www.mybrcc.edu

TITLE:	**Password Protection**
EFFECTIVE DATE:	August 31,2014
LAST REVISION:	August 31,2014 Policy No. 3.1002

Policy Statement

1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any the college facility, has access to the college network, or stores any non-public the college information.

3. Policy

3.1. Password Creation

3.1.1. Users must not use the same password for the college accounts as for other non-the college access (for example, personal ISP account, option trading, benefits, and so on).

3.1.2. Where possible, users must not use the same password for various the college access needs.

3.1.3. All user-level passwords must contain 8 characters.

3.2. Password Change

3.2.1. All system-level passwords (for example, root, enable, server admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

3.2.2. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 90 days.

3.3. Password Reuse

3.3.1. All user-level passwords can not reuse pervious 3 passwords.

3.4. Password Protection

3.4.1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.

3.4.2. Passwords must not be inserted into email messages or other forms of electronic communication.

3.4.3. Passwords must not be revealed over the phone to anyone.

3.4.4. Do not reveal a password on questionnaires or security forms.

3.4.5. Do not hint at the format of a password (for example, "my family name").

3.4.6. Do not share the college passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

3.4.7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

3.4.8. Do not use the "Remember Password" feature of applications (for example, web browsers).

3.4.9. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.5. Application Development

Application developers must ensure that their programs contain the following security precautions:

3.5.1. Applications must not store passwords in clear text or in any easily reversible form.

3.5.2. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

3.6. Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

3.6.1. Passphrase should be long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

4. Policy Compliance

4.1. Compliance Measurement

The Chief Information Officer will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

4.2. Exceptions

The Chief Information Officer must approve any exception to the policy in advance.

4.3. Non-Compliance
An employee found to have violated this policy maybe subject to disciplinary action, up to and including termination of employment.

5. Definitions
Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

Source of Policy:	Information Technology	Responsible Administrator:	CIO
Related Policy:		LCTCS Policy Reference:	NA
		LCTCS Guideline Reference:	
Approved by:		Date:	08/31/14
Chancellor	Andrea Lewis Miller		