

Department:	CMC- IT-ADHICS- 014
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Version	1

ANTI VIRUS POLICY**1. PURPOSE**

1.1 To outline the protection controls from malicious codes (such as Virus, Spyware, malware, Trojans) etc., which may harm Computer Devices and servers of Canadian Medical Center, and to establish the requirements for addressing any problems resulting from such infections.

2. POLICY STATEMENT

2.1 All Canadian Medical Center computer devices connected to the Canadian Medical Center Mobility network (herein referred to as "the network") or networked resources shall have anti-virus software installed, configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices.

2.2 Exceptions to this policy may be allowed if the computer device cannot have anti-virus software installed. Possible examples of this would be vendor-controlled systems, FDA validated systems, or devices where anti-virus software has not yet been developed. In these cases, the Information Technology Staff must develop a plan to protect the device from infection.

2.3 An exception may be granted if an infected computer device is discovered that performs a critical function and may not be immediately taken "off-line" without seriously impairing some business function. Under those circumstances, a plan will be developed to allow the computer device to be taken off-line and the infection purged while protecting the function of the device.

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 and physical assets (information and computing resources including Desktops, Laptops and Servers) of Canadian Medical Center.

5. RESPONSIBILITY

5.1 IT Department is responsible for development, maintenance, enforcement and endorsement of the policy.

5.2 The IT 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 IT Department is responsible to conduct awareness about the policy to Users.

5.5 The Top Management are responsible for compliance to this policy within their area(s) of concern

5.6 IT Department who are administering the antivirus system are responsible to implement the policy and centrally monitor and analyze the logs of the system.

Department:	CMC- IT-ADHICS- 014
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Version	1

ANTI VIRUS POLICY

6. PROCEDURE:

6.1 Antivirus Installation

- 6.1.1 The IT Department shall ensure that all Desktops & Laptops are installed & configured with the official antivirus software.
- 6.1.2 The System Administrators of servers shall ensure that all servers are installed & configured with official antivirus software.
- 6.1.3 The Antivirus software shall operate on a real time basis on all servers, desktops and laptops.
- 6.1.4 Server machines running exclusively on UNIX-based operating systems where the risk of viruses is minimal, may not have anti-virus software installed.
- 6.1.5 Antivirus software shall be configured to do a full system scan once in a week and a real time scan of all the files from external storage media when they are accessed, copied or moved.
- 6.1.6 The antivirus software shall be configured to clean the malicious contents automatically.
- 6.1.7 Antivirus software shall be configured to quarantine the infected files if they cannot be cleaned.
- 6.1.8 Antivirus software on the E-mail Servers at the gateway level shall be configured for scanning all internal and external mails.
- 6.1.9 Antivirus scanning shall be enabled automatically as and when the Desktops, Laptops, and Servers are started/restarted.
- 6.1.10 Users shall be trained to use antivirus software. However Users shall not be allowed to install and un-install or change the configuration settings of the Antivirus Software.

6.2 Antivirus software and signature file maintenance

- 6.2.1 New Antivirus signatures shall be applied within 24 hours of release by the vendor.
- 6.2.2 IT Department who are administering the antivirus system shall ensure that new signature are updated. Similarly all relevant network and systems endpoints shall be configured for automatic updates.
- 6.2.3 IT Department who are administering the antivirus system shall maintain updated documents required for installation, configuration and administration of all Antivirus Software components.
- 6.2.4 IT Department shall coordinate with external security authorities on latest virus breakouts in the region and shall ensure preventive action is initiated.
- 6.2.5 In case of worm/virus or a malicious content originated from any information system, the respective information system shall be disconnected from [Entity Name]'s network as a prevention against spread of virus/worm into the network.

6.3 Antivirus Server Security

- 6.3.1 The Antivirus system servers shall be placed in a controlled physical access environment with access to authorized personnel only.
- 6.3.2 Logical (electronic) access to the Antivirus servers shall be restricted to the authorized personnel only.

6.4 Third Party Access

Department:	CMC- IT-ADHICS- 014
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Version	1

ANTI VIRUS POLICY

- 6.4.1 Third Party personnel shall not be allowed to connect Laptops/Desktops to the CMC network without updated Antivirus signature.
- 6.4.2 The Information Technology shall verify that the third party user's desktop and laptop do not contain any virus or other vulnerabilities that could affect the Canadian Medical Center's network before being connected to LAN.

6.5 Logging and Monitoring

- 6.5.1 Logging shall be enabled on the Antivirus systems. Antivirus systems parameters and Antivirus log files need to be monitored weekly by the administrators responsible of the antivirus systems.
- 6.5.2 All virus detection incidents shall be logged, along with the action taken
- 6.5.2.1 Quarantine.
- 6.5.2.2 Deletion.
- 6.5.2.3 Successful cleaning
- 6.5.3 Antivirus logs shall be stored online for 90 days based on the risk, business need and any legal or regulatory requirements applicable to CMC and reviewed by CMC IT Department who are administering the antivirus system and verified by the CMC IT Supervisor / Manager
- 6.5.4 The Antivirus system shall also be configured to do the following:
- 6.5.4.1 Send an alert to the System Administrator responsible of the antivirus systems in case of any malicious content not cleaned and on detecting any new virus breakout.

6.6 Incident reporting

- 6.6.1 System Administrators who are administering the antivirus system shall review and report the identified malicious code/content as per the Information Security Incident Management process that is to be developed by the entity.
- 6.6.2 Users shall report any malicious content detected, configuration change or any unusual behavior in their systems to the IT Department.
- 6.6.3 Users shall ensure that if a laptop/ desktop is thought to be infected by a virus, it shall be immediately disconnected from Canadian Medical Center's network

6.7 Change Management

- 6.7.1 All changes concerning Antivirus server / application and configuration settings shall follow the Canadian Medical Center's Change Management Process.

7. DEFINITIONS AND ABBREVIATIONS:

7.1	Computer devices -	Are any type of device connected to a network that could become infected with a computer virus. Examples of computer devices would be, but not limited to, workstations, servers, laptops, PDAs, etc.
7.2	Malicious software	- Is any type of computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, Trojan etc.
7.3	Anti-Virus software -	Runs on either a server or workstation and monitors network connections looking for malicious

Department:	CMC- IT-ADHICS- 014
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Version	1

ANTI VIRUS POLICY

		software. Anti-virus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.
7.4	Virus definition -	files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.

8. DISTRIBUTION LIST:

On shareholder Policies IT/ intranet portal

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 Policy 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.
- 9.3 The IT Department or the function assigned with information security responsibilities] 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 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:

Department:	CMC- IT-ADHICS- 014
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Version	1

ANTI VIRUS 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