CITATION REFERENCE
Official Title: Information Technology: Password Policy
Abbreviated Title: Password Policy
Volume: CCGA Policies
Responsible Office:
Originally issued: January 13, 2014
Effective Date: January 13, 2014
Revised:

Policy: Information Technology: Password Policy

Policy Statement

The College of Coastal Georgia (CCGA) is committed to ensuring that its technology systems data are protected in accordance with the highest possible standards. Passwords serve as the first line of defense for protecting user accounts and sensitive data such as email, Banner, the CCGA campus network, and the learning management system. As such, all CCGA personnel and students are responsible for adhering to the steps outlined below to safeguard their user account passwords.

Reason for Policy

The purpose of this policy is to outline and document the guidelines for acceptable user account passwords. All users of technology at CCGA must adhere to this policy and the password requirements in order to obtain access to college systems and data.

Entities Affected By This Policy

All students, faculty and employees of the CCGA are covered by this policy.

Who Should Read This Policy

All students, faculty and employees should be familiar with this policy.

Contacts

Contact	Phone	E-Mail
Tim Moody	(912) 279-5762	tmoody@ccga.edu

Website Address for This Policy

Related Documents/Resources

Board of Regents IT Handbook section 5.8
http://www.usg.edu/information_technology_handbook/section5/tech/5.8_password_security

Definitions

These definitions apply to these terms as they are used in this policy:

- **Password:** A word or phrase entered at a computing device to gain access to some form college technology.

Overview

Users of technology at CCGA must use an individual password to gain access to systems and data. Examples of technology systems that require a unique user password are: email, my.ccga.edu portal, CCGA Intranet, Banner/COAST.

In order to insure that user passwords are secure and cannot be breached easily, CCGA requires that passwords be a minimum of 8 characters and be complex in that they include numbers and special characters as well as both upper and lower case letters.

Users can easily change their passwords at any time by visiting the account password management page at: http://accounts.ccga.edu

Password Criteria

Poor and weak passwords contain the following characteristics and **CANNOT** be used:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "<Company Name>", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords that have the following characteristics **CAN** be used and are recommendations to follow:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password standards and required change intervals
The password used to gain access to CCGA resources must be unique and used only for CCGA computing systems.

Users shall not use their CCGA passwords for any other personal passwords such as an Internet email account, Facebook, Twitter, etc.

Password requirements:

- All users will be required to change their passwords every 140 days.
- All user passwords must be a minimum of 8 characters in length
- All passwords must contain at least one upper case character
- All passwords must contain at least one lower case character
- All passwords must contain at least one number
- All passwords must contain at least one special character

Password Protection and prohibited actions
Users are prohibited from sharing passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential CCGA information.

Prohibited activities shall include:

- Revealing a password in an email message.
- Sharing password over the phone to anyone.
- Revealing a password to the boss.
- Talking about a password in front of others.
- Hinting at the format of a password (e.g., "my family name").
- Revealing a password on questionnaires or security forms.
- Sharing a password with family members.
- Revealing a password to co-workers while on vacation.
- Storing passwords on a computer without encryption.

Violations
Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. The appropriate college authorities and/or law enforcement agencies will process violations.

The prohibition against giving your password is state law. The Georgia Computer Systems Protection Act states that anyone convicted of disclosing their computer password is subject to fines of up to $5,000, up to one year in prison, or both.

Responsibilities
The responsibilities each party has in connection with this policy:

Party	Responsibility
Chief Information Officer	Ensure compliance with this policy.

Forms
None

Appendices
None