# Student Authentication Policy Report - Oct 10, 2013

Survey: CCC Chancellor's Office 2011-12 Annual Distance Education Survey

## 7. Does your district have a Board of Trustees approved student authentication policy?

|  |  |  |
| --- | --- | --- |
| **Value** | **Count** | **Percent** |
| Yes | 25 | 23.2% |
| No | 84 | 77.8% |

|  |  |
| --- | --- |
| **Statistics** | |
| Total Responses | 108 |

## 8. Description of Policy-Policy Summary

|  | |
| --- | --- |
| **Count** | **Response** |
| **1** | A federal mandate appeared in the reauthorization of the Higher Education Opportunity Act in 2008 that requires faculty to have students sign into courses using identification provided by the college. Interpretation of the language in the Act shows a governmental concern that students taking MSJC online courses are the students enrolled in them. The changes require MSJC to have student’s complete tests and quizzes in the Blackboard system. Faculty can no longer use their own websites to accomplish testing even if the students log into the site. MSJC will be held accountable through the accreditation process. The only exception is when faculty are using publisher content that requires students to purchase a key and log in, since students have to login through MSJC. Academic Integrity It is a requirement for MSJC faculty to define cheating and plagiarism in course documentation and syllabus. Faculty should have a link to the technology acceptable use policy and student conduct policy. Very often community college students do not understand what plagiarism means. A recommended method would be to hold a discussion forum asking students to write what it means to plagiarize. It should be made clear in the course content that the topic should be course specific. The following link would serve as a good example: Rutgers – Interactive Plagiarism Video, Real Life Examples, and Quiz and How to Avoid Plagiarism Online. Faculty can assist students to be ready to take an online class, which will help with online course retention rates. It is recommended that faculty have students take a student readiness self-test. Links to the three student readiness quizzes are provided, in the DE Faculty Handbook. |
| **1** | Policy has been drafted and is about to be approved by the Chancellor's Cabinet and then it will go to the Board of Trustees. Board Policy 4014. The first paragraph reads: To ensure the integrity of the Distance and Correspondence Education offerings and comply with federal regulations (34 CFR§602.17g) and ACCJC policies, each college will ensure student authentication to Distance and Correspondence Education classes using the unique student ID and password issued by the Contra Costa Community College District as part of the enrollment process. Required use of the student ID and password serves as a means to validate that the student who is registered for a course is the same student doing the work and receiving the grades/credits. The District and the colleges will, at all times, work to ensure that each student’s password is protected against public disclosure. Students shall be notified about steps to take in order to request the issuance of a new password should they believe that their existing password has been compromised. |
| **1** | AP 4105 Distance Education - The District procedure complies with Federal regs regarding student authentication. |
| **2** | Distance Education Administrative Procedure 4105 References Title 5 Section 55200, et seq. Designates Open Campus District entity responsible for distance education. Establishes course approval and certification requirements. |
| **1** | The administration at Lake Tahoe Community College strives to have the highest quality distance education program. Planning and coordination of distance education is needed to provide faculty, staff, and students with the appropriate resources for instruction and support. Providing these services with a maximum utility and minimum waste is paramount. A well-organized and facilitated program enhances the college’s ability to expand the program and improve the college’s image as a technologically advanced learning institution. |
| **1** | The Executive VP and Student Services shall utilize one or more of the following methods to authenticate or verify student identify: 1. Secure credentialing/login and password 2. Proctored examinations; or 3. New or other technologies and practices that are effective in verifying student identification. Policy statements regarding student privacy are provided students at time of registration |
| **1** | Standard II.C: Library and Learning Support Services The Distance Education system is lead by the Dean of Learning Resources and Academic Technology. The Dean, faculty and staff of the Division continually work to maximize “distance accessibility” to the college’s learning resources to support Distance Education students. Electronic resources greatly expand the information sources available to the students both on and off campus; these electronic resources include 10,858 electronic books, nearly 10,000 full- text journals available through 11 subscription databases, and a growing collection of electronic reserves. Access to electronic resources from off campus is seamlessly provided via a proxy server that authenticates off-campus users based on their campus identification numbers and last names. Access to all the collections is maintained through the online catalog, the z39.50 compliant Voyager system, which includes a fully web-based public access catalog (HANS), as well as circulation, cataloging, acquisitions, and serials modules. A suite of products from Serials Solutions facilitate student use of the electronic serials in the collection. The library web site is a virtual gateway to information resources of all kind. Integrated library and federated search boxes in WebCT courses, faculty blogs, and web sites. A tool bar, installed on all library computers and available for student download, integrates library search options directly into the web browser; and shared holdings information with Web-based search tools. THE ENTIRE SUB CHANGE CAN BE FOUND AT: www.ohlone.edu, go to Accreditation under A-Z link then go to Substantive Change under first group of files. Thanks |
| **1** | Distance Education Administrative Procedure 4105 References Title 5 Sections 55200, et seq. Designates Open Campus District entity responsible for distance education. Establishes course approval and certification requirements. |
| **1** | Board Policy and Administrative Procedures Draft in progress. BP: The San Diego Community College District’s Colleges and Continuing Education comply with Federal Student Authentication Regulations which require institutions that offer distance education to have processes in place through which the institution establishes that the student who registers in a distance education course is the same student who participates in and completes the course or program and receives the academic credit. References: Authority: 20 U.S.C. 1099b) [64 FR 56617, Oct. 20, 1999, as amended at 74 FR 55427, Oct. 27, 2009] Adopted: Supersedes : New Policy AP: The SDCCD follows these guidelines as procedures for implementing Federal Student Authentication Regulations: At the SDCCD, students who are enrolled in a distance education course must log into a secure course management system that authenticates their identity through a unique user name and password for access. The SDCCD's policies regarding academic integrity and acceptable use of IT services include penalties for unauthorized use of another individual’s name and password and for engaging in academic dishonesty (AP 3100.3 HONEST ACADEMIC CONDUCT). In the future, when other methodologies to assist with student authentication become more available, the SDCCD will explore their use. Adopted: Supersedes : New Policy |
| **1** | While our board of trustees does not yet have an approved student authentication policy, our district does assign each student a unique college ID and is utilized with our password-protected course management system, Blackboard through a secure login process. Passwords are encrypted by Blackboard, and the login page is encrypted by SSL technology. |
| **1** | BP 5500 STANDARDS OF CONDUCT References: Education Code, Sections 66300 and 66301; Accreditation Standard II.A.7.b The following conduct while on District-owned or controlled property or at District-sponsored or supervised functions shall constitute good cause for discipline, including but not limited to the removal, suspension, or expulsion of a student. 13.Cheating, or engaging in other academic dishonesty including copying from another’s work; discussion prohibited by the instructor; obtaining exam copies without permission; and using notes, other information, or devices that have been prohibited. 14.Misrepresentation and/or impersonation, including arranging for or allowing another individual to impersonate or otherwise misrepresent himself or herself to be a student generally or to be a particular student either in person or in an online environment, and/or impersonating or otherwise misrepresenting oneself to be another person in person or in an online environment. 29.Violation of Board policies or administrative procedures governing the use of student user accounts, computers, and telecommunication resources, including but not limited to the unauthorized entry, opening, or viewing of a file; the unauthorized use of another individual’s identification and password; arranging for, allowing, and/or impersonation of one person by another; sending obscene or abusive messages or files; and/or use of computing facilities to interfere with the work of another student or employee of District. Date Adopted: May 16, 2007  Dates Revised: March 4, 2009, May 2, 2012 |
| **1** | BP 4105 The following is an excerpt from AP4105 The District will provide to each student at the time of registration, a statement of the process in place to protect student privacy and estimated additional student charges associated with verification of student identify, if any. The Chief Instructional Officer shall utilize one or more of these methods to authenticate or verify the student’s identity: \*secure credentialing/login and password; \*proctored examinations; or \*new or other technologies and practices that are effective in verifying student identification. |
| **1** | The existing policy is embedded in our Computer Use policy and in the Student Code of Conduct; however, a recommendation has been made that a separate policy be developed that is specific to the use of our LMS system. |
| **1** | The policy is under review right now as the college aligns with the League standards of Board policy and procedures. |
| **1** | AP 4105 The District utilizes a LMS whereby students must authenticate their identity. In order to access the LMS, students must log into the MyCOM Portal with their College of Marin‐issued student user name and password. Date Approved: June 28, 2011 Revised: June 19, 2012 |
| **1** | While it has not yet been adopted as policy, language has been drafted and is currently being vetted through the shared governance structure. |
| **1** | Student Verification and Privacy: Consistent with federal regulations pertaining to federal financial aid eligibility, the District must authenticate or verify that the student who registers in a distance education or correspondence education courses is the same student who participates in and completes the course or program and receives the academic credit. The District will provide to each student at the time of registration, a statement of the process in place to protect student privacy and estimated additional student charges associated with verification of student identity, if any. The Chief Instructional Officer shall utilize one or more of these methods to authenticate or verify the student’s identity: • secure credentialing/login and password; • proctored examinations; or • new or other technologies and practices that are effective in verifying student identification. The Chief Instructional Officer shall establish procedures for providing a statement of the process in place to protect student privacy and estimated additional student charges associated with verification of student identity, if any, to each student at the time of registration. |
| **1** | Currently in draft form--Board Policy and Administrative Procedure BP: The San Diego Community College District’s Colleges and Continuing Education comply with Federal Student Authentication Regulations which require institutions that offer distance education to have processes in place through which the institution establishes that the student who registers in a distance education course is the same student who participates in and completes the course or program and receives the academic credit. References: Authority: 20 U.S.C. 1099b) [64 FR 56617, Oct. 20, 1999, as amended at 74 FR 55427, Oct. 27, 2009] Adopted: Supersedes : New Policy AP: The SDCCD follows these guidelines as procedures for implementing Federal Student Authentication Regulations: At the SDCCD, students who are enrolled in a distance education course must log into a secure course management system that authenticates their identity through a unique user name and password for access. The SDCCD's policies regarding academic integrity and acceptable use of IT services include penalties for unauthorized use of another individual’s name and password and for engaging in academic dishonesty (AP 3100.3 HONEST ACADEMIC CONDUCT). In the future, when other methodologies to assist with student authentication become more available, the SDCCD will explore their use. Adopted: Supersedes : New Policy |
| **1** | The Colleges help protect students’ privacy and authenticate students’ identity by requiring secure login and password whenever a student registers for classes, reviews his/her enrollment information, or logs in to any other secure SMCCCD site. The District will not share any SMCCCD student login and password information with anyone, and students are advised not to share any SMCCCD login and password information. A statement to this effect is posted prominently for students each time they log in to WebSmart, the San Mateo Community College District’s electronic registration system. |
| **1** | Draft of Board Policy and Administrative Procedure in Progress. BP: The San Diego Community College District’s Colleges and Continuing Education comply with Federal Student Authentication Regulations which require institutions that offer distance education to have processes in place through which the institution establishes that the student who registers in a distance education course is the same student who participates in and completes the course or program and receives the academic credit. References: Authority: 20 U.S.C. 1099b) [64 FR 56617, Oct. 20, 1999, as amended at 74 FR 55427, Oct. 27, 2009] Adopted: Supersedes : New Policy AP: The San Diego Community College District’s Colleges and Continuing Education comply with Federal Student Authentication Regulations which require institutions that offer distance education to have processes in place through which the institution establishes that the student who registers in a distance education course is the same student who participates in and completes the course or program and receives the academic credit. References: Authority: 20 U.S.C. 1099b) [64 FR 56617, Oct. 20, 1999, as amended at 74 FR 55427, Oct. 27, 2009] Adopted: Supersedes : New Policy |
| **1** | Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to any system or to another person’s information are a violation of District policy and may violate federal, state and local laws. An account assigned to an individual must not be used by others without written permissions from the Deputy Director for Network Services. The assigned individual is responsible for the proper use of the account including proper password protection. |
| **1** | AR 4000.2 Electronic Communications: Personal passwords/account codes are issued to student users. Users agree to represent themselves according to their true identities in all electronic transactions. Students agree not to share passwords/account codes with others. The learning management system requires unique user IDs and passwords. |
| **1** | Authentication and Verification of Student Identity: One or more of these methods will be used to authenticate or verify the student’s identity: Secure credentialing/login and password Proctored examinations, or New or other technologies and practices that are effective in verifying student identification |
| **1** | Computer accounts are for the use of the assignee only. Unauthorized sharing and/or access of computer accounts of other users are prohibited. |
| **1** | The Board Policy is as follows: The Chancellor will ensure that procedures are in place to meet the accreditation requirements regarding Distance Education, as well as those of State and Federal statutes. The Administrative Procedure is more lengthy, but here is a brief summary: The Chancellor shall establish procedures that will provide methods to authenticate or verify the student’s identity for distance education and correspondence education courses. Authentication and Verification of Student Identity: One or more of these methods will be used to authenticate or verify the student’s identity: Secure credentialing/login and password Proctored examinations, or New or other technologies and practices that are effective in verifying student identification. |
| **1** | Privacy, Security and Acceptable Use of Electronic Resources Policy No. 5350 March 15, 2000 Accounts and passwords may not, under any circumstances, be shared with, or used by, persons or groups other than those to whom they have been assigned by the college. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Distance Education Policy No. 3230 November 2, 2011 Distance education course must be delivered via the Internet using a campus-supported Learning Management System (LMS). |
| **1** | Administrative Procedure 4105: Authentication of Students in Distance Learning Courses: Distance learning course participation will be conducted through Mt. SAC server authenticated methods. Accepted practices for authentication include user ID and password authentication to access the student portal or learning management system or by use of Mt. SAC email address. Adopted April 2012 |
| **1** | The board policy closest to this is BP 3720 COMPUTER AND NETWORK USE: "Employees and students who use District computer networks and other technology, and the information they contain, and related resources have the responsibility not to abuse the resources and to respect the rights of others. The Chancellor shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users." Student authentication authority derives from this policy and is considered a procedure. |
| **1** | The district shall monitor the program to insure the integrity of student work and the credibility of the degrees and credit it awards. |

## 8. Date Policy was Approved (mm/dd/yyyy)-Policy Summary

|  | |
| --- | --- |
| **Count** | **Response** |
| **1** | 04/12 |
| **1** | 05/16/2007 |
| **1** | 05/23/2011 |
| **1** | 05/24/2011 |
| **1** | 06/12/2008 |
| **1** | 06/13/2012 |
| **1** | 06/21/2011 |
| **1** | 06/22/2004 |
| **1** | 06/28/2011 |
| **1** | 10/14/08 |
| **1** | 2008 |
| **1** | 6/19/2012 |
| **1** | 7/10/2012 |
| **1** | 8/28/2012 |
| **3** | June 15, 2009 |
| **1** | Rev. 05/14/12 |
| **1** | in progress |