

Department:	CMC- IT-ADHICS- 013
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

THIRD PARTY SECURITY POLICY

1. PURPOSE

- 1.1 This document describes the policy under which third party persons or organizations connect to or access network resources on CMC networks for the purpose of transacting business related to CMC or other approved business transactions.

2. POLICY STATEMENT:

- 2.1 The policy is organized into three sections; general, physical, and technical according to the precaution or requirement specified.
- 2.2 This Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with system administrators.

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 and it addresses the use of all information and information processing facilities that are required by Users to carry out their daily business activities.

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 This policy has full support from the executive steering committee and human resources. This policy is a living document and may be modified at any time by the IT Supervisor, human resources, or the executive steering committee.

Department:	CMC- IT-ADHICS- 013
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

THIRD PARTY SECURITY POLICY

6. PROCEDURE:

6.1 Pre-Requisites Security Review

- 6.1.1** All new extranet connectivity will go through a security review with the Office of IT Manager. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

6.2 Assessments

- 6.2.1** Every 3rd-party granted access to CMC Information Resources must sign the CMC Third-Party Non-Disclosure Agreement and Business Associate Agreement (if applicable).
- 6.2.2** All 3rd-party relationships must be evaluated for inherent information security risk prior to any interaction with CMC Information Resources.
- 6.2.3** Criteria for inherent risk classifications must be established; "High", "Medium", and "Low".
- 6.2.4** All Third-Party relationships must be re-evaluated for inherent information security risk bi-annually and any time there is a material change in how CMC utilizes the third-party product or service.
- 6.2.5** Third-Party relationships with significant inherent risk (classified as "High" or "Medium") must be evaluated for residual risk using questionnaires, publicly available information, and/or technical tools.
- 6.2.6** Residual information security risk assessments must account for administrative, physical, and technical controls.
- 6.2.7** Residual information security risk thresholds must be established for Third-Party relationships with significant inherent risk (classified as "High" or "Medium").
- 6.2.8** Third-Party relationships that do not meet established residual information security risk thresholds:
- 6.2.9** Must be terminated,
- 6.2.10** Must be formally approved by executive management following an established waiver process, and/or;
- 6.2.11** Changed in a manner that reduces inherent and/or residual information security risk to meet CMC established thresholds.

6.3 Pre-Requisites Security Review

- 6.3.1** All new extranet connectivity will go through a security review with the Office of IT Manager. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

6.4 Point of Contact

- 6.4.1** The CMC authority must designate a person to be the Point of Contact (POC) for the third-party connection. The POC acts on behalf of the CMC and is responsible for those portions of this policy and the "Third Party

Department:	CMC- IT-ADHICS- 013
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

THIRD PARTY SECURITY POLICY

Agreement” that pertain to it. In the event that the POC changes, the relevant third-party person or organization, must be informed promptly.

6.5 Establishing Connectivity

6.5.1 All contracting authorities within that wish to establish connectivity or network resource access to a third party are to file an Extranet connectivity request with IT Manager accompanied by a “Third Party Agreement” signed by the third-party person, organization, or rightful designee. IT Manager will then engage the third party to address security issues inherent in the project. The sponsoring contract authority must provide full and complete information as to the nature of the proposed access to IT Manager, as requested. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. All connectivity requests will have a specific beginning and ending date. In no case will rely upon the third party to protect network or resources. IT Manager will grant access to all approved resources and reserves the right to refuse access on the basis of legitimate security concern as decided by the CISO.

6.5.2 Modifying or Changing Connectivity and Access

6.5.2.1 All changes in access must be accompanied by a valid business justification and are subject to security review. The sponsoring contracting authority is responsible for notifying the third-party person or organization and IT Manager when there is a material change in their originally provided information so that security and connectivity evolve accordingly. Extensions will be granted on a case-by-case basis and must be requested in writing by the sponsoring contracting authority.

6.6 Terminating Access.

6.6.1 When access is no longer required, the sponsoring contracting authority within one hour must notify the IT Manager, who will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. IT security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be deprecated, and/or are no longer being used to conduct business or other approved business transactions will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct business or other approved business transactions necessitate a modification of existing permissions, or termination of connectivity, IT Manager will notify the POC of the sponsoring contracting authority of the change prior to taking any action.

6.7 Enforcement

Department:	CMC- IT-ADHICS- 013
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

THIRD PARTY SECURITY POLICY

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

7. DEFINITIONS AND ABBREVIATIONS:

SI No	TERMS	DEFINITIONS AND ABBREVIATIONS
7.1	Third party security	A third-party security is security given by an entity which secures the legal responsibility of a third party. Third Party Information means Confidential Information that has been disclosed to the Company or an Affiliate of the Company by a third party and that the Company or such Affiliate of the Company is obligated to treat as confidential.
7.2	CMC facilities	Licensed facilities in Abu Dhabi where ADHICS standards are applicable: Canadian Medical Center LLC Canadian Medical Center LLC Branch -2 Canadian Medical Center LLC Branch - 3 Canadian Medical & Rehabilitation Center LLC CMC First Aid Clinic
7.3	ADHICS	Abu Dhabi healthcare information and cyber security standards

8. DISTRIBUTION LIST:

On shareholder Policies IT

9. SPECIAL INSTRUCTIONS:

9.1 This Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

9.2 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.

Department:	CMC- IT-ADHICS- 013
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

THIRD PARTY SECURITY 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:

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
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