

Dear Colleagues,

Broward College is currently responding to an Information Technology audit requested by the State Auditor General's Office, as well as many other Colleges state wide. As part of the audit we will be activating the password and screen saver policy. However you will **not** be required to change your password until the 90 day mark, sometime in April. You do have the option to change your password prior to the 90 days in the case you feel your password has been compromised. You will be notified 20, 10 and then 5 days prior to your password expiring. You have the option of resetting your password either from your desktop at work, or from any location outside of work with web access. This is the link to the new password reset webpage <https://reset.broward.edu>

Attached are the following documents:

- How to Reset your Password on Windows XP
- How to Reset your Password E-mail Policy
- How to Register a Broward College ID Card to a Sharp MFP
- How to Reset your Password Personal Logon Identity WebAccess

### **Important! First time logins only!**

**All Broward College employees will need to login to [reset.broward.edu](https://reset.broward.edu) site one time prior to changing your password in the future. You will be prompted by the enrollment Wizard to create a new Personal Logon Identity the first and time you login into this system.**

It is no longer necessary to contact the Helpdesk for password resets or if you are locked out due to more than **5** invalid logon attempts. You cannot re-use **your last 2 passwords**. When you do change your password you will also need to **re-register your PIN number** on your ID card for access to the Sharp devices. Note: You can also login manually to the Sharp devices. Your new password must follow the policy guidelines below.

## **Broward College – Policy & Procedures**

**Title:** College Network and Software Usage by Employees - **Number:** [A6Hx2-8.01](#)

**Legal Authority:** Florida Statutes: Chapter 119 – Public Records, Chapter 815 – Computer Related Crimes, Chapter 1001.65 - Community college presidents; powers and duties

## **Account Passwords**

- Passwords will be required to change within **90 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 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 (!,\$,%,&....)**
- Passwords transmitted or used online on other networks should be of different variation from those used within Broward College.

## 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.

## 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** 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 **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 Provost and or Vice President.
- Some device categories deviate from the standards; any deviations are documented in the Standards by Device Category Section.