BROWARD COLLEGE

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 1 of 8

EMPLOYEE PROCEDURE

Broward College provides all its employees with a College Network and Internet access so that they can perform their job functions and duties. Use of the College Network shall be based on college operational business and/or academic needs.

Purpose and Network Account Creation

- The purpose of the Network and Software Usage Policy and Procedures is to provide a secure 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.
- User provisioning refers to the process of creating a user account that grants access to the college's network, applications, email, file storage, printing and other resources. Once defined in the college's Enterprise Resource Planning (ERP) system, a user is automatically granted access to all necessary systems and applications.
- The level of network access to system resources and applications will be determined by the employee's job function and departmental requirements. Users may receive additional access to other systems with documented authorization from their supervisor and/or application/data owner.
- All access rights will be set to the minimum necessary level for users to effectively perform their job functions.
- All user accounts must include a username, a strong password, and utilize Multi-Factor Authentication (MFA) via a mobile device or another approved physical device by the college's Information Technology Department. Depending on the sensitivity of information being accessed, multiple layers of MFA may be required. It is strongly recommended that personal mobile devices used for MFA are protected with biometric features (e.g. Face Recognition) or a 6-digit passcode.

Account Logins

- Each employee will be assigned a unique username and will be accountable for all actions taken and data modified or accessed under their account.
- Employees are responsible for safeguarding their accounts. Account credentials, passcodes, passwords, and similar information must not to be shared with anyone under any circumstances.
- Standard user accounts are limited to five incorrect sign-on attempts. After the fifth attempt the account is automatically locked. Employees can contact the College Helpdesk for account assistance.

Account Passwords

- All user accounts must include a strong password.
- The password, at a minimum, must be twelve characters in length.
- Passwords must contain characters from each of the following categories:
  1. English uppercase characters (A to Z)
  2. English lowercase characters (a to z)

Recommending Officer's Signature	Date:	President's Signature:	Date:
Raj Mettai	12/03/24		12/03/24

3. Numeric characters (0 to 9)
4. Non-alphanumeric characters (!,$,%,&,@….)

- Passwords must not contain the user's first name, middle name or last name.
- Passwords for standard users are required to be changed according to the guidelines outlined in the IT Security Privileged Accounts document.
- Passwords for Information Technology domain, enterprise administrators and privileged accounts will conform to the requirements 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.
- Users must not use the same password at the College for other services external to the College.

Users must not embed usernames and/or passwords in procedures, programs, function keys, logon profiles, scripts or non-encrypted password files.

Temporary or Contracted Employees

- A temporary or contracted employee is a contingent worker or non-Broward College employee who may require access to the college's network, systems and applications.
- Contingent workers may be issued a Broward College network account.
- The college's Enterprise Resource Planning (ERP) system is used to provide and manage accounts for contingent workers at the College.
- A College Information Security Affidavit must be signed by the temporary or contracted employee or their employer when deemed necessary.
- All temporary or contracted contingent worker access requests must have a start and end date.
- The person requesting access for the contingent worker is responsible for terminating the contingent worker in the college's Enterprise Resource Planning (ERP) system, when access is no longer needed.
- Information Technology staff will disable the contingent worker's account upon termination notification.

Account Modification

- For access level changes to a standard user account for employees or contingent workers, the Information Technology department must receive a completed Privileged Access Request Form initiated by the employee's supervisor.
- The employee's job function and department requirements will determine the level of access to network resources, applications and data.

BROWARD COLLEGE

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 3 of 8

Account Removal

- De-provisioning is the removal of a user's account from email, file storage, applications, and other college network resources.
- Disabling an account removes a user's ability to log into the college's network.
- Disabled user accounts may exist for a period of 2 years or more before being permanently de-provisioned.
- 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 Talent and Culture to determine that all necessary steps have been taken.
- Terminations are initiated within the college's Enterprise Resource Planning (ERP) system. The de-provisioning process will disable the account automatically. Talent and Culture may notify the Information Technology team of any accounts that need to be disabled manually and prior to the automatic termination process occurs.
- 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 Information Technology staff.
- 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/or Executive of Talent and Culture.

Default and Manufacturer Known User IDs

- Upon installation of software or hardware, Information Technology staff will remove default and/or manufacturer known usernames and passwords. These defaults should be disabled and replaced by approved Broward College usernames and passwords that conform to the IT Security Privileged Accounts document. If a default username cannot be replaced, passwords for these accounts shall be changed to conform to the IT Security Privileged Accounts document.

Account Logoff and Power Management Standards

- Users are required to use the 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. This configuration shall not be adjusted or removed.
- All users are required to lock their workstation when away from their desk or workspace.

Recommending Officer's Signature	Date:	President's Signature:	Date:
Raj Mettai	12/03/24		12/03/24

BROWARD COLLEGE

Title: College Network and Software Usage by Employees	Number: A6Hx2-8.01a
Policy Number: 6Hx2-8.01	Page: 4 of 8

File Storage and Collaboration Tools

- All network file storage should be used strictly for College business and/or academic purposes.
- Employees are required to monitor their network and email storage usage and delete obsolete or redundant files on a regular basis.
- Microsoft Office 365 OneDrive is the college's standard user's individual file store.
- Microsoft Office 365 Teams and SharePoint are for individual and group collaboration.
- P: Drive: is the departmental storage and should be used for sharing files within the department.
- U: Drive: is Community storage and should be used for sharing files within special groups.
- The use of local storage on a computer is deemed temporary and may be automatically deleted at any time by the College.
- Personal applications or files are not to be installed or stored on college devices.
- External storage devices, such as USB drives and flash drives are not supported by the College.

Web Filtering / Geo-Blocking

- The College reserves the right to use web or content filtering and geo-blocking to control internet access.
- The College reserves the right to restrict or deny access to certain domains, content applications and web-sites 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 or other devices as part of a standard computing configuration. Any additional software will be the responsibility of the requesting department or individual. Ex
- Software may only be installed if all the following conditions are met:
  1. The software is on the College's Approved Software list.
  2. Authorized Broward College employees or vendors will install software on college-owned devices.
- The following are prohibited on college-owned devices: illegal software, unlicensed applications, or personal software.
- 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.

Software Approval

If the software does not appear on the Approved Software List, then a software request form must be completed and approved prior to any software installation.

1. An online software approval request form must be completed with the appropriate departmental Associate Dean's approval. A helpdesk request will be created with the form information.

Recommending Officer's Signature	Date:	President's Signature:	Date:
Raj Mettai	12/03/24		12/03/24

2. The Campus Technology 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 required.
3. Upon approval from the Campus Technology staff, the service request will be approved by the Campus Technology Director/Assistant Directors. If approved the request will then be transferred to the Information Security department for final approval or rejection.
4. The approved software will be installed on the requested computer or on classroom computers.
5. Software will be added to the College Approved Software list.

Hardware Approval

If the hardware does not appear on the Approved PC Desktop, Laptop and Tablet 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, computers, workstations, Macs, laptops and servers.

1. Complete an online hardware approval request form.
2. A helpdesk request will be created with the form attached.
3. The helpdesk ticket will be assigned to the campus where the request originated.
4. If this is the first request for this specific hardware, the Campus Technology staff will conduct 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 device, not a demonstration unit, may be required.
5. Upon approval from the Campus technical staff, the form will be signed by the Campus Technology Director/Assistant Directors.
6. Hardware will be added to the Approved Hardware list.

Hardware Purchase Approval

Computers and peripherals (laptops, tablets, scanners, 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. The Campus Technology Director/Assistant Directors 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 up-to-date end-point protection software to detect, block and remove any virus, adware, malware or spyware.
- The user is responsible for all personally owned computing device support requirements, including the cost of repairs, diagnostics 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.
- The use of personal computers for connecting to the College's VPN is prohibited.

Mobile Device Criteria (Instructional)

The purchaser of any mobile device for instruction (classroom or faculty and staff) whether through college funding or grants must minimally provide the criteria listed 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 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. (e.g. 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 Information Technology prior to purchase (electric, space, AC).

Mobile Device Criteria (Non-Instructional)

- 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.

College-Wide Printing

Broward College employees are required to use the approved (multi-functional device) MFD as their primary printing resource. Personal printers are not allowed. In the event a personal printer is needed so an employee can complete their duties, a request must be submitted to the Information Technology department for approval. Standard classrooms are not equipped with printers (excluding computer classrooms). If a classroom printer is needed for academic purposes, it is the responsibility of the department to purchase and maintain supplies for the printer. This request must be made through a Campus Technology Director/Assistant Director. It is also the responsibility of each department head to inform their staff on the proper use of the MFDs and budget allowance. The location of each MFD is determined and authorized by the department of Information Technology. These locations may change at any time based on utilization. Only the Information Technology department is authorized to arrange the placement, removal or relocation of MFDs.

Computer Administrative Rights

A Request Administrative Access To a Workstation form must be completed and approved prior to any Computer Administrative rights are granted. This includes, but is not limited to, computers, workstations, Macs and laptops.

1. Requester completes the online Helpdesk request form for Administrative Rights. The request, with attachment(s), if any, will be transferred to his/her supervisor.
2. If the supervisor recommends approval of this request, then the request will be transferred to the Campus Technology Director/Assistant Directors for approval or rejection.
4. If approved the request will then be transferred to the Information Security department for final approval or rejection.
5. All service requests, approved or rejected, will be recorded in the Helpdesk system.

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 to perform periodic scans of the computer for viruses and other malicious types of programs.
- Information Technology Staff will configure the virus detection software 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.
- Users must not cancel automatic scanning or the update process. If such automatic activity interferes with the user's duties, the user should contact their respective Campus Technology staff or the IT Helpdesk.
- 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 end-point protection software.

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.

BROWARD COLLEGE

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

- 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.

Recommending Officer's Signature	Date:	President's Signature:	Date:
Raj Mettai	12/03/24		12/03/24