

# ADMINISTRATIVE PROCEDURES

<b>Title: SYSTEM PASSWORDS</b>	<b>Identification:</b>	<b>9.06</b>
	<b>Page:</b>	<b>1 of 3</b>
	<b>Effective Date:</b>	<b>March 26, 2013</b>
<b>Authority:</b> <b>SBE 6A-14.0261</b> <b>FS 1001.64; 1001.65</b>	<b>Signature/Approval:</b>	<b>Dr. Ken Atwater</b>

## PURPOSE

This procedure establishes conditions for use of and requirements for appropriate security for the Hillsborough Community College Network Account (NetID). It sets standards for the creation of strong passwords, password protection, and frequency of password changes.

This procedure also establishes guidelines for changing default passwords for the software systems used by the College.

## PROCEDURE

The NetID is a User ID and password combination that serves as the primary digital identity at HCC when accessing computing resources. It provides the foundation for digital identity authentication and authorization.

The NetID provides access to a wide range of computing services such as the network access, email, and wireless access.

### 1. SCOPE

This procedure applies to all students, faculty, staff, alumni, retirees, third party vendors and other College affiliates who access HCC networks and computer systems.

### 2. SYSTEM REQUIREMENTS

- A user must to change the password on the first use.
- Employees will be required to change the passwords every 90 days. Students will be required to change the passwords every 180 days.
- Passwords should be a minimum of 8 characters long and contain numbers, letters and/or punctuation marks. Passwords longer than 8 characters are strongly recommended.
- When the Network Account password is changed, the account owner must create a password that is different from the last three passwords.
- A password can only be changed a minimum of once every 10 days. This is to prevent the premature cycling of passwords to maneuver around the password history clause. Should you need to have your password reset, contact the OIT Helpdesk.
- Consecutively entering an invalid password 5 times within 14 minutes will cause an account to be locked out.

# ADMINISTRATIVE PROCEDURES

Identification: 9.06

Page: 2 of 3

Effective Date :  
March 26, 2013

## 3. INDIVIDUAL RESPONSIBILITIES

NetID owners are expected to:

- Comply with the College's Acceptable Use Policy, the e-mail policy and the other policies.
- Create a strong password.
- Safeguard the password. For example, individuals should not write down or store the password on paper or on a computer system where others might acquire it. See *protect your password from misuse* procedure for additional guidelines.
- Never share the password with coworkers, supervisors and others.
- Reserve the NetID and password for authorized HCC systems and services only. Individuals should create a different username and password for external services such as stores, banks, music services, web sites, personally owned computers, or other systems.
- Be responsible for all activities associated with the NetID owner's accounts. All use of the HCC NetID is assumed to be performed by the person assigned to that account.
- Failure to conform to these requirements may lead to suspension of account privileges or other action as provided by College Policy, procedures or provision of law.

## 4. PASSWORD CREATION GUIDELINES

The software used to change passwords will screen for most of the following guidelines as an aid in creating secure passwords. This does not relieve a person of responsibility for creating and securing a good password.

- It must be at least eight characters in length. (Longer is strongly recommended)
- It should contain at least one alphabetic and one numeric character.
- It must be significantly different from previous passwords.
- It cannot be the same as the NetID.
- It should not start or end with the initials of the person issued the NetID.
- It should not include the first, middle, or last name of the person issued the NetID.
- Use of special characters (~!#\$%^&<>?/) in a password is considered a best practice.
- It should not be information easily obtainable about the NetID owner. This includes license plate, social security, telephone numbers, or street address.
- It should not include dictionary words.

## ADMINISTRATIVE PROCEDURES

---

Identification: 9.06

Page: 3 of 3

Effective Date :  
March 26, 2013

---

### 5. **SYSTEM PASSWORDS**

Most of the software systems are delivered with a default user ID and password. Information Systems is required to change default system passwords for software systems. It is expected that strong passwords be used for all software systems.

---

**HISTORY:** New