Policy: Access to the CCBC Network

Policy Date: 6/8/2009

1.0 Purpose

The Community College of Baltimore County (CCBC) has implemented Identity Management technology to manage access to the CCBC network and other technology resources. Identity Management provides a single userid and password that are used to access computers on the College campuses, the College network, and computer applications provided by the College. This document provides policy and procedure for the CCBC userid and password. Use of a CCBC provided userid and password requires full compliance with the CCBC Acceptable Use of Information Technology policy, found on the College Web site.

2.0 Policy

The College provides access to College resources to students, faculty, staff, consultants, vendors, guests, and others who have reason to use College technology. It is the policy of CCBC that all users of College technology resources must use their College issued CCBC userid and password to access technology resources at the College. Certain College computer classrooms may be configured to use a generic connection to the network and not require the use of the College issued userid and password. In those classrooms, use of the generic userid, or the student issued userid is at the discretion of the faculty member for that classroom experience.

A CCBC userid and password are automatically generated in Banner for all faculty, staff, and students. The userid and password are provided to faculty and staff by their employing department. The userid and password for students are provided to the student by mail generated by Enrollment Services. In addition, adjunct faculty and students may use the Userid/Password SelfHelp application provided in numerous places on the College web environment. The SelfHelp application will ask the user for information unique to that person and if answered successfully, will reveal the userid. The SelfHelp application can also be used to reset the password. For security reasons, the SelfHelp application will not work for full time administrative employees of the College. The College Helpdesk provides assistance for all users for userids and passwords.

The remainder of this policy and procedure document addresses management of the userid and password and various special cases.

3.0 Userid Changes

The userid issued by the College is used for all applications to which the user has access. The userid is used to access application services provided by the College. These include access to the College network, email, file storage, access to Banner, and other services unique to the person. Userid changes cannot be automated, are labor intensive, and time consuming. A request for a userid change should be submitted to the ITS Helpdesk.

4.0 Password Changes

The College requires that passwords are changed at a minimum of 180 day increments. Passwords may be changed more frequently. Shortly before the password is set to expire, the user will receive an electronic notification indicating that the password is about to expire. The notification will contain guidance on how to change the password.

Passwords may be changed at the desktop, using the SelfHelp application, or by calling the Helpdesk. When changing the password, the College standard is to use strong passwords. A strong password is a minimum of six characters and must contain at least one upper case, one lower case, and one numeric character. The CCBC Knowledgebase contains guidance and tips on passwords and changing passwords.

Because CCBC uses an Identity Management infrastructure, a password change will be effective for all applications to which the user has access.

5.0 Guest Userids

The College has many relationships other than faculty, staff, and students. Guest access includes long term access to College resources, such as for recurring consultants. Guests also include casual, unsponsored visitors to the College.

5.1 Sponsored Guest Access

A College sponsor must request a userid and password for a long term guest. Long term guests include Board of Trustee members, consultants, vendors, and others who will perform work and/or use College resources on behalf of the College. The request should be made to the ITS Helpdesk (443 840 4357, helpdesk@ccbcmd.edu).The request must include:

- The full name of the guest
- Sponsoring Office
- Sponsor contact name, telephone number, and email address
- Termination date of the guest userid
- College resource requirements – specific College applications such as a College email account

Prior to the termination date, the College sponsor will receive an automated notification that the guest userid will expire on the termination date. Unless renewed, the guest userid will be disabled on the termination date. The College sponsor may renew the guest userid for up to an annual renewal period.

5.2 Non-Sponsored Guest Access

The College recognizes an obligation for public service. The College also has an obligation to ensure appropriate use of College resources and to be responsive to law enforcement inquiries on use of the College network. The College will provide a guest CCBC userid to non-sponsored guests when personal identification credentials are provided by the non-sponsored guest. Acceptable personal identification includes one of the following:

- Drivers license with picture ID and name
- Government issued identification such as passport with picture ID and name
- Other authoritative identification that contains both a name and picture ID

Minors without appropriate personal identification may use the identification of an accompanying adult.

Non-sponsored guests may request a CCBC userid at the following College service points:

- The College Library on any campus
- The ITS Helpdesk on any campus

- The Public Safety Office on any campus
- The Enrollment Services One-Stop-Shop on any campus

All non-sponsored CCBC userids will be disabled at midnight of the date of issue. Use of a CCBC provided userid and password requires full compliance with the CCBC Acceptable Use of Information Technology policy, found on the College Web site. The College may immediately disable or may refuse to grant a guest userid if there is evidence of non-compliance with the Acceptable Use policy.

6.0 Expiration of Userids

The College userid and password is intended to be used for the duration of the user's relationship in good standing with the College. The College may disable an account at any time if there is evidence of violation of the CCBC Acceptable Use of Information Technology, policy, found on the College Web site. Normal termination of function of the CCBC userid applies as follows:

6.1 Students – userids are intended to remain active in perpetuity

6.2 Retirees – userids are intended to remain active in perpetuity

6.3 Staff – userids are terminated when the staff person leaves the institution

6.4 Adjunct Faculty – userids are disabled after two consecutive full academic semesters with no paycheck paid to the employee

6.5 Sponsored Guests – userids are disabled on the termination date, defined when the userid was created. The termination date may be extended by request of the College sponsor of the guest.

6.6 Non-sponsored Guests – userids are disabled at midnight of the date of issue