Saint Michael's College

Password Standard

1.0 Purpose

This document describes the acceptable means for password construction, protection, and maintenance.

2.0 Password Construction

2.1 Passwords must be at least 8 characters long and no more than 28 characters.

2.2 Passwords cannot contain all or part of your Mikenet name or full name.

2.3 Your password must contain characters from at least 3 of the 4 categories listed here:

- Uppercase letters (A through Z)
- Lowercase letters (a through z)
- Numeric characters (0 through 9)
- Special (!@#$%^&*()_+) character

3.0 Password Management

3.1 Password 'Storage'

- Passwords should be memorized.
- Passwords must not be stored in a manner which allows unauthorized access. For example, writing the password down and attaching it to the monitor or placing it in a desk drawer or under the keyboard is unacceptable.
- Passwords must not be remembered by unencrypted computer applications such as email.
- Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.
- Computers must not be configured to login without a password. Exceptions may be granted for specialized devices such as kiosks which have extremely restricted accounts. Whenever possible, computer labs should be designed to authenticate each user individually for accountability purposes.

3.2 Password Aging

- Users must change their passwords at least every 90 days.
- Simply changing the case of one or more letters doesn't satisfy this rule (Password1 is viewed the same as PASSword1).
- Care must be taken to prevent the compromise of one username/password from compromising multiple systems or resources. For example, users must not use the username and password combination from any non-SMC account as the username and password for their SMC Mikenet account. This is especially important if the non-SMC system does not use encrypted authentication.

4.0 Password Transmission

4.1 Passwords may not be transferred electronically over the Internet using insecure methods. Insecure methods include Post Office Protocol (POP), Internet Mail Access Protocol (IMAP), File Transfer protocol (FTP), Hyper-Text Transfer Protocol (HTTP), and Telnet.

4.2 When it is necessary to disseminate passwords in writing, the recipient will take measures to protect the written password from unauthorized access. For example, after memorizing the password, one must destroy the written record.

4.3 When transmitting a password orally, take measures to ensure that the conversation is not overheard by unauthorized individuals.

5.0 Additional Password Considerations

5.1 System Administrators

- System administrators, or those serving that role, may need to create and disseminate passwords to others. Whenever possible, use a method of password creation that provides the password only to the intended end-user.
- System administrators must harden their systems to deter password cracking:

5.2 An automated method to mitigate "brute force" password attacks must be used. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location or at minimum alert the system administrator in real- time that an attack is underway so that manual action can be taken.

5.3 Logging must be set up to record all failed login attempts and preferably successful attempts as well.

5.4 Events Necessitating Password Change: if any of the following events occur, a password change will be mandatory:

- Unauthorized password discovery or usage by another person.
- System compromise (unauthorized access to a system or account).
- Insecure transmission of a password, for example via email or instant message. (Even an email transferred via secure Post Office Protocol (POP) or Secure Internet Message Access Protocol (S-IMAP) could be compromised at the Simple Mail Transport Protocol (SMTP) level or read while in your inbox- change the password anyway.)
- Accidental disclosure of password to an unauthorized person.
- Replacement of account user with another individual requiring access to the same account.
- Password is provided to IT support staff in order to resolve a technical issue (It is strongly recommended that IT support staff request an end-user password as a last resort.)
- A password is provided to the end-user and the system administrator knows the password. For example, the system administrator provides a new account password or has to reset an account password.

6.0 Password Guidelines

6.1 Unacceptable Methods to Create a Password:

- Do not use dictionary or actual words. Non-English words are no more secure than English words. (If you accidentally use a tiny dictionary word like "I", "a","an", or "if" in an otherwise secure password, that is fine.)
- Do not use words or numbers associated with you. Examples include:
  (1) Social security numbers
  (2) Names, family names, pet names
  (3) Birthdays, phone numbers, addresses

- Avoid using your login name or any variation of it as your password. If your login is ‘fredrick’, do not use substitution or letter reordering. Examples would be ‘fr3dr1ck’, where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.
- Password cracking tools are sophisticated and are able to crack passwords that are created using these unacceptable methods.

6.2 Acceptable Methods to Create a Password:

- Use a minimum of 6 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.
- Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use letters from a passphrase or sentence, e.g., “One ring to rule them all, one ring to bind them” results in the password of “1R2rtA,or2Bt” by using the first letter, capitalization, and some substitution.
- Use mixed case (upper & lower).
- Use punctuation symbols (Ex:_-+=!@%*&”:,./).