BUFFALO STATE COLLEGE

DIRECTORY OF POLICY STATEMENTS

Policy Number: IV:07:02   Date: Fall 2016

Subject: **Student Identity Verification of Online Learning Activities**
                      (formerly Student Identity Verification in Distance Education Courses)

This policy applies to all credit-bearing courses including distance education courses or programs offered via the campus-supported learning management system (LMS).

The Higher Education Opportunity Act (HEOA) requires that institutions offering distance education courses or programs have processes in place to ensure that the student registering for a course is the same student who participates in the course or receives course credit. The HEOA requires institutions to verify the identity of a student who participates in class or coursework by using methods such as the following:

- A secure log-in and pass code

- Proctored examinations

- New or other technologies and practices effective in verifying student identity

Compliance
Students are required to log in to the LMS using campus-assigned credentials, issued at the time the student first acknowledges admission to Buffalo State. Enrollment information is passed from the campus student information system (SIS) to the LMS to ensure that students have access to all (and only those) courses in which they are enrolled.

Student Identity Verification
The student username and password is the network authentication security measure. All students are provided a network username and password for secure access to information systems including the LMS for distance education. Students activate their network username and password through the identity management process embedded within the SIS. Upon the first log-in, students must create their own unique password. The new password must be at least six but no more than 14 characters long, and is case sensitive. Security suggestions include the following:

- Use a combination of upper- and lowercase letters, numbers, and special characters.

- Avoid using dictionary words; these are easily cracked.

- Avoid using names of people you know, or names of pets.

- Avoid using your phone number or street address.

- Avoid using your Social Security number.

Password resets are accomplished through the identity management process embedded within the SIS that requires its own unique password.

Protection of Student Privacy
All processes related to the verification of student identity are protected by automated internal processes to defend against intrusion. These processes adhere to the information security guidelines established by SUNY, the State of New York, and FERPA regulations and are regularly audited.
Charges Associated with Identity Verification
There are no additional fees to students associated with identity verification.

Responsibility for Identity Verification
Computing and Technology Services is responsible for the consistent application of the automated processes related to student identity verification.

Student Responsibility for Safeguarding Credentials
Students are responsible for safeguarding their student accounts and for all activity associated with those accounts. Sharing of log-on credentials with anyone other than the registered student completing the coursework is considered a violation of the Academic Misconduct Policy.

Computing and Technology Services
Fall 2012

Revision - Online Advisory Committee
Spring 2015 - April 29, 2015

Revisions - Committee for Online Strategic Enrollment Planning (COSEP)
Fall 2015 - September 24, 2015