



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Employees	<b>Number:</b> <b>A6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 1 of 5

Broward Community 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 Community College’s infrastructure.
- User IDs and passwords control access to all Broward Community College Information Technology resources.
- For an employee to gain Network access, the Information Technology department will assign a user ID upon receipt of a completed Network Security Request Form. The new employee’s supervisor must approve and sign the form. To insure timely access to the system, supervisors are expected to process paper work within the first week of employment and/or assignment of subordinates.
- The employee’s job function and department requirements will determine the level of access to network directories and applications. Users can be provided access to other systems with written authorization from their supervisor and application data owner.
- All network accounts will require both a user ID and a password
- All network 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 is assigned a user ID and password and 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.
- Passwords will be required to change within 45 days of last change.
- The password, at a minimum, must be seven characters in length.
- Passwords shall never be written down or e-mailed.
- Passwords shall not be common words used at Broward Community 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.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
---	-----------------------	----------------------------------	-----------------------



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Employees	<b>Number:</b> <b>A6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 2 of 5

- 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 (!,\$,%,&....)
- Passwords transmitted or used online on other networks should be of different variation from those used within Broward Community College.

### Temporary or Contracted Employees

- Temporary or contracted employees gain access by the same procedures referenced above
- All temporary or contracted employees must be issued a Broward Community College network account to gain access to the College Network.
- Upon approval, the Information Technology department will provide a Broward Community College User ID and password for network access and application use for temporary or contracted employees.
- Prior to the creation of the User ID, a non-employee demographic record for temporary or contracted employees will be created in the Human Resources CID system for tracking purposes.

### 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.

### Account Removal

- Upon termination, all employees must have their Broward Community College network access permanently disabled.
- In preparation of a scheduled termination of an employee, the employee’s supervisor must complete an Account Change Removal Form and submit the form to Information Technology such that the form will be received prior to the scheduled termination date of the employee.
- 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 on their Human Resource record.
- Faculty and Adjuncts will have their network access removed and all files associated with the user account deleted after six months of not having an active assignment on their Human Resource record.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
---	-----------------------	----------------------------------	-----------------------



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Employees	<b>Number:</b> <b>A6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 3 of 5

- Weekly 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.
- All work study students will have their network access removed and all files associated with the user account deleted after 30 days of the last paycheck received.
- 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 Community 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**

- 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 mainframe 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.
- Users shall use the Windows screen saver feature on their workstation to blank out and lock their computer display screen after a period from one to ten 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 60 minutes of inactivity. Exceptions with approval from the campus Provost and or Vice President.

### **Network Storage**

- All network file storage should only be used for College 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.

<b>Recommending Officer's Signature</b> 	<b>Date</b> 5/1/08	<b>President's Signature</b> 	<b>Date</b> 5/1/08
---	-----------------------	----------------------------------	-----------------------



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Employees	<b>Number:</b> <b>A6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 4 of 5

- Drive S: is the college wide shared storage. This data is seen by everyone in the college. Drive S: was created as a temporary holding place when sharing data outside of your department. Files on the Drive S: are subject to removal without notice. Total storage capacity on Drive S: is limited to 700MB per user. Drive S: Should not contain data with usernames, passwords, credit card information or Social Security information.
- 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 Community College’s computers.
  - 2) Only authorized Broward Community 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.

### 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 an active virus detection software that 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 Community College sources via the Internet (or any other public network) must be screened with Broward Community College approved virus detection software.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
---	-----------------------	----------------------------------	-----------------------



**Broward  
Community  
College**

## Procedure Manual

<b>Title:</b> College Network and Software Usage by Employees	<b>Number:</b> <b>A6Hx2-8.01</b>
<b>Legal Authority:</b> Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties	<b>Page:</b> 5 of 5

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.
- Any criminal activity or any conduct that violates applicable laws.

<b>Recommending Officer’s Signature</b> 	<b>Date</b> 5/1/08	<b>President’s Signature</b> 	<b>Date</b> 5/1/08
--	-----------------------	---	-----------------------