

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

1. PURPOSE

1.1 The purpose of this policy is to establish security requirements in order to ensure controlled access to the information resources of Canadian Medical Center Group of Companies are controlled, and to minimize probabilities of information leakage, tampering, loss and system compromises.

2. POLICY STATEMENT

2.1 Canadian Medical Center Group of Companies must ensure appropriate controls are in place to establish secure areas. Sensitive information and assets must be protected while considering the safety of personnel. Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

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
- 3.1.6 CMC Healthcare L L C - SOLE PROPRIETORSHIP L.L.C.

4. TARGET AUDIENCE

4.1 This policy applies to all Users of Canadian Medical Center Group of Companies who use or require Logical Access to information processing facilities as part of their day-to-day activities.

5. RESPONSIBILITY

- 5.1 The Information Technology Department is responsible for development, maintenance, enforcement and endorsement of the policy.
- 5.2 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.
- 5.3 All Users are responsible to read, understand and adhere to this policy in their day to day activities.
- 5.4 The Information Technology Department is responsible to conduct awareness about the policy to Users.
- 5.5 Senior Management are responsible for compliance to this policy within their area(s) of concern.
- 5.6 The Information Technology Department shall maintain a list of Users having primary responsibility for information assets/systems/application and the information assets to which their authority extends.
- 5.7 Information Technology Department are responsible to implement the defined security controls on the respective information systems.

6. PROCEDURE:

6.1 Physical Access Provisioning & De-Provisioning

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

- 6.1.1 Access to Canadian Medical Center's premises will be granted as per the procedure of physical access of the Entity to be developed by the facility based on the business needs.
- 6.1.2 Visitors' access, including third party vendors, to Canadian Medical Center premises will be granted on case by case basis as per the Entity procedures.
- 6.1.3 De-Provisioning of physical access is valid under the following circumstances:
 - 6.1.3.1 End of employee's service
 - 6.1.3.2 Vendors/Contractors completing their engagement or as per the expiration of the temporary gate pass.
 - 6.1.3.3 If requested by the Head of the department which the user belongs to.
 - 6.1.3.4 If user found to have violated the policy or misused the provided access in any mean.

6.2 Identification Cards:

- 6.2.1 All employees shall wear the employee ID card issued by the HR department while they are inside the premises of Canadian Medical Center.
- 6.2.2 All non-employees (contractors, consultants, suppliers, vendors, partners, etc.) shall wear respective identification cards while they are within the premises of Canadian Medical Center.
- 6.2.3 The ID cards shall be placed in a manner that is clearly visible.
- 6.2.4 All new employees shall be primarily issued with temporary ID cards, till they are issued with their ID cards.
- 6.2.5 All Users shall return their ID card in the event of resignation, termination, transfer or retirement to HR Department.

6.3 Physical Access Control

- 6.3.1 Physical access to areas containing critical information and information processing systems shall be controlled and allowed for authorized Users only.
- 6.3.2 Entry to Canadian Medical Center premises shall be provided to visitors only after notifying the particular employee whom the visitor is asking to visit and verifying the purpose of visit with him/her.
- 6.3.3 Visitors shall be escorted at all times by authorized employee while in Canadian Medical Center premises.
- 6.3.4 Users shall refrain from entering critical areas without getting proper approval from authorized employee.
- 6.3.5 All areas that contain critical information and information processing facilities shall be fitted with strong physical access control mechanisms.
- 6.3.6 Physical access shall be deactivated or revoked for terminated Users.
- 6.3.7 Physical access rights of all Users shall be reviewed on a periodic basis (minimum once every six months) by the Information Technology Department in coordination with respective Managers / Supervisors responsible of critical information and information processing facilities in order to check if there are access rights that are no longer needed.
- 6.3.8 The names and designations of Users who have the right to authorize others to have access to areas that contain critical information or critical information processing facilities shall be maintained by the Information Technology Department in coordination with the respective Managers / Supervisors.
- 6.3.9 Users shall keep their cabinets/drawers locked when leaving the offices at the end of the day.

6.4 Secure Working Areas

- 6.4.1 Users shall refrain from eating or drinking near information processing facilities and equipment. Food shall be consumed at the designated place allocated by the Entity.

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

6.4.2 Users shall keep electronic media such as DVDs; Flash drives etc., containing confidential information inside the locked cabinets or drawers thus protecting them from attempts of unauthorized access.

6.4.3 Users shall refrain from smoking inside the premises of Canadian Medical Center apart from the designated smoking zones.

6.4.4 All documents shall be protected in accordance with their classification level and specific protection requirements.

6.5 User Access Provisioning

6.5.1 All formal procedure shall be in place for user registration & de-registration.

6.5.2 All access privileges shall be allocated on a “need basis” – only the minimum privileges required for the user’s functional role shall be allocated.

6.5.3 User access provisioning should be initiated in the following cases, but not limited to:

6.5.3.1 New employment

6.5.3.2 Users being promoted/demoted/transferred

6.5.3.3 Temporary assignment of job responsibilities

6.5.3.4 Access to external Users (such as vendors, contractors and partners) & third parties, etc.

6.5.3.5 All high privilege access shall be provided only after approval of Information Technology Department and Assigned person from Top Management.

6.5.3.6 Any information systems’ service account or generic account shall be created with approval from the Information Technology Department or to owner assigned to ensure accountability.

6.5.3.7 The list of service accounts or generic accounts shall be identified & documented by respective systems administrators.

6.6 User Access De-Provisioning

6.6.1 User Access de-provisioning is valid under the following circumstances.

6.6.1.1 End of User’s service.

6.6.1.2 If requested by the Manager of the concerned department.

6.6.1.3 External Users such as (vendors, contractors and partners) & third parties, etc., completing their engagement.

6.6.1.4 If a User is found to have violated any policy or misused the provided access in any mean.

6.6.2 The HR department shall be responsible of initiating the de-provisioning of user access for the resigned or terminated user, in coordination with the respective manager of the user.

6.6.3 The HR department shall be responsible of defining procedure for access revocation due to resignation or termination of employees.

6.6.4 The Information Technology Department shall be responsible of ensuring access revocation of the resigned or terminated user from all information processing facilities which the user had during the tenure of employment with Canadian Medical Center.

6.6.5 On completion of revocation of access, the IT Department Head of the Department shall be responsible of verifying and signing the access termination of the resigned or terminated user shall review and endorse the access termination evidences.

6.7 User Access Authentication

6.7.1 Users shall be provided with a unique User ID combined with a password for authentication, as a minimum.

6.7.2 Users shall be provided with one ID per system or application with the appropriate privileges mapped to carry out their day to day activities.

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

6.7.3 IT Department head shall assign unique user identification to the authorized user upon notification of access request approval.

6.8 Access Related to Third Party (vendors/consultants)

6.8.1 All contracts with third party (such as vendors, contractors and partners) & third parties shall include security requirements and clauses outlining the access requirements to CMC systems.

6.8.2 The IT Manager shall review and agree on any special requirements related to providing access to vendors/consultants and ensure including such requirements in the contracts/agreements.

6.8.3 The IT Manager reserves the right to require additional access controls to be applied in relation to any contract.

6.9 Review of Access

6.9.1 The IT Department shall generate Users list from the Information Systems on a regular basis, at least twice a year. This list shall be reviewed by Business Owner and the directors/managers of the users, to identify redundant, dormant, or expired user accounts, or incorrect privileges.

6.9.2 User accounts that are inactive for a period of 3 months shall be disabled by System Administrators on a regular basis.

6.9.3 All privileged and administrators accounts shall be reviewed on a quarterly basis, and changes to such accounts shall be logged for periodic review.

6.10 Network Security

6.10.1 Provisioning or de-provisioning of access to Canadian Medical Center network & its services shall be carried out in accordance with the Access Control Policy and User access management procedures of CMC.

6.10.2 IT Department shall ensure that only authorized Users are able to access network resources.

6.10.3 Unwanted ports and services, configured on any network equipment, shall be disabled or removed.

6.10.4 For shared networks, especially those extending across Canadian Medical Center's boundaries, strict access control shall be implemented to restrict unauthorized access as per business requirements.

6.10.5 The configurations of all network and security devices shall be backed up as per the Entity Information-Data Backup Policy.

6.10.6 The default passwords of network and security devices shall be changed by the IT Department immediately after installation.

6.10.7 All Passwords of network or security devices shall comply with the Entity Password Policy.

6.10.8 Network and security devices placed on all external network connections, shall display banner message warning unauthorized Users that unauthorized use is prohibited (e.g. If you are NOT authorized to access this equipment, Please log out immediately).

6.10.9 All network and security devices shall be protected against physical and environmental threats in accordance with the facility physical and environmental security policy.

6.10.10 Failover mechanism shall be deployed when setting up all network devices, to avoid single point of failure that could cause the unavailability of the network services.

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

- 6.10.11 Segregation, in the form of multiple DMZ's, shall be implemented when publishing public facing services.
- 6.10.12 Change management procedure and proper authorization shall be followed prior to modifying configurations of any network and security device.
- 6.10.13 IT Department shall harden all network devices as per the approved minimum security baseline documents.
- 6.10.14 All Information systems shall be logged out or sessions terminated automatically after a defined period of inactivity

6.11 Remote Access Security

- 6.11.1 Provision of remote access shall be provided based on the need to know and need to use basis and after necessary approval.
- 6.11.2 IT Department shall only grant remote access to authorized personnel.
- 6.11.3 Remote access shall be authenticated using a two-factor authentication mechanism.

6.12 General Guideline on User Access

- 6.12.1 Users shall be held responsible for all activities carried out using their access accounts.
- 6.12.2 Users shall refrain from sharing or declaring any of their access control credentials with anyone.
- 6.12.3 The password of all generic accounts shall be changed immediately by the IT Department of the information systems when a User or Users of the account have resigned / terminated or transferred. A record shall be maintained for the change of password respectively.
- 6.12.4 Users shall be aware of their access rights and the terms & conditions for use in the respective information systems.
- 6.12.5 All User access request records shall be maintained for reference & audit process for a period of (to be decided by the facility based on the risk, business need and any legal or regulatory requirements applicable to the Entity or the specific information).
- 6.12.6 All records related to User access shall be destroyed on completion of the defined retention period.
- 6.12.7 Access to shared folders shall be authorized for business purposes only.
- 6.12.8 Users shall report any kind of misuse or unauthorized access of their access credentials or any other security incidents related to User's access.

7. DEFINITIONS AND ABBREVIATIONS:

SI No	TERMS	DEFINITIONS AND ABBREVIATIONS
7.1	Access Control	Access control is a security technique that regulates who or what can view or use resources in a computing environment.
7.2	Access control limits	Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

8. DISTRIBUTION LIST:

On shareholder Policies IT

9. SPECIAL INSTRUCTIONS

- 9.1. Any violation or breach to the policy may be subject to HR disciplinary procedure in accordance with the Code of Conduct for Employees and any other applicable UAE Laws in this regard.
- 9.2. If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from Information Technology.
- 9.3. The Information Technology reserves the right to check the compliance of this policy on a periodic basis.
- 9.4. Any exceptions to this policy with valid business justification require approval from Information Technology on a case to case basis.
- 9.5. The Information Technology in coordination with the Information Systems Owners, Business Processes Owners reserve the right to review Users' lists and ascertain the privileges granted.
- 9.6. The Information Technology reserves the right to review the use of high privilege ID's at regular intervals.
- 9.7. CMC facilities functioning at university level will be managed as per university rules and regulations as applicable in UAE internally & externally.
- 9.8. CMC Healthcare providing School Clinic's ADHICS requirements must be maintained as per applicability of the scope wherever necessary.

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
02	01/05/2021	Added additional scope for access control management 3.1.6	Page 1
02	01/05/2021	Special instruction- 9.7 updated	Page 5
02	01/05/2021	Special instruction 9.8 updated	Page 5

13. APPENDIX:

- 13.1 CMC-HR-F-039 Acceptable Use Policy acknowledgement form V1

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

Canadian Medical Center Group
Human Resource Department



ACCEPTABLE USE POLICY ACKNOWLEDGMENT FORM
CMC-HR-F-039

I will create a personal, confidential password and will not write it down I understand that disclosure of my password to anyone else is a **SECURITY VIOLATION**.

In addition, I agree to the following:

1. I will not attempt to learn another user's password or use someone else's password.
2. I will not gain access to any system with my password and then allow another person to enter or retrieve data from the system.
3. I will Immediately change my password and notify, supervisor and the Information Security Manager if believe my password has been compromised.
4. I will not use any information system for unethical, illegal, or criminal purposes.
5. I will not use any Information system to send nuisance messages such as chain letters and obscene or harassing messages.
6. I will not use any Information system for unauthorized commercial uses.
7. I will only use information systems and resources for official authorized purposes.
8. I will use anti-virus software as provided by CMC IT and scan all computer disks and files from other sources.
9. I will not access or attempt to access any unauthorized data or files.
10. I will not download or install or use any unlicensed copyrighted material (music, movies, software, etc.) on any CMC computer.
11. I will not make unauthorized copies of any data files or software.
12. I will not install or play games on any CMC computers.
13. I will not install any type of unauthorized wireless access point on CMC network.
14. I will not use any unauthorized remote access software or use any proxy avoidance Internet sites to bypass Internet filtering and/or auditing.
15. I will report all security violations immediately to my supervisor and the Information Security Team.
16. I understand that information systems staff have the right to copy and examine any files that reside on any CMC system to investigate possible security violations and to protect CMC network and systems from anything that threatens or degrades operations.
17. I hereby acknowledge that all Protected Health Information accessed through any CMC system is confidential. Protected Health Information means any Information that is created or received which identifies an individual and relates to the past, present or future physical or mental health or condition of that individual.
18. I will only access the electronic data of patients I am providing care for as related to my specific job functions

Employee Name	Employee Signature	Date	Unit/Name of Branch

Note: This acknowledgement is valid throughout the employment or service of an individual with Canadian Medical Center Group and/or its subsidiaries. This acknowledgement survives the expiration or termination of the employment or service of an individual with Canadian Medical Center Group and/or its subsidiaries.

CMC-HR-F-038 VER 01

•Restricted/ محظور

Page 1 of 1

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY

Document Developed By:

Licensing Officer	Ms. Aprilia Ariesia		01/07/2020
	Name	Signature	Date
IT Support	Mr. Muhamed Shifas Avudiyil		01/07/2020
	Name	Signature	Date

Document Developed & Reviewed By:

IT supervisor/IT Manager	Mr. Yahya Mannoparambil		01/07/2020
	Name	Signature	Date
Asst. Manager Quality	Ms. Dhanya Thankappen		01/07/2020
	Name	Signature	Date

Document Approved By:

Chief Operating Officer/Chief Financial Officer	Mr. Imran Saleem		01/07/2020
	Name	Signature	Date
Manager Human Resources /Chief Administration Officer	Mr. Sallam Mohammed Naji		01/07/2020
	Name	Signature	Date

14. APPROVAL SHEET:

**CONTROLLED DOCUMENT**

Department:	Administration/IT
Document No	CMC- IT-ADHICS- 004
Issue Date:	01/07/2020
Revision Date:	01/05/2021
Next Review Date	01/05/2023

ACCESS CONTROL POLICY