Procedure Manual

Title: College Network and Software Usage by Employees	**Number:** A6Hx2-8.01a
Policy Number: 6Hx2-8.01	**Page:** 1 of 11

Broward College provides all its employees with College Network and Internet access so that they can obtain up-to-date information useful to them for the performance of their job functions and duties. 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.
- Broward College One Access is the College's Identity Provider (IdP). It provides the college with multi-factor authentication and single-sign on throughout various applications at the College.
- Workday is Broward College's computer application used for Human Resources, payroll, financial, academic and student functions.
- College Integrated Database (CID) is Broward College's student enterprise resource planning (ERP) computer application. CID is used to support and assist both student and business functions. Students will use applications integrated with CID to perform various academic functions.
- User provisioning is the creation of a user's account including email, personal drive, printing access and other BC assets. Once entered into Workday, a user will be automatically provisioned throughout all the necessary Broward College systems.
- The employee's job function and department requirements will determine the level of access to network resources and applications. Users may be provided additional access to other systems with documented authorization from their supervisor and application data owner.
- All access rights will be set to the minimum necessary for users to perform their job functions.
- All user accounts will require both a username and a password.
- All user 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.

Account Logins

- Each employee must be assigned a unique username. The employee is held responsible for all actions performed, and all data which is modified or retrieved under their username and password.
- Usernames, accounts, or passwords may not be shared with another person under any circumstances.
- Users are limited to five incorrect sign-on attempts. After the fifth attempt the account is automatically suspended. Employees can call the College Help Desk at 954-201-7521 to have their accounts un-locked, or reset their password via Broward College One Access.
- Users may not embed usernames and/or passwords in a procedure, program, function key, logon profile, script or non-encrypted password file. Information Technology Staff, may if necessary, embed usernames and/or passwords using secure methods when performing integration work.

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

Account Passwords

- All accounts will require both a username and a password.
- The password, at a minimum, must be-eight characters in length.
- 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 their first name, middle name or last name.
- Passwords for general users will be required to change within 90 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 8 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.
- 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.
- 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.

Temporary or Contracted Employees

- A temporary or contracted employee is a contingent worker or non-Broward College employee who may require access to its network systems and applications.
- All temporary or contracted employees may be issued a Broward College network account to utilize any IT resources.
- Workday is used to provision and maintain all new contingent workers at the College.
- A Fair Use and Information Security Affidavit must be signed by the temporary or contracted employee when deemed necessary.
- All temporary or contracted access requests must have a start and end date.
- The person requesting access for the temporary or contracted employee is responsible for terminating the contingent worker within Workday when access is no longer needed.
- Information Technology staff will remove the contingent worker upon notification from the non-employee's supervisor that they no longer need access or upon proper termination procedures within Workday.

Account Modification

- For employees to have changes approved in their level of network access, the Information Technology department must receive a completed Network Security Change Request Online Form initiated by their supervisor.
- The employee’s job function and department requirements will determine the level of access to network directories and applications.

Account Removal

- De-provisioning is the removal of a user’s account including email, H drive, and all BC assets.
- Disabling is the removal of a user’s Network and System Access to the BC Network and other resources.
- Disabled user accounts may exist in the system for a period of 2 years before being permanently de-provisioned for maintenance purposes.
- Upon separation from Broward College, all employees must have their Broward College network access permanently disabled.
- In preparation of a scheduled termination of an employee, the employee's supervisor must coordinate with HR to determine that all the necessary steps have been taken.
- All terminations are initiated within Workday. The de-provisioning process will disable and eliminate the account automatically. HR may notify the Information Technology team of any accounts that need to be disabled manually and prior to the Workday termination automation.
- The Information Technology Staff will disable all network access that is not part of the de-provisioning process at the end of the employee’s last working day.
- Accounts may remain on the system for historical auditing and tracking purposes but will be disabled by Technology Staff.
- Full and part-time staff and student workers will have their network access removed immediately if they do not have an active assignment. Faculty and Adjuncts will be provided their current level of network access for 180 days after their last assignment end date.
- Security Reports will be created and reviewed to identify employees who no longer meet network access standards. These employees will have their network access disabled immediately, and their supervisors will be notified.
- In the event of any perceived risk to the College, Information Technology Staff will immediately disable an account upon written notification from Vice President Information Technology, Employee Relations and Executive Director of Talent and Culture.

Default and Industry Known User IDs

- Upon installation of software, personnel installing software will remove default and industry known usernames and passwords. These defaults should be disabled and replaced by approved Broward College usernames and passwords. If a default username cannot be replaced, passwords for these accounts shall be changed in accordance with the same procedures that govern individual accounts.

Account Logoff and Power Management Standards

- To prevent account and system information from being viewed by anyone other than the user of that account, any information displayed on a terminal or monitor signed onto the CID Enterprise resource planning (ERP) system will be erased and the user will be signed off the system after 20 minutes of inactivity. The Workday ERP system is defaulted to 10 minutes of inactivity.
- Users are required to use the Windows screen saver feature on their workstation to blank out and lock their computer display screen after a period of 10 minutes of inactivity of the computer. This process requires the user to enter a password to unlock the computer.
- Users shall use the Windows power management feature on their workstation that will go into standby mode after 20 minutes of inactivity. Exceptions with approval from the campus President and Vice President for Information Technology.
- Some device categories deviate from the standards; any deviations are documented in the Standards by Device Category Section.
- All users must lock their machine when away from their desk.

Network Storage

- All network file storage is used for College business and/or academic data files.
- In order to optimize College technology resources and control infrastructure costs, employees are required to monitor their network storage usage and delete obsolete or redundant files on a regular basis.
- Drive H: and Microsoft Office 365 OneDrive are the individual's business storage.
- Drive P: is the departmental storage and should be used for sharing files within the department.
- Drive U: is Community storage and should be used for sharing files within special groups.
- Employees may call the Help Desk at 954-201-7521 or submit a Help Desk online request if they wish to request an increase of the network storage limit. These requests will be reviewed and approved by Information Technology Staff.
- Recoverability of data on network storage is limited by the a four-week retention period. Restoration of backup data can only be executed within four weeks after deletion or modification. Data files stored on the computer's local drive(s) are not backed up by Information Technology Staff and are the responsibility of the individual data owner.

Software Installation

- The College will provide licensed software for College owned computers as part of a standard configuration. Any additional software installed on a 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 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 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.

Software Approval

- If the software does not appear on the published Approved Software List, then a software approval online request form must be completed and approved prior to any software install. This includes, but is not limited to, PC’s, workstations, Macs and laptops.
- **Section (1) Academic (Book adoption or Non-Academic requests refer to section 2)**
  1. Complete an online software approval request form with the appropriate departmental associate dean’s approval. A helpdesk service request will be created with the form information. The service request will be assigned to the campus where the request originated.
  2. The Campus Technology technical staff will conduct the physical software testing. The physical testing will test the software’s compatibility, security, performance and any other tests recommended by the College’s technical staff. An evaluation copy of the software, not a demonstration copy, may be needed.
  3. Upon approval from the Campus technical staff, the service request will be approved by the Campus Technology Officers/Director/Assistant Director of Information Technology.
  4. Software will be added to the published Approved Software list.
- **Section (2) Book Adoption or Non-Academic**
  1. Complete an online software approval request form. A helpdesk service request will be created with the form information. The service request will be assigned to the campus where the request originated.
  2. If this is the first request for this specific software, the Campus Technology technical staff will conduct the physical software testing. The physical testing will test the software’s compatibility, security, performance and any other tests recommended by the College’s technical staff. An evaluation copy of the software, not a demonstration copy, may be needed.
  3. Upon approval from the Campus technical staff, the form will be approved by the Campus Technology Officers/Director/Assistant Director of Information Technology.
  4. Software will be added to the published Approved Software list.

Hardware Approval

- If the hardware does not appear on the published Approved Hardware List, then an online Hardware request form must be completed and approved prior to placing a requisition for that hardware. This includes, but is not limited to, PC’s, workstations, Macs, laptops and servers.
  1. Complete an online hardware approval request form.
  2. A helpdesk service request will be created with the form attached.
  3. The service request will be assigned to the campus where the request originated.

4. If this is the first request for this specific hardware, the Campus Technology technical staff will conduct the physical hardware testing. The physical testing will test the hardware's compatibility, security, performance and any other tests recommended by the College's technical staff. An evaluation of the hardware, not a demonstration, may be needed.
5. Upon approval from the Campus technical staff, the form will be signed by the Campus Technology Officers/Director/Assistant Director of Information Technology.
6. Hardware will be added to the published Approved Hardware page.

Hardware Purchase Approval

- Computers and peripherals (printers, tablets, etc.) will go through a business approval process once the requisition is initiated by the end user. The requestor will be required to enter justification/reasoning for the hardware purchase. At some point during the approval process the Campus Technology Officer/Director/Assistant Director will review the request and either approve or reject the requisition.

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.

Mobile Device Criteria

The purchaser of any mobile device for instruction (classroom or faculty and staff) whether through college funding or grants must minimally provide the following criteria for evaluation during the creation of a requisition. In addition the Information Technology department has the right to encourage the use of approved and standard mobile hardware:

A. Non-Instructional Mobile Device Criteria

- The mobile device must be necessary for the employee's need for remote connectivity.
- The awareness of the operation and integration of the specific mobile technology is critical to the person's job description.
- The expressed utilization of the device is specifically for college business or instruction.

B. Instructional Mobile Device Criteria

The purchaser of any mobile device for instruction (classroom or faculty) whether through college funding or grants must minimally provide the following criteria for evaluation:

- A statement on how the device(s) will impact and enhance instruction and student success.
- A description on how that device is currently being utilized in the field of study. (Ex: Teachers are integrating iPads into the classroom – hospitals are integrating iPads into daily operations)
- List of software or applications needed programmatically for the device.
- If purchased as classroom units, funding for proper storage and security must be budgeted.
- If purchased as classroom units, the environmental impact on that room needs to be assessed by facilities and IT prior to purchase (electric, space, AC).

College Wide Printing

All Broward College employees are required to use the Ricoh multifunction devices (MFD) as their primary printing resource. Personal printers are not allowed. In the rare instance where a personal printer is required so an employee can complete their job duties, this request will be addressed accordingly. Standard classrooms are not outfitted with printers (excluding computer classrooms). If a classroom printer is needed for academic reasons it is the responsibility of the department to purchase and maintain supplies for the printer. This request must be made through your Campus Technology Officer/Director/Assistant Director of Information Technology. It is also the responsibility of each department head to inform their employees on the proper use of the Ricoh MFD's in order to fall within their budget limits. The location of each Ricoh MFD is determined and authorized by the department of Information Technology.

Computer Administrative Rights Approval

- A Computer Administrative Rights online request form must be completed and approved prior to any Computer Administrative rights being granted. This includes, but is not limited to, PC's, workstations, Macs and laptops.
  1. Requester completes the online service request form for Administrative Rights. The request, with attachment(s), if any, will be transferred to his/her supervisor on the originating campus.
  2. If the supervisor recommends approval of this request, then the request will be transferred to the Campus Technology Officer/Director/Assistant Director of IT.
  3. If the Director/Assistant Director recommends approval of this request, then the request will be transferred to the Campus Technology Officer. The request will be either approved or rejected.
  4. All service requests, approved or rejected, will be available within the IT Service Management system.

Anti-Virus and Malware

- 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 anti-virus detection software that detects viruses and prevents them from executing, 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 contact their respective Campus Information Technology Staff or the Help Desk at 954-201-7521.
- All software and files downloaded from non-Broward College sources via the Internet (or any other public network) will be screened with Broward College approved virus detection software.

The following activities are prohibited, unless written approval from Information 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.
- Unsecured transmission or storage of personally identifiable information.
- Confidential or sensitive data stored in an unencrypted format on portable machines or media.
- Any criminal activity or any conduct that violates applicable laws.

Standards by Device Category

Academic

Features	Podiums	Self-Registration	Open Labs	Computer Classrooms	Laptop Carts	Checkout Laptops	Testing Centers
Base Software Image	X	X	X	X	X	X	X
Login and Network Access	X	X	X	X	X	X	X
Auto Login							X
Manual Login	X	X	X	X	X	X	
USB	X	X	X	X	X	X	X
DVD Drives	X		X	X			X
App Store Access	X			X	X		
Antivirus	X	X	X	X	X	X	X
Operating System Updates	X	X	X	X	X	X	X
3rd Party Updates	X	X	X	X	X	X	X
Date Time Clock							
Backups							
H, U and P Drive	X		X	X	X		

Standards by Device Category

Administration

Features	Employee Desktop	Employee Laptop	Employee Telecommuting
Base Software Image	X	X	X
Login and Network Access	X	X	X
Auto Login			
Manual Login	X	X	X
DVD Drives	X		Some Models
App Store Access	X	X – On-Campus	X – VPN
Antivirus	X	X	X
Operating System Updates	X	X	X
3rd Party Updates	X	X	X
Date Time Clock			
Backups			
H, U and P Drive	X	X	X

Standards by Device Category Definitions:

- **Base Software Image:** The college-wide standard software image, is the base software image that consists of the most frequently used college-wide applications such as: Microsoft Office, Acrobat Reader, and Antivirus.
- **Auto Login:** The auto login process was created to allow for non-students and students to access systems used as kiosks or testing center computers.
- **Manual Login:** The manual login refers to a user signing in to a computer using their username and password supplied by the College.
- **USB:** Refers to the availability of USB 2.0 and/or 3.0 ports on the computers for the installation of various peripherals and external thumb drives.
- **DVD drives:** Availability of a CD/DVD and in many places Blu-Ray drives.
- **App Store Access:** Access to the Microsoft Broward College App Store. Broward uploads many applications to this app store so users can do self-installations. Details of this service can be found in the IT Knowledge base.
- **Antivirus:** Protection against computer viruses and malware. This will include active protection by scanning new files and also periodic system scanning.
- **Operating System Updates:** Updates to the base operating system, this can be Mac OSX and Windows 7/10.
- **3rd Party Updates:** Updates to known applications installed on computers. Applications such as: Google Chrome, Firefox, Java, etc.
- **Backups:** Backups of local files on the desktop or laptop.
- **H/U/P Drives:** Broward College network shares: H – Home Drive, U- Communities Drive and P – Departmental Drive. All shared storage is periodically backed up by the IT department.