Verification of Student Identity in Distance Education

I. SCOPE

This policy applies to all credit-bearing distance learning courses and programs offered by Muhlenberg College, beginning with the application for admission and continuing through to a student's graduation, transfer, or withdrawal from study.

II. POLICY STATEMENT

All credit-bearing courses and programs offered through distance learning methods must 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 academic credit. One or more of the following methods must be used:

A. A secure login and password
   Each Muhlenberg student is assigned a unique student id and password to login to a number of Muhlenberg's systems. These include the learning management system (Blackboard) and student information system (SIS). The student is instructed to keep this ID/Password personal and confidential per the Muhlenberg College Policy on Electronic Communication and Internet Access.
B. Proctored examinations; use of essays, in-person exams, and other activities that require face-to-face interaction by faculty that minimize the possibility of academic dishonesty; and/or
C. New or emerging technologies and practices that are effective in verifying student identification.

All methods of verifying student identity in distance learning must protect the privacy of student information.

Personally identifiable information collected by the College may be used, at the discretion of the institution, as the basis for identity verification. For instance, a student requesting that their Blackboard (LMS) be reset may be asked to provide two or more pieces of information for comparison with data on file, or to come to the OIT Help Desk in person with a BergID card or other verification. In the same way, a student requesting that their Capstone (SIS) password be reset may be asked to provide two or more pieces of information for comparison with data on file, or to come to the Registrar's Office in person with a BergID card or other verification.

III. RESPONSIBILITIES

All users of the College's learning management systems are responsible for maintaining the security of usernames, passwords, and any other access credentials assigned as per the Policy on Electronic Communication and Internet Access and the Family Educational Rights and Privacy Act. Access credentials may not be shared or given to anyone other than the user to whom they were assigned to for any reason. Users are responsible for any and all uses of their account. Users are held responsible for knowledge of the information contained within the most recent College Catalog as well as the Student Policy and Resource Guide. Failure to read College guidelines, requirements, and regulations will not exempt users from responsibility.

Students are responsible for providing complete and true information about themselves in any identity verification process.

Faculty teaching courses through distance education methods hold primary responsibility for ensuring that their individual courses comply with the provisions of this policy. Faculty are responsible for informing the Associate Dean of Digital Learning of any new technologies being used to verify student identity, so that published information on student privacy can be maintained appropriately, and so that the College can coordinate resources and services efficiently. Because technology and personal accountability may not verify identity absolutely or ensure academic integrity completely, faculty are encouraged, when feasible and pedagogically sound, to design courses that employ assignments and evaluations unique to the course and that support academic integrity.

Department Chairs, Program Directors, and the Associate Dean of Digital Learning are responsible for ensuring that faculty are aware of this policy and comply with its provisions.

The Provost is responsible for ensuring College-wide compliance with the provisions of this policy and that Deans, Directors, and the Associate Dean are informed of any changes in a timely fashion. The Provost is responsible for publishing College-wide information on how identity verification processes protect student privacy, and is also responsible for coordinating and promoting efficient use of College resources and services, and for ensuring that College level processes also remain in compliance with this policy.