

## Procedure Manual



<b>Title: College Network and Software Usage by Students</b>	<b>Number:</b> A6Hx2-8.01b
<b>Policy Number:</b> 6Hx2-8.01	<b>Page:</b> 1 of 4

### STUDENT PROCEDURE

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.
- Broward College One Access is the College's branded single sign-on portal. It provides the college with a unified single sign-on experience for a range of applications and services.
- Usernames and passwords control access to all Broward College Information Technology resources.
- Students should use their e-mail address (username@mail.broward.edu) as their username.
- 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 strong password. For enhanced security it is strongly recommended that students add an additional layer of account protection by using Multi-Factor Authorization (MFA) utilizing a mobile device. Personal mobile devices used for MFA should be protected with biometric features (e.g. Face Recognition) or a 6-digit passcode.
- Passwords, passcodes and similar information must not be shared with anyone 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 removed from the class distribution list.

#### Account Activation Steps

- Log on to MyBC: [www.broward.edu/mybc](http://www.broward.edu/mybc)
  1. Enter login credentials
  2. Student must read the Broward College Policies and Guidelines and accept the terms.

#### Account Passwords

- All student accounts must include a strong password.
- The password, at a minimum, must be twelve characters in length.

<b>Recommending Officer's Signature</b> Raj Mettai	<b>Date:</b> 12/03/24	<b>President's Signature:</b> 	<b>Date:</b> 12/03/24
---	--------------------------	---	--------------------------

## Procedure Manual



<b>Title: College Network and Software Usage by Students</b>	<b>Number:</b> A6Hx2-8.01b
<b>Policy Number:</b> 6Hx2-8.01	<b>Page:</b> 2 of 4

- Passwords must contain characters from each of the 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 (!, \$, %, &, @, ...)
- Passwords must not contain the Student's first name, middle name or last name.
- Passwords for students are required to be changed according to the guidelines outlined in the IT Security Privileged Accounts document.
- The password reuse policy is set so that the last 8 passwords cannot be reused.
- Passwords must never be shared, written down, emailed, communicated, or stored in an unencrypted format.
- Passwords must not be common words used at Broward College, family member's names, local sports teams, phone numbers, bank or personal identification information.
- No program, procedure, computer screen, mobile device, or tablet may display a password.
- Students must not use the same password at the College for other services external to the College.

### Accounts / Microsoft License

- If a student is enrolled and paid for a course, the student will be granted a full Microsoft desktop license. The license permits the installation and use of Microsoft Office products (Outlook/email, Word, Excel, OneDrive, etc.) on a personal computer. Additionally, the student will be able to access the web version of these products via the internet along with limited access to other Microsoft products. The full desktop license is valid for 1-year after the completion of the student's last attended term. After 1 year, if the student is not enrolled, the student will have web access only to Microsoft Office products including Outlook/email, Word, Excel, OneDrive, etc.
- Any student who is not enrolled for a continuous 2-year period from their last attended term will have their license revoked and will only be reissued upon re-enrollment. Once a license is revoked, the student will no longer be able to log into the Broward College One Access portal, and their Outlook/emails and OneDrive files will be deleted.
- Alumni web email accounts will only be active for 2 years after the student graduates or 2 years after the student's last term attended. After 2 years, Alumnus will no longer be able to log into the Broward College One Access portal, and their Outlook/emails and OneDrive files will be deleted.
- Outlook/email boxes will be limited to 10 GB of space and OneDrive space will be limited to 20 GB of space.
- In the event of any perceived risk to the College, the Information Technology department will immediately disable a student's account upon written notification from the Dean, Provost, Vice President of Student Affairs or the Vice President of Information Technology.

### Web Filtering / Geo-Blocking

- The College reserves the right to use web or content filtering and geo-blocking to control internet access.

<b>Recommending Officer's Signature</b> Raj Mettai	<b>Date:</b> 12/03/24	<b>President's Signature:</b> 	<b>Date:</b> 12/03/24
---	--------------------------	---	--------------------------

## Procedure Manual



<b>Title: College Network and Software Usage by Students</b>	<b>Number:</b> A6Hx2-8.01b
<b>Policy Number:</b> 6Hx2-8.01	<b>Page:</b> 3 of 4

- The College reserves the right to restrict or deny access to certain domains, content applications and websites as deemed necessary.
- The College reserves the right to block or deny access to geographic regions as deemed necessary.

### Software Installation

- The College will provide licensed software for College owned computers as part of a standard desktop configuration. Any additional software installed on a computer will be the responsibility of the Department to arrange with the Information Technology Department.
- Software may only be installed if all 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.
  3. Computers and other devices designated as part of a curriculum may be modified as needed to meet the curriculum's requirements. The department overseeing the curriculum must coordinate with the Information Technology Staff to ensure these modifications do not adversely impact the College's network and systems.

### 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 student is responsible for having up-to-date end-point protection software to detect, block and remove any virus, adware, malware or spyware.
- The student is responsible for all personally owned computing device support requirements, including the cost of repairs, diagnostics, upgrades or replacement of the device.
- Personally owned computers will only connect to the college's network as a guest device and be granted internet access only.

### End-point Protection

- Computers that do not have active, end-point protection software shall not be connected to the College Network.
- The Information Technology department will configure Broward College devices with end-point protection software that detects viruses and prevents them from executing.
- The Information Technology department will configure the virus detection software on Broward College devices to perform periodic scans of the computer for viruses and other malicious types of programs.
- Information Technology Staff will configure the virus detection software on Broward College devices to download and update the virus definitions on a periodic basis.
- The Information Technology department will configure Broward College devices to automatically receive operating system updates.

<b>Recommending Officer's Signature</b> Raj Mettai	<b>Date:</b> 12/03/24	<b>President's Signature:</b> 	<b>Date:</b> 12/03/24
---	--------------------------	---	--------------------------

## Procedure Manual




<b>Title: College Network and Software Usage by Students</b>	<b>Number:</b> A6Hx2-8.01b
<b>Policy Number:</b> 6Hx2-8.01	<b>Page:</b> 4 of 4

### College-Wide Printing

Multi-functional devices (MFD) are available for students to print or scan documents for a fee.

**The following activities are prohibited. Written approval from the Information Technology department is needed for demonstrating these activities 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 username and password.
- Executing any form of network monitoring which will intercept data not intended for the user's computer.
- 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.
- Unsecured transmission or storage of personally identifiable information.
- Confidential or sensitive data stored in an unencrypted format on portable machines or storage media.
- Any criminal activity or any conduct that violates applicable laws.

<b>Recommending Officer's Signature</b> Raj Mettai	<b>Date:</b> 12/03/24	<b>President's Signature:</b> 	<b>Date:</b> 12/03/24
---	--------------------------	---	--------------------------