

Procedure Manual



Title: College Network and Software Usage by Students	Number: A6Hx2-8.01b
Policy Number: 6Hx2-8.01	Page: 1 of 3

Broward 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 College’s infrastructure.
- Usernames and passwords control access to all Broward College Information Technology resources.
- Students should use their full e-mail address (username@mail.broward.edu) as their username for all systems at Broward College.
- 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 the admissions process.
- Each student is assigned a username and password and is held responsible for all actions performed, and all data which is modified or retrieved under their username and password.
- All accounts will require both a username and a password.
- Usernames or passwords may not be shared with another person under any circumstances.

Distribution Lists



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

Account Activation Steps

- Log on to myBC: www.broward.edu/mybc
 1. Enter username
 2. Enter password
 3. Student must read the Broward College Policies and Guidelines and accept the terms.

Account Passwords

- All accounts will require both a username and a password.
- The password, at a minimum, must be-eight characters in length.
- Passwords for general users will be required to change within 180 days of last change.
- Passwords for Information Technology domain and enterprise administrators will be required to change within 30 days of last change.
- The password reuse policy will be set so that old passwords are remembered 4 times before allowing the user to reuse a password.
- Passwords shall never be written down, e-mailed nor stored in unencrypted files.
- Passwords shall not be common words used at Broward College, family member’s names, local sports teams, bank or personal identification numbers.

Recommending Officer’s Signature 	Date: 2/3/2020	President’s Signature 	Date: 2/3/2020
--	--------------------------	---	--------------------------

Procedure Manual



Title: College Network and Software Usage by Students	Number: A6Hx2-8.01b
Policy Number: 6Hx2-8.01	Page: 2 of 3

- No program, procedure, hardcopy report, terminal, monitor, or computer screen may display or echo a password.
- Users shall not use the same password at the College for other services external to the College.
- Passwords must contain characters from three of the four following categories:
 1. English uppercase characters (A to Z)
 2. English lowercase characters (a to z)
 3. Numeric characters (0 to 9)
 4. Non-alphanumeric characters (!,\$,%,&....)
- May not contain the First Name, Middle Name or Last name.
- Service and generic accounts used by Information Technology Staff must use more complex password algorithms than the standard password policy and must have interactive logon disabled.

Account Removal

- In the event of any perceived risk to the College, Information Technology Staff will immediately disable an account upon written notification from the Student Dean, Provost or Vice President of Student Affairs.

Personally Owned Computing Equipment


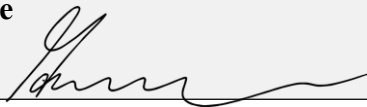
- Broward College is NOT responsible for configuring and supporting personally-owned computing equipment that is used to access College Computing Resources.
- Broward College is NOT responsible for backing up or the restoration of any data stored on personally owned computing equipment.
- The user is responsible for having an up-to-date anti-virus and anti-malware protection application and for any virus, adware, and spyware removal.
- The user is responsible for all personally owned computing device support requirements, including the cost of repairs, diagnostics or replacement of his/her device.

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 College's computers.
 2. Only authorized Broward 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 Information 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.

Recommending Officer's Signature 	Date: 2/3/2020	President's Signature 	Date: 2/3/2020
--	--------------------------	---	--------------------------

Procedure Manual





Title: College Network and Software Usage by Students	Number: A6Hx2-8.01b
Policy Number: 6Hx2-8.01	Page: 3 of 3

Anti-Virus

- Computers that do not have active, approved virus detection shall not be connected to the College Network.
- Information Technology Staff will configure desktop computers with active virus detection software that performs periodic, complete scans of the computer (at least weekly) for viruses.
- Information 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 or an instructor.
- All software and files downloaded from non-Broward College sources via the Internet (or any other public network) must be screened with Broward College approved virus detection software.

The following activities are prohibited, unless written approval from Technology Staff is obtained demonstrating that the activities will be executed for academic purposes:

- 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.

Recommending Officer's Signature 	Date: 2/3/2020	President's Signature 	Date: 2/3/2020
--	--------------------------	---	--------------------------