

Department:	CMC- IT-ADHICS- 011
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

PASSWORD SECURITY POLICY

1. PURPOSE:

- 1.1 To establish the standards for creation and management of passwords used in Canadian Medical Centre facilities.
- 1.2 The objective of this policy is to define and provide guidelines for Users in choosing secure passwords and identify protection controls of those passwords.

2. POLICY STATEMENT:

- 2.1 Passwords for access to the CMC network and computer systems must meet the following requirements:
 - 2.1.1 Consist of a minimum of 8 and a maximum of 16 characters.
 - 2.1.2 Contain a minimum of one upper-case letters
 - 2.1.3 Contain at least one number.
 - 2.1.4 Contain at least one special characters from the following set:
 - 2.1.5 ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ { | } ~
- 2.2 Have a maximum password lifetime of 90 days.

3. SCOPE:

- 3.1 All Canadian Medical Center Group of Companies Staff for the following :
 - 3.1.1 Canadian Medical Center LLC
 - 3.1.2 Canadian Medical Center LLC Branch -2
 - 3.1.3 Canadian Medical Center LLC Branch - 3
 - 3.1.4 Canadian Medical & Rehabilitation Center LLC
 - 3.1.5 CMC First Aid Clinic

4. TARGET AUDIENCE

- 4.1 This policy applies to all Users of Canadian Medical Center Group of Companies (CMC) staff; All staff using HIS System, Active Directory and shared computer network.

5. RESPONSIBILITY

- 6.1 The Information Technology Department is responsible for development, maintenance, enforcement, and endorsement of the policy.
- 6.2 The Information Technology Department is responsible to support the relevant business unit / section in implementation of the defined controls and ensuring compliance with this policy.
- 6.3 All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
- 6.4 This Policy shall be implemented by the system administrators and designated personnel (if any).
- 6.5 System administrators and users assume the following responsibilities:

Department:	CMC- IT-ADHICS- 011
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

PASSWORD SECURITY POLICY

- 6.5.1 System administrator must protect the confidentiality of passwords on their systems and configure their systems to meet the requirements set forth in this policy.
- 6.5.2 Each user is responsible for all actions and functions performed by his/her account.
- 6.5.3 Users must create and manage passwords according to the standards outlined below.
- 6.5.4 Suspected password compromise must be reported to the IT Security Officer/IT Manager.

6. PROCEDURE:

6.1 Password Protection Requirements:

- 6.1.1 Passwords must never be shared or revealed to anyone other than the authorized account owner (unless approved by the IT Manager).
- 6.1.2 Users should never use their CMC network password for non-CMC "personal" accounts (e.g., personal email).
- 6.1.3 Passwords must never be written down or stored in a way in which they could be viewed by someone other than the authorized account owner. If a password must be stored, it must be encrypted using an encryption method approved by Information Security.
- 6.1.4 Systems will be configured to lockout user accounts after 10 unsuccessful login attempts. The account will remain locked reset by an IT Officer.
- 6.1.5 Passwords must be changed immediately if it is suspected that the user ID and password have been disclosed to an unauthorized person or if a system has been compromised or is under the suspicion of having been compromised.
- 6.1.6 To minimize the risk of someone guessing your password:
- 6.1.7 Use two or three short words that are unrelated.
- 6.1.8 Deliberately misspell words
- 6.1.9 Take the first letter from each word of a phrase.
- 6.1.10 Do not use any part of the account identifier (your login ID, name, etc.)
- 6.1.11 Do not use a proper name or any word in the dictionary without altering it in some way
- 6.1.12 Exceptions will be permitted only on receipt of written approval from Information Security. Information Security will retain documentation of currently permitted exceptions and will review them on an annual basis.
- 6.1.13 The Information technology officer/IT Manager must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

Department:	CMC- IT-ADHICS- 011
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

PASSWORD SECURITY POLICY

7. DEFINITIONS AND ABBREVIATIONS:

7.1	Password	A series of letters, numbers and/or symbols that is used to authenticate an individual's identity and which is used to grant access to the CMC management facilities.
7.2	Password lifetime	The length of time a password may be used before it can be changed.
7.3	User	Anyone who holds a valid account on the facility's network.
7.4	ADHICS	Abu Dhabi Healthcare Information and cyber security standards

8. DISTRIBUTION LIST:

On shareholder Policies HR

9. SPECIAL INSTRUCTIONS:

9.1 Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.

10. CROSS REFERENCE, RELATED LEGISLATION, FORMS, POLICY & DOCUMENTS:

10.1 Guidelines for the implementation of the Abu Dhabi healthcare information and cyber security standard (ADHICS) 2019 ADHICS-Implementation-Guidelines

10.2 https://www.getsafeonline.org/themes/site_themes/getsafeonline/download_centre/Sample_Acceptable_Usage_Policy.pdf

11. KEY RESULT AREAS:

11.1 The procedure is fully implemented if there are nil incidences of non-compliance with this policy.

12. AMENDMENT HISTORY:

Version	Revision Date	Description of Amendments	All pages
01	01/07/2020	New policy	All pages

13. APPENDIX:

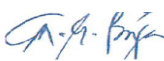
NA

14. APPROVALS:

Document Developed By:

Department:	CMC- IT-ADHICS- 011
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

PASSWORD SECURITY POLICY

IT Support	Mr. Muhamed Shifas Avudiyil		01/07/2020
	Name	Signature	Date
Document Developed & Reviewed By:			
IT supervisor/IT Manager	Mr. Yahiya Mannoparambil		01/07/2020
	Name	Signature	Date
Nurse Manager & Quality Control Supervisor	Ms. Monina Baja		01/07/2020
	Name	Signature	Date
Document Approved By:			
Chief Operating Officer/Chief Financial Officer	Mr. Imran Saleem		01/07/2020
	Name	Signature	Date