

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

1. PURPOSE:

1.1 To ensure that activities concerning support and maintenance of data, technology, and application are controlled and carried out in a standardized manner to reduce probabilities of errors and compromises, and to increase efficiency and security. Objective outcome of effective operations management includes, but is not limited to:

- 1.1.1 Improved security and reduce probabilities of compromise.
- 1.1.2 Reduced errors
- 1.1.3 Controlled unauthorized activities.
- 1.1.4 Regulated efforts
- 1.1.5 Increased efficiency
- 1.1.6 Reduced security incidents

2. POLICY STATEMENT:

2.1 The Communication & Operations Management Policy provides direction for the right and secure operation of information processing facilities in CMC & Group facilities.

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 The policy covers all the operations and communications for information process management as well as network and security devices owned by Canadian Medical Center facilities which ensures smooth operational functions.

5. RESPONSIBILITY

5.1 The IT Manager & Team Members or the job title assigned with responsibilities of managing operational is responsible for asset protocols, operational documentation and actions for CMC facilities.

5.2 The Information Security Section/part of IT Department or the function assigned with information security responsibilities 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 Security Section/Department or the function assigned with information security responsibilities is responsible to conduct awareness about the policy to users.

6. PROCEDURE:

6.1 Asset inventory

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

- 6.1.1 All sections of IT Department shall ensure having an up-to-date inventory of information systems such as, software, servers, appliances, devices, tools, which are in use in CMC & Group The inventory shall also highlight the information systems that were de-commissioned.
- 6.1.2 Access to the information systems inventory shall be restricted within group of employees of IT Department and shall be shared strictly on a need-to-know basis.
- 6.1.3 All IT assets must be assigned with owner/custodian who must maintain perpetual inventory control, a record of the new location and new equipment custodian of all equipment issued to others.

6.2 Operational Procedures Documentation

- 6.2.1 Operating procedures are used in all day-to-day maintenance of CMC & Group facilities of IT systems, infrastructure, medical Devices and Equipment in order to ensure the highest possible service from these assets. These operating procedures must be documented to an appropriate level of detail for the departmental team that will be using them. Transition of Information Systems and Applications shall be ensured.

6.3 Capacity Management

- 6.3.1 All sections of IT section of IT Department shall ensure the availability of adequate capacity of IT resources to deliver the required IT services pertaining to their areas of operations.
- 6.3.2 All sections of IT Department shall conduct forecasting reviews to anticipate future needs of IT requirements for delivering the IT services in alignment with the strategic direction of Canadian Medical Center & group facilities and upcoming projects and initiatives. These capacity requirements shall be documented as IT capacity plans.
- 6.3.3 All sections of IT Department shall continuously monitor, analyse and evaluate the performance and capacity of all IT infrastructure and services, to ensure that no excessive systems resources are consumed and there is no significantly degrading systems response time.
- 6.3.4 The Canadian Medical Center & group facilities IT department will follow Change Management Process defined in Capacity Management document.

6.4 Segregation of Duties/Roles

- 6.4.1 The Canadian Medical Center & group facilities of IT shall allow no single person to access, modify, use assets, or subverting a critical process without authorization or detection.
- 6.4.2 Roles and responsibilities shall be defined. The Canadian Medical Center & group facilities of IT should rotate and segregate duties and areas of responsibilities to minimize the chance of accidental or unintended access or modification, as far as resources are available and it is practical.
- 6.4.3 If duties are not segregated, Canadian Medical Center & group facilities IT shall implement appropriate detective controls such as monitoring of activities, audit trails and management supervision.

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

6.4.4 Information security audit and assessment are carried out independently on rotation basis.

6.5 Separation of Development, Test and Operational Environment

6.5.1 The development and test environments must be separate from the live operational environment to reduce the risk of accidental changes or unauthorized access. The environments must be segregated by the most appropriate controls including, but not limited to, the following:

- 6.5.1.1 No live data shall be used to perform testing to any information systems, neither in a production nor in a test environment.
- 6.5.1.2 Running on separate computers, domains, instances and networks.
- 6.5.1.3 The Canadian Medical Center & group facilities shall ensure that all changes are strictly applied and tested in a test environment prior to authorizing the change for the production environment.

6.6 Protection from Malware

6.6.1 The Canadian Medical Center & group facilities ensure that detection, prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness and training. Controls against malicious code include but not limited to:

- 6.6.1.1 strict prohibition on the use of unauthorized software
- 6.6.1.2 our operating systems are updated promptly when updates which affect robustness against malicious code are issued.
- 6.6.1.3 up-to-date malicious code detection and repair software where available – the checks against malicious code that this software carries out include:
- 6.6.1.4 **Checking any files on electronic or optical media, and files received over** networks before use
- 6.6.1.5 checking electronic mail attachments and downloads for malicious code before use
- 6.6.1.6 checking web pages for malicious code
- 6.6.1.7 Firewall and endpoint security.

6.6.2 Canadian Medical Center & group IT department will follow process defined in Anti-Virus policy (CMC-IT-ADHICS-014) and Network Security documents.

6.7 Logging and Monitoring

6.7.1 Protection of log information

6.7.1.1 Logging controls and log information are protected against tampering and unauthorized access in CMC facilities.

6.7.2 Administrator and operator log

6.7.2.1 System administrator and operator activities are logged, including, where practicable:

- 6.7.2.1.1 the time at which a success/failure event occurred and within which process.
- 6.7.2.1.2 the account, administrator and operator identifiers

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

6.7.2.1.3 This could be used to monitor unauthorized admin activities.

6.8 Patching

- 6.8.1 All servers and system must have appropriate critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate.
- 6.8.2 There must be a full record of which patches have been applied and when.

6.9 Quality Management

- 6.9.1 The Canadian Medical Center & group IT Department turn to standards for guidelines, definitions, and procedures that help us achieve objectives such as:
 - 6.9.1.1 Satisfying their customers' quality requirements internal & external
 - 6.9.1.2 Ensuring their products and services are safe.
 - 6.9.1.3 Complying with regulations in United Arab Emirates
 - 6.9.1.4 Meeting environmental objectives
 - 6.9.1.5 Protecting products against climatic or other adverse conditions
 - 6.9.1.6 Ensuring that internal processes are defined and controlled.

6.10 System Acceptance

- 6.10.1 The Canadian Medical Center & group shall ensure that the requirements and criteria for acceptances of new systems are clearly defined, agreed, documented and tested. The following criteria shall be considered, but not limited to:
 - 6.10.1.1 Performance and system capacity requirements;
 - 6.10.1.2 Error recovery, restart procedures and contingency plans;
 - 6.10.1.3 Preparation and testing of routine operating procedures;
 - 6.10.1.4 Agreed set of security controls in place;
 - 6.10.1.5 Business continuity arrangements;
 - 6.10.1.6 Training in the operation or use of new equipment;

6.11 Electronic Communication Services Access Provisioning & De- Provisioning

- 6.11.1 Electronic communication accounts shall be created as per the Entity approved process (IT Request Form Number: CMC-HR-F-006)
- 6.11.2 Any generic or group email account shall have an owner assigned for accountability.
- 6.11.3 Electronic communication accounts de-provisioning (disabling) request shall be raised per CMC & Group Human Resource Information approved process.
- 6.11.4 Electronic communication accounts de-provisioning (disabling) is valid under the following circumstances:
 - 6.11.5 End of employee's service.
 - 6.11.5.1 End of employee's service.
 - 6.11.5.2 Contractors completing their engagement.
 - 6.11.5.3 If requested by the Director of the concerned department to which the user belongs.

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

6.11.5.4 If user found to have violated the policy or misused the provided service in any mean.

7. DEFINITIONS AND ABBREVIATIONS:

7.1	TERMS	DEFINITIONS AND ABBREVIATIONS
7.2	IT Request form	The form which granting IT access for employees/contractors or any other mean required for business purpose.
7.3	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

8. DISTRIBUTION LIST:

On shareholder Policies IT

9. SPECIAL INSTRUCTIONS:

- 9.1 If Users are unsure or not clear of anything in this policy, they should seek clarification or advice from IT Department CMC.
- 9.2 The IT Department CMC facilities reserves the right to check the compliance of this policy on a periodic basis.
- 9.3 Any exceptions to this policy with valid business justification require approval from IT Manager on a case-to-case basis.

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	24/01/2021	New policy	All pages

13. APPENDIX:

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

COMMUNICATION AND OPERATIONS

13.1 IT Request Form Number: CMC-HR-F-006)

Canadian Medical Center Group
Human Resource Department



IT Request Form
CMC-HR-F-006

IT REQUEST FORM

Employee Name:
Employee Number:
Designation:
Department:
Date of Joining:

Date:

List of Equipment and Services: (please specify equipment or services in the specification column)

S. No	Equipment / Services	Specification	Check list (IT Engineer)
1	Intranet / Mail / Mail in Mobile		
2	Printer / Scanner / Laptop / PC / IP Phone		
3	Door Access		
4	Tablet / Wi-Fi (Official)		
5	Others, please specify		

Comments :

Declaration

I, hereby state that I will treat any information received during the use of above mentioned IT equipment/services as confidential, and will not disclose such information to any third person, except in accordance with applicable laws and policies.

Requestor Name: Requestor Signature: Date:	Approver Name: Approver Designation: Approver Signature: Date:
IT Engineer Name: IT Engineer Designation: IT Engineer Signature: Date:	HR Representative Name: HR Representative Designation: HR Representative Signature: Date:



المركز الكندي الطبي
CANADIAN MEDICAL CENTER

CONTROLLED DOCUMENT

Department:	CMC- IT-ADHICS- 017
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

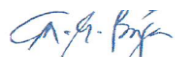
COMMUNICATION AND OPERATIONS

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 Mannooparambil		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