Cochise College
Administrative Policy

Category: Technology
Policy Number: 6055
Title: Passphrase Complexity & Protection Policy

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Cochise College's resources. The purpose of this policy is to establish a standard for passphrase/password control management at Cochise College including the creation of strong passphrases/passwords, protection of passwords and the frequency of renewing passwords.

Procedure: 6055.1
Scope

This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) used to gain access to a system, network or service in use at Cochise College. All users, including contractors and vendors with access to Cochise College systems, are responsible for taking the appropriate steps to select and secure their passwords.

This policy extends to all devices and software that make use of authentication to control access, including network devices such as firewalls, routers and switches, servers, computers including workstations and laptops, and software such as operating systems and applications that process, transmit or store sensitive college information that must be protected as defined in the college's *Data Classification Policy*.

Procedure: 6055.2
Roles & Responsibilities

College Employees and Contractors/Vendors: Understand their responsibilities for selecting and safeguarding passphrases/passwords. Immediately notify the Business Owner and Information Security Team (IST) if they suspect a password has been compromised.

College Leadership: Ensure that the resources they own comply with the guidelines set forth in this policy. Instruct users regarding system Passphrase/Password Policy. Report any suspected violations or password compromises to IST.

Information Security Team: The Information Security Team is responsible to ensure compliance with this policy as a component of the college's information security program. In addition, the Information Security Team is responsible to provide training to Business Owners and Users regarding this policy.

System and Application Administrators: Assist Business Owners with implementing measures to enforce this policy.

COCHISE COLLEGE

Procedure: 6055.3
Password Choice and Complexity

Passwords and passphrases are synonymous and essentially serve the same purpose of preventing unauthorized access to secure services or information. Passwords are generally short and can be more difficult to remember and easier to crack. Passphrases are typically easier to remember and type and are considered more secure due to their overall length. An example of a passphrase:

> The phrase "The soccer team won the championship"
>
> Translated to the passphrase "The$occerTe@mwontheChamp1on$hip!"

All users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords.

The following requirements are to be adopted for the selection of strong passwords (note that "Password" applies to both passwords and passphrases unless otherwise noted):

- Passwords/Passphrase should be a minimum of twelve (12) characters in length and constructed of at least one character from each of the following lists:

    1. Uppercase alphabetic (A-Z)
    2. Lower case alphabetic (a-z)
    3. Numbers (0-9)
    4. Special Character, e.g. ! $ % & , ( ) * + - . / ; : < = > ? [\ ] ^ _ { | } ~ # " @ and the 'space' character

- Passwords less than sixteen (16) characters in length should <u>not</u> contain any of the following:
    - A word or series of words that can be found in a standard dictionary of any language, dialect, jargon or slang
    - A word with a number added to the beginning or end, e.g. secret1 or 1secret
    - Word or words spelled backwards
    - Word or number repetitive or sequence patterns, e.g. aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Based on personal information, such as a user id, family or children's name, pet, fantasy character, address, birthday, etc.
    - Computer terms and names, commands, sites, companies, hardware or software

- Mandatory password changes will be required twice a year. Passwords will automatically expire at regular intervals and require the user to reset the password in accordance with the requirements for that system.
- Passwords must be changed immediately upon:
    - Initial user logon after a password has been assigned or reset
    - If it is suspected that the password has been compromised
    - Upon the departure of personnel with access to system accounts
- New passwords should be screened, where possible, against lists of commonly used or compromised passwords.
- Password "lockout" features should be enabled on any systems where it is available and reasonable to implement. Users should be locked out of systems after five (5) unsuccessful attempts within a thirty (30) minute period of time. Access should be denied for thirty (30) minutes or until reset by authorized staff.
- Two-factor authentication solutions should be adopted where possible, especially for accounts accessing confidential or restricted use data or privileged systems or application accounts.

Procedure: 6055.4
Password Protection

The following practices are recommended for password protection:

- Passwords should not be reused.
- Passwords should be memorized and never written down.
- Never reveal a password or hint at its format to anyone, e.g. via email, questionnaire or form. Office of Technology Services (OTS) staff will never make the request to reveal your password. Report any demand to reveal a password to the Information Security Team.
- Passphrases should not be plainly visible in clear text on a screen, hardcopy or on any other output devices.
- Passwords should not be stored in electronic form – in computer files or on portable devices such as USB memory keys unless strongly encrypted.
- Passwords should not be stored in browser caches or other "auto complete" types of features available in browsers and other application software. These password "memorization" functions should be disabled and never utilized.
- Passwords must not be inserted into email messages or other forms of electronic communication without the use of strong encryption.
- Do not use the same password for Cochise College accounts as for other external non-Cochise access (e.g., personal ISP account, option trading accounts, benefits accounts, etc.).

- Accounts or passwords should not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Password resets and the addition, deletion, and modification of user IDs, credentials and other identifier objects must only be done by authorized members of Office of Technology Services (OTS).
- OTS staff will ensure the identity of the requester is first verified prior to performing password or account modifications.
- Systems and applications should wherever possible enforce the selection, protection and use of passwords meeting the above criteria.

Procedure: 6055.5
Compliance

This policy is a component of Cochise College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA and other regulations.

Procedure: 6055.6
Exceptions

In the event a device or software cannot support this policy compensating controls will be documented and used to mitigate the risk of a breach by a compromised passphrase/password.

The Chief Technology Officer (CTO) or a designated appointee is authorized to make exceptions to this policy.

Procedure: 6055.7
Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The college reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure: 6055.8
Definitions

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Passphrase: A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally derived from a phrase that is more easily remembered and longer for added security.

Password: A sequence of alphanumeric and special characters entered in order to gain access to a computer system or resource.

Strong Password: A password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

User: Any Cochise College faculty, staff, student or partner who has been authorized to access any college electronic information resource.