



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Students	<b>Number:</b> <b>B6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 1 of 4

Broward Community College provides all of its students with College Network and Internet access so that they can obtain up-to-date information useful for their advancement in academics. Use of the College Network shall be based on college or academic need.

### **Purpose and Network Account Creation**

- The purpose of the Network and Account Policy is to provide a secure computer network environment for Broward Community College’s infrastructure.
- User IDs and passwords control access to all Broward Community College Information Technology resources.
- For any students to receive account access, the student must first agree to the account policy. (See Account Activation Steps)
- Notification of the availability of email accounts is done through publications on each campus, student orientation, and by instructors.
- When a new student applies to Broward Community College or when a student returns to the College after not having attended classes for at least a year.
- Each student is assigned a user ID and password and is held responsible for all actions performed, and all data which is modified or retrieved under their user ID and password.
- All accounts will require both a username and a password.
- User IDs or passwords may not be shared with another person under any circumstances.
- Users are limited to five incorrect sign on attempts before the account is disabled.
- All network accounts will have the same format. First letter of first name and first seven letters of the last name. If there are identical names the last letter will be changed to a number.

### **Distribution Lists**

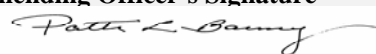
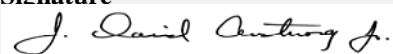
- When a student adds a class they are automatically added to the distribution list. Conversely, when a student drops a class they are deleted from the distribution list.

### **Account Activation Steps**

- Log onto myBCC/SOS Login: [www.broward.edu](http://www.broward.edu)
  1. Enter Login ID
  2. Enter PIN
  3. Select Personal tab
  4. Select Student e-mail tab
  5. Student must read the Broward Community College Student Computer Fair Use Guidelines and Agreement and accept the terms.
- Only current students will be provided with a Broward Community College e-mail account.

### **Account Passwords**

- Logon IDs and passwords must control access to all Broward Community College Information Technology resources.

<b>Recommending Officer’s Signature</b>	<b>Date</b>	<b>President’s Signature</b>	<b>Date</b>
	5/1/08		5/1/08



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Students	<b>Number:</b> <b>B6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 2 of 4

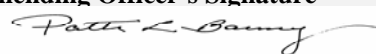
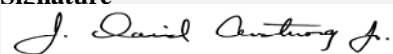
- All passwords will have a minimum length of five characters.
- Passwords shall contain a combination of letters and numbers.
- Passwords shall never be written down or e-mailed.
- Passwords shall not be common words used at Broward Community College, family member’s names, local sports teams, bank or personal identification numbers.
- No program, procedure, hardcopy report, terminal, monitor, or computer screen may display or echo a password.
- Passwords transmitted or used with internet accounts should be of different variation from those used within Broward Community College.

### Account Removal

- At the end of each term, accounts for students who have not attended Broward Community College within the last year are deactivated.
- Accounts may remain on the system for historical auditing and tracking purposes but must be disabled.
- In the event of any perceived risk to the College, Technology Staff will immediately disable an account upon written notification from the Student Dean, Provost or Vice President of Student Affairs .

### Network Storage

- Recoverability of data (email, files) on network storage is limited by the three week retention period for backup tapes. Restoration of backup data can only be executed within three weeks after deletion or modification. Data files stored on the computer’s local drive(s) are not backed up by Technology Staff and are the responsibility of the individual data owner.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
--	-----------------------	--	-----------------------



**Broward  
Community  
College**

## Procedure Manual

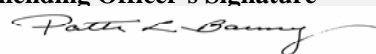
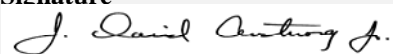
<b>Title:</b> College Network and Software Usage by Students	<b>Number:</b> <b>B6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 3 of 4

### Software Installation

- The College will provide licensed software for College owned personal computers as part of a standard desktop configuration. Any additional software installed on a personal computer will be the responsibility of the Department or individual.  
Software may only be installed if all of the following conditions are met:
  - 1) Only licensed software or evaluation software pre-approved compatible with the College Network will be installed on Broward Community College’s computers.
  - 2) Only authorized Broward Community College employees or vendors will install software on College computers.
- Computers and hardware devices that are designated as part of a curriculum may be modified as required by the curriculum. Coordination with Technology Staff to ensure that the modifications are not having adverse effects on the College Network is the responsibility of the department overseeing the curriculum.

### Anti-Virus

- Computers that do not have active, approved virus detection shall not be connected to the College Network.
- Technology Staff will configure desktop computers with an active virus detection software that performs periodic, complete scans of the computer (at least weekly) for viruses.
- Technology Staff will configure the virus detection software to download and update the virus definitions on a periodic basis (at least weekly).
- Users must not cancel automatic virus scanning or updating of definitions. If such automatic activity interferes with the user’s duties, the user should call the College Help Desk at 954-201-7521 for additional support.
- All software and files downloaded from non-Broward Community College sources via the Internet (or any other public network) must be screened with Broward Community College approved virus detection software.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
--	-----------------------	--	-----------------------



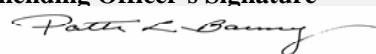
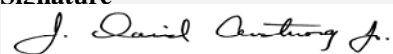
**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Students	<b>Number:</b> <b>B6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 4 of 4

The following activities, but not limited to, are **prohibited**:

- Attempts in any way to interfere with the availability or quality of service, and/or damaging network devices.
- Storing, downloading, posting, or displaying obscene or offensive data, even temporarily, in areas where someone might view them passively or inadvertently, except in cases where academically necessary.
- Attempts to circumvent established security procedures or to obtain access privileges to which a user is not entitled.
- Attempts to modify computer systems or software in any unauthorized manner.
- Unauthorized access, alteration, or destruction of another user’s data, programs, or electronic mail.
- Attempts to obtain unauthorized access to either local or remote computer systems or networks.
- Manipulation of others to gain information for the purpose of gaining access to commit fraud or damage to the system.
- Using a program or procedure that looks like a normal logon process but instead records the user’s password and user name.
- Executing any form of network monitoring which will intercept data not intended for the user’s host.
- Attempting port scanning, network sniffing, packet spoofing, denial of service and forged routing information.
- Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s network session.
- Theft or destruction of computer hardware or software.
- Any criminal activity or any conduct that violates applicable laws.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
--	-----------------------	--	-----------------------