Password Complexity & Protection Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

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

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 Washtenaw Community College. All users, including contractors and vendors with access to Washtenaw Community 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*.

ROLES & RESPONSIBILITIES

College Employees, Students, and Contractors/Vendors: Understand their responsibilities for selecting and safeguarding passphrases/passwords. Perform password changes as requested. Required to immediately notify the

Help Desk or Information Security Office if they suspect a password has been compromised.

College Leadership: Ensure that the business processes and technologies utilizing passwords under their responsibility comply with the guidelines set forth in this policy. Report any suspected violations or password compromises to the Help Desk or Information Security Office.

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

Security Incident Response Team: Responsible to provide security incident management in response to reported incidents and passphrase/password compromises.

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

REQUIREMENTS & PRACTICES

All users are responsible for selecting and 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:

- Passwords should be a minimum length of twelve (12) characters. Alternatively, a longer passphrase may be used (as described below) with a minimum recommended length of twenty (20) characters. Passwords should be 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 and passphrases are synonymous and essentially serve the same purpose of preventing unauthorized access to secure services or information. Passwords are generally shorter 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 "My 2018 Ford Mustang is red"

  Translates to the passphrase "My18F0rdMust@ngi$R3d"

- It is recommended that passwords less than twenty (20) characters in length not 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.
  - Comprised of three (3) or more of the same character
  - 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

The following practices are recommended for password protection:

- Accounts or passwords should not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords should be memorized and never written down. Don't risk potentially exposing it to others.
- Never reveal a password or hint at its format to anyone, e.g. via phone, email, questionnaire or form. Information Technology Services (ITS) staff will never make the request to reveal your

password. Report any demand to reveal a password to the Information Security Office.

- The College will enforce a password change frequency of at least once a year, however it is recommended that passwords should be changed every 180 days
- 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 administrative accounts
- Passwords should not be reused
- Passwords 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 PDAs, cell phones, USB memory sticks, etc. unless strongly encrypted
- 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 your Washtenaw Community College account that you use elsewhere, e.g. don't use your Amazon, Netflix, bank account, benefits account, etc. password. Similarly, do not use your College password elsewhere.
- The use of password management applications designed for safe and secure storage is recommended, e.g. LastPass, over the use of browser password "memorization" functions and other "auto complete" types of features available in browsers and other application software.
- Password resets and the addition, deletion, and modification of user IDs, credentials and other identifier objects must only be done by authorized members of Information Technology Services (ITS)
- ITS staff will ensure the identity of the requester is first verified prior to performing password or account modifications

Those with administrative responsibilities on systems or services which manage passwords should ensure that:

- Passwords should automatically expire at regular intervals and require the user to reset the password in accordance with the requirements for that system
- 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 six (6) unsuccessful attempts within a thirty (30) minute period of time. Access should be denied for thirty (30) minutes or until reset by authorized staff.
- Systems and applications should wherever possible enforce the selection, protection and use of passwords meeting the above criteria

In the future, password self-service solutions will be adopted to provide end-users with the ability to change forgotten passwords via a series of pre-established (user composed) security questions and responses or other secure identity verification mechanisms (e.g. SMS or PDA application-based PIN response). Additionally, two-factor authentication solutions will be adopted where possible, especially for accounts accessing confidential or restricted use data or privileged systems or application accounts

COMPLIANCE

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

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 Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

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

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 Encryption: Strong encryption is provided by well-established encryption algorithms, e.g. AES, SSL, which utilize long cryptographic keys, typically 256 bits or longer.

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 Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Data Classification Policy

Request for Policy Exception

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO