Webber International University

Florida, North Carolina, and South Carolina Campuses

Distance Education: Verification of Student Identity	Approval Date: January 2012
	Approved By: Joint Institutional Planning Committee Florida Faculty: April 28, 2014 North Carolina Faculty: May 9, 2014
Standard 10.6a (FR 4.8.1)	Reviewed and Reaffirmed: February 25, 2014 (JIPC) July 20, 2021 (JIPC)

Reference:

Standard 10.6a: An institution that offers distance or correspondence education "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."

Policy

In compliance with SACSCOC Standard 10.6a, it is the policy of Webber International University, at all campuses/locations, to ensure 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 credit. It ensures this by verifying each student's identity.

At Webber International University, and at all campuses/locations, the primary and preferred method of verification is through the use of a secure login and pass code. In addition to being an effective and accepted means of verification of student identity, this option does not normally require that a student be burdened with any additional charges related to verification of identity.

In order to ensure protection of the usernames and passcodes, the following mechanisms are in place:

1. By Default, Citrix user logon is encrypted using RC5 (Rivest Cipher) this is 128-bit encryption that protects the users who are logging into Citrix.

2. Citrix NetScaler is the first line of Firewall that operates from L4 to L7. This virtual appliance sits between the clients on the internet and the Web server farms and protects against known and unknown threats by employing a hybrid security model, blocking all the traffic and allowing good traffic to come through.

3. All users must contact the IT department to reset their passwords. For security purposes, the User must present his/her first and last name and a personal identification number. In addition, passwords must have 12 characters and two special characters before password reset is implemented.

4. For emails, a 2- step verification for the users to logon to their email account is in place.

5. All Microsoft email accounts permit users access to block phishing when suspected.

Implementation responsibility: Academic Affairs
Policy review cycle: At least every three years
Compliance: Mandatory