possible criminal prosecution for agreement violations such as sharing one's password with anyone for any reason, falsifying one's identity on any university system connections, and/or not abiding by all [Institution] policies, as well as all relevant federal, state and local laws.

B. Overall Technical Considerations

Online Security

- All online activities are conducted behind our firewalls.
- Access to student information is protected from unauthorized external access by a firewall between the internet service provider (ISP) and the college network.

- All online services are encrypted to prevent attackers from capturing data between the student's device and campus.
- All [Institution] applications use Secure HTTP (HTTPS).
- [Institution] utilizes Secure Sockets Layer (SSL) certificates to establish an encrypted link between the web server and the client's browser. This link ensures that all data passed between the web server and web browser remain private and integral.
- 128-bit encrypted secure login and password approach.

System Monitoring

- [Institution's] computer services team receives and stores a record of all login attempts made on all students' accounts that includes the IP address of the browser that was used for the login attempt, the location of the attempt and other relevant information that can be used for investigative purposes in the event of a data breach.
- Authentication-related security events are logged in within the security events framework. These report log events include: • Authentication - events such as login, logout, authentication failure, session expiration, and usage of privileged command-line authentication tools. • Input Validation – events that indicate potential violations of specific security rules designed to protect Blackboard Learn. • Security Validation – events that track configurable rules to protect Blackboard Learn and provide the first defense line.

Communication

- We require students to correspond with faculty only via their official college email.
- All course communication is done through the [LMS] course or College student email.
- [Institution] faculty solely use university owned and managed secure authenticated systems to communicate with students.
- To ensure communications are being made directly with the enrolled student, faculty and staff conduct electronic communications to and with students using the College-issued email account that is accessed with the unique G# login assigned.
- Students are REQUIRED to use their [LMS] canvas account or their [Institution] email account for all electronic communication. To ensure the identity of the student communicating electronically, [Institution] faculty and staff will not reply to student communication that is sent through an email account other than their [Institution] issued email account or [LMS] account.

Video Conferencing

- Zoom sessions require passwords.
- The College requires students to use their full name and to be present on camera for the duration of the course.
- Faculty may hold students in a virtual "waiting room" to ensure student authentication prior to beginning a synchronous class meeting.
- The university provides Zoom FERPA guidelines for faculty and students who utilize the technology in the university courses. The purpose of these guidelines is to validate but also protect student identity and abide by FERPA while participating Zoom meetings.
- [Institution] … integrated the Zoom conferencing system into [LMS] which adds three layers of security for both authentication and privacy as it prevents links of synchronous sessions (and the corresponding recordings) from being viewed outside of the [LMS] site.

C. ACCESS TO ONLINE RESOURCES

Secure Login

Multi-Facto Authentication

- [Institution] uses two-factor authentication to provide additional security for the individual's username and password.

- [Institution] requires a second factor (multifactor authentication) to access enterprise applications including the learning management system
- All students are required to use multifactor authentication when using a single sign on for student email, [SIS] access, and [LMS] access that involves verification codes being texted to the student's cell phone.
- The university uses multi-factor authentication for all online systems. In this process, users must provide additional confirmation of their identity through something they possess (e.g. a cell phone, tablet or hardware token) to submit an additional verification of identity at login.
- Multi-factor authentication protects student's accounts via Microsoft Azure; students have multiple options for enrolling, such as by using the Microsoft Authenticator mobile app, and can set multiple authentication methods (such as text messages).
- [Institution] implemented DUO two-factor authentication for students. DUO integrates with SSO-enabled applications to verify a student's identity by using a second factor in addition to a password, such as a phone call or an emailed passcode. This prevents anyone other than the authorized user from logging into university accounts, even if they know the password. With DUO, students log in as usual with their *** ID, and then use a personal device, landline, tablet, or a FIDO Certified U2F token to verify their identity by responding to a push notification on a mobile app, entering a passcode received in a text message, or answering a phone call.
- Instructors can also use BIO SIG ID to verify student identity.
- BioSig-ID provides an added layer of authentication to ensure that the person completing the coursework is the student who is registered for the class.

Single Sign-On

- The [LMS] system integrates with the College's authentication services to ensure appropriate and secure student access to courses and other Student Information Systems.
- All Students and Staff are issued Microsoft Active Directory accounts to authenticate against internal, hosted and cloud solutions. Rights to specific files and functions are based on Active Directory Group Membership.
- The primary method of identification is the secure One Identity Password Manager that uses a Lightweight Directory Access Protocol (LDAP) connection to ensure securely managed accounts across all campuses.
- Online courses are managed through the [LMS] which has Single Sign On (SSO) Security.
- A Single-Sign-On system with two-factor authentication is used for accessing the learning management system and other remote student tools and platforms.
- Students use single sign-on (SSO) services to access the institution's LMS, student information system, and academic and student support resources.
- The College has implemented Single Sign On for all software that supports it, including our ERP, LMS, Email and other systems.
- Single Sign-On (SSO) is the protocol used to authenticate students across various systems, such as [LMS], [SIS], *** Web, Microsoft 365, Microsoft Outlook email, and DegreePlanner. Using SSO, our students can log in with a single ID and password to gain access to multiple connected systems. This assists students by allowing them to access different systems seamlessly.

Unique Username

- Login identifiers are only provided to students who have been properly registered and who have been approved to participate in online courses by the respective academic school/program.
- The format used in creating a student's username is their first name initial + full last name + the last 3 digits of their Social Security Number (SSN).
- At the time of initial registration, all students are issued a unique eight-digit student identification number. This student ID becomes the unique identifier for students

throughout their academic career at the university. The student ID differs from the student's social security number, which is not used for academic activity, either online or in-person.
- Students are assigned a unique student identification number, a student email address, and unique student login to the learning management system.
- Students are assigned a unique identification (ID) number when they enroll at the college. They must use this student ID to log into the college's single sign-on platform to access their online courses.
- As part of the admissions process, college systems generate an account for each student with a unique user ID, which provides access to the online student information and registration system (***), the learning management system (***), and student email. The student activates their account by entering multiple pieces of personal information (such as student ID number, birth date, zip code), which are verified against college records, and by creating a private and secure password.
- The username is specific to the student and is used in Secure Sockets Layer (SSL) secured login portals to identify the student to the student information system, as well as the [Institution] Learning Management System.

Strong Passwords

Complex Structure

- At initial login, students reset password based on requirements and verify identity using 2-factor authentication.
- Passwords must meet a set of criteria which ensures a standard level of security is met. Passwords must have a minimum of 12 characters, cannot contain the username, cannot contain 3 consecutive characters of the given name, and must have at least one lowercase letter, one uppercase letter, one number and a special character.
- Students are instructed to use the Enroll feature in the password management software to setup security questions for an added layer of security and privacy.
- The institution's systems mask passwords as they are entered; and, if an error is made in typing a username or password, the system does not reveal to the user which item was incorrect

Regular Updates

- [Institution] students are assigned a unique [Institution] username and maintain a password that must be changed at 6-month intervals.
- Students are required to change their passwords every 180 day.
- Every student has a unique login password which changes on a 90-day cycle.
- Passwords can be reset by students at any time if they feel their credentials have been compromised.
- If a student forgets their password, they can recover their account and set a new password if they can answer 3 of 5 (randomly selected order) student-created security questions. These questions are required to be created at first login.

D. Online Proctoring Applications

Respondus

- Instructors can require the use of Respondus LockDown Browser and Respondus Monitor. Respondus LockDown Browser is a secure browser for taking tests in Canvas. It prevents a student from printing, copying, going to another URL, or accessing other applications during a test. Instructors may also use Respondus Monitor, a companion product for LockDown Browser that enables institutions to protect the integrity of non-proctored off-campus online exams.

- Implementation of Respondus, an online proctoring service, has been instituted across all courses. This service verifies student identity by recording students while taking exams. It also utilizes a lockdown browser to ensure integrity of the student's work.
- Respondus Lockdown Browser is a custom browser that locks down the testing environment within our Canvas Learning managements systems and does not allow students to view other information while taking a test. Respondus Monitor builds on the power of LockDown Browser, using a student's webcam and video analytics to prevent cheating during non-proctored exams.
- We provide students and faculty with links to instructions and recordings for how to use Respondus Monitor and Lockdown Browser.

Honorlock

- Honorlock system with safe scan and visual presentation of ID.
- The University uses the trademarked Honorlock system for on-demand, web-accessible, remote exam proctoring that monitors and records student exam sessions using a webcam with microphone.
- The college's online test proctoring platform, Honorlock, provides another layer of student authentication. Before students enter an exam, Honorlock requires them to present picture IDs that are verified with students' names. A snapshot is taken of the student as well. Once students are allowed to enter the system and start the exam, the entire session is video recorded, which includes the student and the student's screen. The software flags any other person who might enter the view. If a student's authentication is in question, faculty and staff can review the videos to ensure the student is truly the authorized student.

Proctorio

- We are using Proctorio to ensure integrity in online testing.
- We have purchased an institutional license for Proctorio for multi-factor identity verification, exam monitoring, and administrator-controlled examinations.
- The institution requires that all asynchronous online courses have proctored exams using the web proctoring tool Proctorio. Proctorio authenticates the identity of the test taker and captures the entire exam session by utilizing the student's webcam and mic in a recording which is later reviewed by the instructor.

Other

- We use *ProctorU* for student authentication and testing.
- *ProctorU* will be added to the toolbox this semester to provide proctoring for higher stakes testing.
- We … also use *Examity* in select courses.
- Student authentication in the online environment continues through our use of *XProctor* by faculty to verify student identity and ensure academic integrity.
- Also have begun using SmarterServices and is piloting *SmarterProctoring* this fall.
- [Health sciences] departments … use proctoring companies like *ProctorU*, *ExamSo*ft and *RPNow.*
- Using CARES money, we are establishing a virtual proctoring service in-house for our faculty.

E. Visual Confirmation of Identity

Confirmation Requirement

- Weekly synchronous requirement for each hybrid and blended course.
- The college requires at least one proctored activity in each online course.
- Each distance education course requires a minimum of one proctored assignment/ examination to validate student identity.
- A faculty member must require a video proctored final exam.

- The College requires all online courses to offer an identity verification assignment each semester. This assignment can vary from a proctored exam, synchronous or asynchronous video presentation, or synchronous video interaction.

Instructional Sessions

- Identities are verified via Zoom through facial recognition.
- Asking students to use video feed during virtual class meetings.
- During synchronous class meetings via Zoom or Microsoft Teams, students must at least momentarily enable the video function of the platform to allow an instructor to confirm the students' identities.
- All students use webcams to prove their identity. While faculty may not expect them to always keep it on, they do require periodic check-ins by webcam or smart phone.
- The requirements for students to indicate 'present' on the Zoom chat as well as the rule to be 'on camera' for the class duration.
- The camera must be able to see their face and their desk.
- [Students] must have a camera on for faculty to log attendance with sight recognition to the photo loaded into the SIS.
- Student photos from their ID cards are part of the class roll for each course. Faculty may verify that course and exam participants match the photo id.
- All students enrolled at the college receive a photograph ID card. This photograph is stored in the [LMS] integrated database. … Instructors have access to student photographs through the [LMS] integrated database, verifying that the student who signed up for the course does indeed match the student seated in the virtual classroom.

Testing

- The pre-approved identity authentication plans include … an oral examination through video-conferencing software. … Oral examinations are to include live video as well as the presentation of a valid state-issued ID.
- The remote-proctoring software for online exams in the LMS requires the students identify themselves on the camera with a photo-ID, which also records them throughout the taking of the exam with artificial intelligent software seeking suspicious behaviors.
- Students are required to present a government-issued photo ID via webcam for each Honorlock-proctored exam session.
- Respondus Monitor asks for the student's ID and records the image of the student's face to verify identity.

F. AUTHENTICITY OF STUDENT WORK

- TurnItIn monitors student submissions for plagiarism when implemented with an assignment.
- The College has made effective use of software that protects against plagiarism (Turnitin).
- [Institution] has embedded anti-plagiarism software and proctoring tools inside numerous online/hybrid courses. These tools provide faculty with important feedback around how, and where, an instance of academic dishonesty might have occurred.
- We also redesigned assessments to reflect a digital environment that would be difficult to complete in a dishonest fashion.
- Some faculty have moved to other forms of student assessment including oral presentations and oral exams.
- Randomized test questions and shortened testing time are used to deter cheating and plagiarism.

Document History

Adopted: SACSCOC Board of Trustees, June 2023