

Department:	CMC- IT-ADHICS- 006
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

INFORMATION DATA BACK UP POLICY

1. PURPOSE

- 1.1 The objective of this policy is to define adequate back up requirements for the critical information and data of Canadian Medical Center facilities (3.1) and ensure their availability in the event of disruption.

2. POLICY STATEMENT:

- 2.1 To provide our staff a template that can be modified for your company's use in developing a Data Backup Policy.
- 2.2 To focuses on codifying your backup strategy.

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 information / data stored and processed in production, development, test environments, file servers, as well as network and security devices owned by Canadian Medical Center facilities.

5. RESPONSIBILITY

- 5.1 The Information Security Manager or the job title assigned with responsibilities of managing information security is responsible for development, maintenance, enforcement and endorsement 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
- 5.5 Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections and Business Processes Owners are responsible for compliance to this policy within their area(s) of concern.
- 5.6 The Business Processes Owners and Senior Management or job titles assigned with responsibilities of managing entity's business divisions and sections are responsible for ensuring that the backups are taken as per the operational requirements along with IT team.

Department:	CMC- IT-ADHICS- 006
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

INFORMATION DATA BACK UP POLICY

5.7 The Backup team or the function assigned with responsibilities of backup management is responsible for scheduling the backups as per the operational requirements defined with business owners.

5.8 The Backup team or the function assigned with responsibilities of backup management is responsible for handling backup media.

5.9 The Backup team or the function assigned with responsibilities of backup management is responsible for the implementation of this policy on the day-to-day operations.

6. PROCEDURE:

6.1 Backup Requirements

- 6.1.1 Information / data Backup requirements of all information systems within Canadian Medical Center shall be identified and documented.
- 6.1.2 Information / data stored locally on Users' computers will not be included in scheduled backup. Thus, Users shall transfer their data onto their network drive folders so that it will be included in the scheduled backup.
- 6.1.3 The IT Department shall decide on the minimum back up requirements for their respective information / data and information processing systems.
- 6.1.4 The IT Department shall decide on the frequency and type of back up for their respective application, database and operating systems and network devices.
- 6.1.5 The IT Department shall record and maintain the backup requirements for all information systems. The details shall include information/data to be backed up, backup frequency, storage media, retention and disposal.

6.2 Backup Schedule

- 6.2.1 Backup of information / data shall be taken regularly as defined by Business Processes Owners or IT Manager to ensure information/data is available in the event of failure of information processing systems.
- 6.2.2 The IT Department shall perform a minimum level of backup for each server hosting actual production data as agreed with business owners.
- 6.2.3 The IT Department shall ensure that any newly commissioned server into production is included for the minimum level of data backup.
- 6.2.4 In the event of schedule backup failure, the IT Department shall ensure rescheduling of backup and shall keep the business owners informed on the same.
- 6.2.5 The IT Department shall identify the root cause for the failure of backup and the same shall be documented and shared with Business owner
- 6.2.6 Backup of systems, applications, devices, etc. shall be taken before and after applying any changes, such as upgrades, patching, etc.

6.3 Backup Media handling and storage

- 6.3.1 All backup media must be clearly identified in a consistent manner.
- 6.3.2 Backup copies of critical data (identified by CMC facilities) must be maintained at an identified offsite location.
- 6.3.3 The offsite location for storage back up is maintaining in CMC Delma

Department:	CMC- IT-ADHICS- 006
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

INFORMATION DATA BACK UP POLICY

- 6.3.4 The offsite location for storage of backup tapes must be in a separate geographic region with a minimum distance of 40 KMs from the onsite location.
- 6.3.5 Offsite backup must be maintained in a fire-resistant enclosure and must be covered with appropriate physical security.
- 6.3.6 Access to backup media while onsite, in-transit, or offsite must be restricted.
- 6.3.7 If backup tapes are discovered to be damaged or corrupted, then these tapes must be destroyed.
- 6.3.8 All backup media shall be disposed-off in a secure manner at the end of their life, according to their retention period, or if found to be corrupted or damaged, and the disposal procedure must ensure the following:
- 6.3.9 The media is properly degaussed
- 6.3.10 Labels/tags containing reference to CMC internal information are removed
- 6.3.11 Tapes and others non-reusable data storage media are physically destroyed.
- 6.3.12 A detailed schedule for the movement of back tapes to offsite location shall be documented and a record for the movement of tapes to & from offsite location shall be maintained.
- 6.3.13 All backup tapes must be regularly transported to the offsite storage location as defined by Business Processes Owners or in coordination with the IT Department
- 6.3.14 Handling backup media must be done according to the manufacturer's recommendations and guidelines to prevent damage.

6.4 Backups restore and testing

- 6.4.1 Backup shall be randomly tested for data recovery by the IT Department Recovery testing shall be done at least once in a year.

7. DEFINITIONS AND ABBREVIATIONS:

7.1	TERMS	DEFINITIONS AND ABBREVIATIONS
7.2	Back up	A back up is sets forth the important of the data and system backups, defines the ground rules for planning ,executing and validating backups and includes specific activities to ensure the critical data is backed up to secure storage media located in a secure location. This ensures that information from business applications such as Oracle, Microsoft SQL email server databases and user file is copied to disk and or tape to ensure data recoverability in the event of accidental data deletion, corrupted information or s system disruption. It's a protection, scheme ensures the recoverability of servers, network components and other

Department:	CMC- IT-ADHICS- 006
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

INFORMATION DATA BACK UP POLICY

		infrastructure devices, as well as critical application, databases and important files.
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 HR

9. SPECIAL INSTRUCTIONS:

- 9.1 Any violation or breach to the policy may be subject to CMC HR disciplinary procedure in accordance with Relevant HR Law 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 IT Department CMC.
- 9.3 The IT Department CMC facilities 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 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	01/07/2020	New policy	All pages

13. APPENDIX:

NA



المركز الكندي الطبي
CANADIAN MEDICAL CENTER

CONTROLLED DOCUMENT

Department:	CMC- IT-ADHICS- 006
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

INFORMATION DATA BACK UP POLICY

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