Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 1 of 21

Broward College provides all of 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.
- Workday is Broward College's computer application used for Human Resources, payroll and financials.
- College Integrated Database (CID) is Broward College's student ERP computer application. CID is used to support and assist both student and business functions. Students will use applications integrated with CID to apply to Broward College for admissions, register and pay for classes, as well as viewing their grades.
- 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.
- 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 user ID 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 user ID. The employee is held responsible for all actions performed, and all data which is modified or retrieved under their user ID and password.
- User IDs, 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 must call the College Help Desk at 954-201-7521 to have their accounts re-activated.
- User IDs or passwords may not be embedded in a procedure, program, function key, logon profile or script, or non-encrypted password file.

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 60 days of last change.
- Passwords for domain and enterprise administrators will be required to change within 45 days of last change, all remaining users will be set to 60 days of last change.

Recommending Officer's Signature	Date:	President's Signature	Date:
Patti L Bamy	10/04/2013	J. David Armstrong Jr.	10/04/2013

- The password reuse policy will be set so that old passwords cannot be used for a period of 1 year.
- Passwords shall never be written down or e-mailed.
- 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.
- Passwords shall 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 (!,$,%,&….)
  5. Passwords transmitted or used online on other networks should be of different variation from those used within Broward College.

Temporary or Contracted Employees

- A temporary or contracted employee is a non Broward College employee who requires access to its network systems and applications
- All temporary or contracted employees must be issued a Broward College network account to utilize any IT resources.
- A Non-Employee Access form must be completed and approved by a Director or Dean and or above. This form should be sent to the helpdesk to initiate the provisioning process.
- A Fair Use and Information Security Affidavit must be signed by the temporary or contracted employee and attached to the helpdesk ticket.
- 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 submitting a helpdesk ticket when access is no longer needed.
- Technology staff will remove the employee from the de-provisioning exception table upon notification from the non-employee's supervisor that they no longer need access.

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 Form. The employee's supervisor must sign the form.
- The employee's job function and department requirements will determine the level of access to network directories and applications.

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 3 of 21

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 Access to the BC Network.
- Disabled user accounts will 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 complete a Personnel Recommendation form and submit it to Human Resources. Upon receipt, Human Resources will end the active assignment in CID. The employee will be automatically disabled on the date inputted by HR.
- Human Resources will notify Information Technology of all departing personnel so that access is removed in a timely manner. If an employee gives HR a two week notice, then HR should notify the Technology Staff within seven days of termination.
- The Technology Staff will disable all network and e-mail access 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.
- Monthly 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, Technology Staff will immediately disable an account upon written notification from Human Resources.

Default and Industry Known User IDs

- Upon installation of the software, personnel installing software will remove default and industry known user IDs and passwords. These defaults should be disabled and replaced by approved Broward College user IDs and passwords. If a default user ID 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 signed off the system after 20 minutes of inactivity. This will require the user to re-sign on to gain access to the system.

Recommending Officer's Signature	Date:	President's Signature	Date:
Patti L Bamy	10/04/2013	J. David Armstrong Jr.	10/04/2013

- 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 from 10 minutes of inactivity of the computer. This process requires the user to enter a password to again view the computer display and 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. (Ctrl + Alt + Delete)

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: is the individual's home/private directory and will be limited to 1GB per user.*
- *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 if they wish to request an increase of the network storage limit. These requests will be reviewed and approved by Technology Staff.*
- *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.*

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 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.

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 5 of 21

Software Approval

- If the software does not appear on the published Approved Software List, then a software approval 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 a software approval request form with the appropriate departmental associate dean's signature. E-mail the completed form to the helpdesk. A helpdesk ticket will be created with the form attached. The ticket 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, will be needed.
  3. Upon approval from the Campus technical staff, the form will be signed 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 a software approval request form. E-mail the completed form to the Helpdesk. A helpdesk ticket will be created with the form attached. The ticket 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, will be needed.
  3. Upon approval from the Campus technical staff, the form will be signed by the Campus Associate Deans of technology followed by the Campus Dean of Technology or Director of Systems and Campus 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 a 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 a hardware approval request form.
  2. E-mail the completed form to the Helpdesk.
  3. A helpdesk ticket will be created with the form attached.
  4. The ticket will be assigned to the campus where the request originated.
  5. 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 copy of the hardware, not a demonstration copy, will be needed.

6. Upon approval from the Campus technical staff, the form will be signed by the Campus Technology Officers/Director/Assistant Director of Information Technology.
7. Hardware will be added to the published Approved Hardware Page.

Hardware Purchase Approval

- Computers and peripherals (printers, tablets, etc.) will go through a Workday 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.

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 Workday:

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 Sharp multifunction printers (MFP) 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 labs). 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 IT. It is also the responsibility of each department head to inform their employees on the proper use of the Sharp MFP's in order to fall within their budget limits. Broward College students are not allowed to use the Sharp MFP's. The location of each Sharp MFP is determined and authorized by the AVP of Auxiliary Services.

Computer Administrative Rights Approval

- A Computer Administrative Rights 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 Section A (see Computer Administrative Rights Criteria form) and signs Section B of the Computer Administration Rights Request form. The requester must sign and attach a copy of the Computer Administrative Rights Request Procedure (this form) to the request form. The request, with attachment(s), will be transferred to his/her supervisor on the originating campus.
  2. If the supervisor recommends approval of this request and signs section B, then the request will be transferred to the Campus Technology Officer/Director/Assistant Director of IT.
  3. If the Campus Technology Officer/Director/Assistant Director recommends approval of this request and signs section B then the request will be transferred to the Chief Technology and Operations Officer.
  4. This request will be reviewed by the Chief Technology and Operations Officer. The request will be either approved or rejected. The request will then be transferred back to the originating Campus Technology Officer/Director/Assistant Director of IT.
  5. All forms, approved or rejected, will be scanned and filed by Campus Technology.

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 anti-virus detection software that detects viruses and prevents them from executing, 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 College sources via the Internet (or any other public network) must be screened with Broward College approved virus detection software.*

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 8 of 21

- *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.
- 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

- Podiums
    - Base Software Image
    - Podium PC's have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus. Podium PC's are reset upon power off or reboot, removing any files that are saved to the podium. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
    - Login and Network Access
    - Auto Login: The auto login process was created to allow adjunct faculty or new-hires to have immediate access to the teaching station. When the PC is powered on or re-booted, login is automatic with a generic user ID (i.e. s-podium) and password. This account is password protected

and has no access to the user and departmental drives. There are access exceptions that allow access to student data files and applications. When a computer is idle for 90 minutes, the screen-saver is activated. Users press any key to resume the session. No password is necessary.

- Manual Login: In the event that professors or employees require access to personal or departmental data, they need to log off the workstation, and log back in using their assigned username and password. To do so, they select "Logoff" from the "Start Menu" to end the auto logon session. The users' login window will be displayed. Users type in their username and password. Upon successful logon, they will have access to information on their assigned network drives (usually the "H" and "P" drives). Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the Screensaver is activated. Users must enter their password to resume the session.
- USB (Flash Drives),CD or DVD Drives
- Since the installation of software is not necessary, users are encouraged to use flash drives to view lessons or PowerPoint presentations. Presentations may also be downloaded from email to the podium and saved to the desktop. All files stored on the podium by users will be replaced at reboot.
- User Software Installation
- When college employees or students access a podium computer, they cannot install software. Faculty should make arrangements by registering a Helpdesk ticket for the installation of any needed software. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use.
- Please refer to the Broward College Approved Software List.
- Hardware Installs
- In the event that a piece of hardware requiring software installation is needed, the user should make arrangements by registering a Helpdesk ticket for the software installation needed for the operation of the hardware. A campus technician will contact the user to verify software license, image compatibility and schedule installation.
- Please refer to the Broward College Approved Hardware List.
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Active Antivirus protection is enabled and protects the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Since the podium workstation is protected from changes, there is no need for antivirus scanning of the local computer. Antivirus updates are applied as software vendors release them (see Client Software Updates for further explanation).
- PC Defragmentation

- Podium computers do not benefit from defragmentation utilities because they are protected from change.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and scheduled maintenance. Therefore, they are not available to the user. Users should use the Outlook calendar for scheduling and planning.

- Self-Registration
  - Base Software Image
  - Registration PC's have the College- wide standard software image. Registrations' PC's are meant to be used only for registration functions. In the event an errant piece of software is downloaded, the PC's are reset upon power off or reboot, removing any files that are saved to the PC. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
  - Login and Network Access
  - Registration PC's use auto login. These PC's are to be used only for self-registration and registration related activity.
  - USB (Flash Drives),CD or DVD Drives
  - USB drives, CD's or DVD's are not to be used on Registration PC's.
  - User Software Installation
  - None
  - Hardware Installs
  - None
  - Windows Updates
  - Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
  - Antivirus
  - Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet. There is no need for antivirus scanning of the local computer.

Antivirus updates are applied as software vendors release them (see Client Software Updates for further explanation).
  - PC Defragmentation
  - Registration computers do not benefit from defragmentation utilities because they are protected from change.
  - Client Software Updates i.e. Adobe, Flash…
  - Because of the static nature of Registration and Student E-mail stations, they are updated at the time of re-imaging.
- Open Labs
  - Base Software Image
  - Open Lab PC's have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus. Open Lab PC's are reset upon power off or reboot, removing any files that are saved to the desktop. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
  - Login and Network Access
  - Auto Login: The auto login process was created to allow students to have immediate access to the open lab PC's. When the PC is powered on or re-booted, login is automatic with a generic user ID (i.e. 71-224) and password. This account is password protected and has no access to the user and departmental drives. There are access exceptions that allow access to student data files and applications. When a computer is idle for 10 minutes, the screen-saver is activated. Users need to press any key to resume the session. No password is necessary.
  - Manual Login: In the event that professors or employees require access to personal or departmental data, they need to log off the workstation, and log back in using their assigned username and password. To do so, they select "Logoff "from the "Start Menu" to end the auto logon session. The users' login window will be displayed. Users type in their username and password. Upon successful logon, they will have access to information on their assigned network drives (usually the "H" and "P" drives). Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the Screensaver is activated. Users must enter their password to resume the session.
  - USB (Flash Drives),CD or DVD Drives
  - Users are encouraged to use flash drives to view lessons or PowerPoint presentations in the Open Lab. Users can also download presentations from email to the PC and save them to the desktop. All files stored on the PC by users are replaced at reboot.
  - User Software Installation
  - When users or students access a computer in an Open Lab, they cannot install software.
  - Please refer to the Broward College Approved Software List
  - Hardware Installs

- When users or students access a computer in an Open Lab, they cannot install hardware.
- Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Active Antivirus protection is enabled and protects the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Since the workstation is protected from changes, there is no need for antivirus scanning of the local computer. Antivirus updates are applied as software vendors release them (see Client Software Updates for further explanation).
- PC Defragmentation
- Lab computers do not benefit from defragmentation utilities because they are protected from change.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Therefore they are not available to the users in Open Labs.

- Dedicated Labs
  - Base Software Image
  - Dedicated Lab PC's have the College- wide standard software image installed. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus. Dedicated Lab PC's are reset upon power off or reboot, removing any files that are saved to the PC. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
  - Login and Network Access
  - Auto Login: The auto login process was created to allow students to have immediate access to dedicated lab PC's. When the PC is powered on or re-booted, login is automatic with a generic user ID (i.e. 71-224) and password. This account is password protected and has no access to the user and departmental drives. There are access exceptions that allow access to student data files and

applications. When a computer is idle for 10 minutes, the screen-saver is activated. Users press any key to resume the session. No password is necessary.

- Manual Login: In the event that professors or employees require access to personal or departmental data, they need to log off the workstation, and log back in using their assigned username and password. To do so, they select "Logoff "from the "Start Menu" to end the auto logon session. The users' login window will be displayed. Users type in their username and password. Upon successful logon, they will have access to information on their assigned network drives (usually the "H" and "P" drives). Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the Screensaver is activated. Users must enter their password to resume the session. Users should always log-off prior to leaving the dedicated lab computer.
- USB (Flash Drives),CD or DVD Drives
- Users are encouraged to use flash drives to view lessons or PowerPoint presentations. Users can also download presentations from email to the PC and save them to the desktop. All files stored on the PC by users are replaced at reboot.
- User Software Installation
- When users or students access a computer in a Dedicated Lab, they cannot install software. Faculty should make arrangements by registering a Helpdesk ticket for the installation of any needed software prior to class. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use. Please refer to the Broward College Approved Software List
- Hardware Installs
- In the event that a piece of hardware requiring software installation is needed, the user should make arrangements by registering a Helpdesk ticket for the software installation needed for the operation of the hardware. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Since the workstation is protected from changes, there is no need for antivirus scanning of the local computer. Antivirus updates are applied as software vendors release them (see *Client Software Updates* for further explanation).
- PC Defragmentation

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 14 of 21

- Lab computers do not benefit from defragmentation utilities because they are protected from change.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Therefore they are not available to the users in the Dedicated Labs.

- Laptop Carts
  - Base Software Image
  - Laptops have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus. Laptops are reset upon power off or reboot, removing any files that are saved to the laptop. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
  - Login and Network Access
  - Auto Login: The auto login process was created to allow students to have immediate access to the laptops. When the PC is powered on or re-booted, login is automatic with a generic user ID (i.e. 71-224) and password. This account is password protected and has no access to the user and departmental drives. There are access exceptions that allow access to student data files and applications. When a computer is idle for 10 minutes, the screen-saver is activated. Users press any key to resume the session. No password is necessary.
  - Manual Login: In the event that professors or employees require access to personal or departmental data, they need to log off the workstation, and log back in using their assigned username and password. To do so, they select "Logoff "from the "Start Menu" to end the auto logon session. The users' login window will be displayed. Users type in their username and password. Upon successful logon, they will have access to information on their assigned network drives (usually the "H" and "P" drives). Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the Screensaver is activated. Users must enter their password to resume the session. Users should always log-off prior to leaving the laptop cart computers.
  - USB (Flash Drives),CD or DVD Drives

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 15 of 21

- Users are encouraged to use flash drives to view lessons or PowerPoint presentations. Users can also download presentations from email to the PC and save them to the desktop. All files stored on the laptop by users are replaced at reboot.
- User Software Installation
- When college employees or students access a podium computer, they cannot install software. Faculty should make arrangements by registering a Helpdesk ticket for the installation of any needed software. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use.
- Please refer to the Broward College Approved Software List
- Hardware Installs
- In the event that a piece of hardware requiring software installation is needed, the user should make arrangements by registering a Helpdesk ticket for the software installation needed for the operation of the hardware. A campus technician will contact the user to verify software license, image compatibility and schedule installation.
- Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Since the workstation is protected from changes, there is no need for antivirus scanning of the local computer. Antivirus updates are applied as software vendors release them (see Client Software Updates for further explanation).
- PC Defragmentation
- PC computers do not benefit from defragmentation utilities because they are protected from change.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Therefore, they are not available to users of laptop cart computers. Laptop Short-Term Checkout

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 16 of 21

- Laptop Short-Term Checkout
  - Base Software Image
  - Laptops checked out for short-term usage have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus. Laptops are reset upon power off or reboot, removing any files that are saved to the laptop. This action is performed for security purposes and assurance that all users will have a consistent environment. This method applies to all supported operating systems including, but not limited, to Microsoft Windows.
  - Login and Network Access
  - Auto Login: The auto login process was created to allow students, faculty and staff to have immediate access to the laptops. When the laptop is powered on or re-booted, login is automatic with a generic user ID (i.e. 71-224) and password. This account is password protected and has no access to the user and departmental drives. There are access exceptions that allow access to student data files and applications. When a computer is idle for 10 minutes, the screen-saver is activated. Users press any key to resume the session. No password is necessary.
  - Manual Login: In the event that professors or employees are using the laptops on campus and require access to personal or departmental data, they need to log off the laptop, and log back in using their assigned username and password. To do so, they select "Logoff "from the "Start Menu" to end the auto logon session. The users' login window will be displayed. Users type in their username and password. Upon successful logon, they will have access to information on their assigned network drives (usually the "H" and "P" drives). Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the Screensaver is activated. Users must enter their password to resume the session.
  - Web Access to Drives: Employees have the ability to access Home (H:), Department (P:) and Community (U:) drives using the Internet. Using the web link, https://fsweb.broward.edu , the user will be directed to a secured log-in screen which when authenticated will provide access to all of the user's drives. Users should log-off prior to closing the internet connection.
  - USB (Flash Drives),CD or DVD Drives
  - Users are encouraged to use flash drives to view lessons or PowerPoint presentations. Users can also download presentations from email to the PC and save them to the desktop. All files stored on PC the laptop by users are replaced at reboot.
  - User Software Installation
  - When users or students check out a short-term laptop, they cannot install software. Users should make arrangements by registering a Helpdesk ticket for the installation of any needed software prior to checking out the unit. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use. All laptops will be reimaged upon return.
  - Please refer to the Broward College Approved Software List

Recommending Officer's Signature	Date:	President's Signature	Date:
Patti L Bamy	10/04/2013	J. David Armstrong Jr.	10/04/2013

- Hardware Installs
- In the event that a piece of hardware requiring software installation is needed, the user should make arrangements by registering a Helpdesk ticket for the software installation needed for the operation of the hardware. A campus technician will contact the user to verify software license, image compatibility and schedule installation. All laptops will be reimaged upon return. Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Since the workstation is protected from changes, there is no need for antivirus scanning of the local computer. Antivirus updates are applied as software vendors release them (see *Client Software Updates* for further explanation).
- PC Defragmentation
- Laptop computers will not benefit from defragmentation utilities because they are protected from change.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Therefore they are not available for users' laptops.

- Employee Desktop – Office
  - Base Software Image
  - Office PC's have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus.
  - Login and Network Access
  - The users type in their username and password. Upon successful logon, they will now have access to information on their network drives. Screensavers and session timeouts are now in effect to protect private information. In compliance with college policy A6Hx2-8.01(Account Log Off and

Power Management), when a computer is idle for 10 minutes, the screen saver is activated. Users must enter their password to resume the session.

- USB (FLASH DRIVES), CD or DVD Drives
- Users are encouraged to use flash drives to transport and backup critical information.
- User Software Installation
- Office users cannot install software applications or drivers. A helpdesk ticket must be submitted, and a technician will respond to perform the installation. A campus technician will contact the user, to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use. Please refer to the Broward College Approved Software List
- Hardware Installs
- Office users cannot install hardware such as iPods, scanners or internal hard disk drives. However, devices such as USB hard drives and thumb drives do not require installation and may be easily used. A helpdesk ticket must be submitted, and a technician will respond to perform the installation. A campus technician will contact the user, to verify software license, image compatibility and schedule installation. Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
- Antivirus
- Antivirus scans are performed on a weekly basis. Active Antivirus protection is enabled and protects the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Antivirus updates are applied as software vendors release them.
- PC Defragmentation
- PC Defragmentation will be displayed in the Advertised Programs Application located on the desktop. This will allow the end user to run the program. Please submit a Helpdesk ticket if performance issues persist.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 19 of 21

- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Therefore they are not available. Users should use the Outlook calendar for scheduling and planning.

- Employee Assigned Laptops
  - Base Software Image
  - Employee assigned laptops have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus.
  - Login and Network Access
  - Users type in their username and password. If on the campus, upon successful logon, they will now have access to information on their network drives. Home users will not have network access, but still must log-in to the computer. Upon successful logon, they will now have access to information on the local computer's drive. Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the screen saver is activated. Users must enter their password to resume the session.
  - Web Access to Drives: Employees have the ability to access Home (H:), Department (P:) and Community (U:) drives using the Internet. Using the web link, https://fsweb.broward.edu , the user will be directed to a secured log-in screen which when authenticated will provide access to all of the user's drives. Users should log-off prior to closing the internet connection.
  - USB (FLASH DRIVES), CD or DVD Drives
  - Users are encouraged to use flash drives to transport and backup critical information.
  - User Software Installation
  - Employees cannot install software applications or drivers. A helpdesk ticket must be submitted, and the laptop brought to campus. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since software not on the approved software list must go through the college approval process, adequate time must be provided prior to use. Please refer to the Broward College Approved Software List
  - Hardware Installs
  - Office users cannot install hardware such as iPods, Scanners, or internal hard disk drives. Devices such as USB hard disk drives and thumbs drives are accepted. A helpdesk ticket must be submitted, and a technician will respond to perform the installation. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Please refer to the Broward College Approved Hardware List
  - Windows Updates
  - Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee.
  - Antivirus

- Antivirus scans are performed on a weekly basis. Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Antivirus updates are applied as software vendors release them.
- PC Defragmentation
- PC Defragmentation will be displayed in the Advertised Programs Application located on the desktop. This will allow the end user to run the program.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software.
- Date & Time Clock - The date and time clock are used by Microsoft for critical system functions that are used for Operating System and Security updates and schedule maintenance. Users should use the Outlook calendar for scheduling and planning.

- Employee Home Issued PC's
  - Employee Home Issued PC's have the College- wide standard software image. The base software image consists of the most frequently used college-wide applications, such as Microsoft Office, Acrobat Reader, and Forefront Antivirus.
  - Login and Network Access
  - Users type in their username and password. Home users will not have network access, but still must log-in to the computer. Upon successful logon, they will now have access to information on the local computer's drive. Screensavers and session timeouts are now in effect to protect private information. When a computer is idle for 10 minutes, the screen saver is activated. Users must enter their password to resume the session.
  - Web Access to Drives: Employees have the ability to access Home (H:), Department (P:) and Community (U:) drives using the Internet. Using the web link, https://fsweb.broward.edu , the user will be directed to a secured log-in screen which when authenticated will provide access to all of the user's drives. Users should log-off prior to closing the internet connection.
  - USB (FLASH DRIVES), CD or DVD Drives
  - Users are encouraged to use flash drives to transport and backup critical information.
  - User Software Installation
  - Home users cannot install software applications or drivers. A helpdesk ticket must be submitted, the CPU brought into the campus, and a technician will perform the installation. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Since

software not on the approved software list must go through the college approval process, adequate time must be provided prior to use. Please refer to the Broward College Approved Software List

- Hardware Installs
- Home users cannot install hardware such as iPods, Scanners, or internal hard disk drives. Devices such as USB hard disk drives and thumbs drives are able to be used. A helpdesk ticket must be submitted, the CPU brought into the campus, and a technician will perform the installation. A campus technician will contact the user to verify software license, image compatibility and schedule installation. Please refer to the Broward College Approved Hardware List
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee. Home users will need to bring their CPU back to campus for Windows updates.
- Antivirus
- Antivirus scans are performed on a weekly basis. Active Antivirus protection is enabled and will protect the workstation and network from files that are accessed via the Internet or transported from USB drive or other portable media. Antivirus updates are applied as software vendors release them. Home users will need to bring their CPU back to campus for antivirus updates.
- PC Defragmentation
- PC Defragmentation is handled by submitting a helpdesk ticket and performed by a member of the campus technology staff.
- Client Software Updates i.e. Adobe, Flash…
- Software vendors often provide new releases with provisions to be automatically installed as soon as they are released. However, installation of these service releases can and has impacted educational software, and has prevented this software from functioning. After a software update, (specifically, Adobe products in this case), the technology support team will evaluate the impact of this update on the installed educational software as well as on the online products, such as D2L and WebCT. In the past, Java releases have caused numerous problems with updates and incompatibility. After the "update" has been verified, a college-wide, update will be distributed at one-time to make sure that all college computers are operating with the same software. Home users will need to bring their CPU back to campus for software updates.
- Windows Updates
- Mandatory Windows updates are being installed without user intervention. These updates are distributed only after they have been downloaded and tested by the imaging committee. Home users will need to bring their CPU back to campus for Windows updates.
- Date & Time Clock - The date and time clock are used for critical system functions that are used for Operating System and Security updates and schedule maintenance. Users should use the Outlook calendar for scheduling and planning.