

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

### 1. PURPOSE:

- 1.1 To outline the basic principles of protecting all the information assets of CMC and make all Users within the facility aware of the potential security threats and associated business risks.
- 1.2 The Information Security Policy should provision business continuity and minimize business damage by preventing and managing to an acceptable level the impact of information security incidents. Adherence to this policy will help to protect the facility. We are committed to good information security provision for our patient, customers and for our employees. It is recognized that detailed policies and procedures are required, and the facility is committed to implementing these in full.

### 2. POLICY STATEMENT:

- 2.1 This is to ensure to protect the facility from information security threats, whether internal or external, deliberate or accidental.
- 2.2 All CMC staffs, patient's, visitors, contractors shall ensure:
  - 2.2.1 Maintaining confidentiality, integrity and availability of information.
  - 2.2.2 Handling information appropriately and according to its data classification.
  - 2.2.3 Preventing disruption to work being undertaken within academic, research and support services that lead to financial loss or loss of reputation to the facility.
  - 2.2.4 Ensuring business continuity and minimizing business damage by managing and minimizing the impact of information security incidents.
- 2.3 Ensure that information is accessible only to those authorized to have access.
  - 2.3.1 Safeguard the accuracy and completeness of information and processing methods.
  - 2.3.2 Ensure that authorized users have access to information and associated assets when required
  - 2.3.3 ensure that information it manages shall be secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.
  - 2.3.4 Define an information classification scheme describing classes and how information of a particular class should be managed (stored, accessed, transmitted, shared, and disposed of);

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

- 2.3.5 Meet all information security requirements under appropriate regulations, legislation, organization policies and contractual obligations.
- 2.3.6 Address the security of all of our services and processes to ensure that risks are identified, and appropriate controls are implemented and documented.
- 2.3.7 Provide a secure working environment for staff and contractors at our sites.
- 2.3.8 Produce business continuity and incident response plans for strategic facility IT and information services, which will be maintained and tested on a regular basis.
- 2.3.9 Require all third parties working on our behalf to ensure that the confidentiality, integrity and availability requirements of all business systems are met.
- 2.3.10 Promote this policy and raise awareness of information security throughout the facility.
- 2.3.11 Provide appropriate information security training for our staffs.

### 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 (CMC) staff who deal with health information's (All staff using HIS System, Active Directory and shared computer network where health information's accessibility)

### 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.

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

5.4 This Policy shall be implemented by the system administrators and designated personnel (if any).

5.5 Suspected activities must be reported to the IT Security Officer/IT Manager by end users.

### 6. PROCEDURE:

6.1 Canadian Medical Center facilities are committed towards securing the confidentiality, Integrity and Availability of information for the day-to-day business operations.

6.1.1 The security of information and other assets is therefore regarded as fundamental for the successful business operation of Canadian Medical Center & Group.

6.1.2 This high-level information security policy is a key component of Canadian Medical Center's overall information security management framework and should be considered along with Canadian Medical Center's specific and more detailed information security policies, procedures, standards & guidelines.

6.1.3 Adherence to this policy will help to protect data/ information of Canadian Medical Center & Group and its customers from information security threats, whether internal or external, deliberate or accidental.

### 6.2 Core Principles

6.2.1 Canadian Medical Center recognizes that secure operations are dependent upon securing three core organizational elements, which are people, process and technology. Thus, all Canadian Medical Center activities must adhere to the general principles laid down.

6.2.1.1 Maintain the confidentiality, integrity & availability of Information & Information assets.

6.2.1.2 Meet the UAE regulatory, statutory and legislative requirements.

6.2.1.3 Report and investigate all suspected breaches of Information Security.

6.2.1.4 Provide appropriate Information Security Training & awareness to all employees (permanent & contract employees)

6.2.1.5 Design appropriate controls and procedures to support the implementation of this Information Security Policy.

6.2.1.6 Ensure all stakeholders are responsible for implementation of respective security policies & procedures within their area of operation and oversee adherence by their team members.

6.2.1.7 Continually improve Information Security through implementation of corrective and preventive actions.

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

6.2.1.8 Prepare, maintain and test Business Continuity Plans in a practical manner based on the business needs.

6.2.1.9 Annually review this policy for adequacy and appropriateness

### 6.3 Risk Management

- 6.3.1 Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.
- 6.3.2 Unauthorized disclosure of this information to outsiders is strictly forbidden and can be prosecuted by Canadian Medical Center or any other authority.
- 6.3.3 Public Information has been specifically approved for public release by a designated authority within each entity of Canadian Medical Center & Group. Examples of Public Information may include marketing brochures and material posted to Canadian Medical Center entity internet web pages.
- 6.3.4 Non - Public Information Policy and Security has levels of Security Information, (SECRET, CONFIDENTIAL, RESTRICTED, PUBLIC as per classification)
- 6.3.5 Depending on the level of classification there are different rules controlling the level of clearance needed to view such information, and how it must be stored, transmitted, and destroyed. Additionally, access is restricted on a "need to know" basis. Simply possessing a clearance does not automatically authorize the individual to view all material classified at that level or below that level. The individual must present a legitimate "need to know" in addition to the proper level of clearance.
- 6.3.6 Computer and Information Control all involved systems and information is assets of Canadian Medical Center and is expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or data and/or software based.
- 6.3.7 Ownership of Software: All computer software or data developed by CANADIAN MEDICAL CENTER employees or contract personnel on behalf of CANADIAN MEDICAL CENTER or licensed for CANADIAN MEDICAL CENTER use is the property of CMC & Group and may not be copied for use at home or any other location, unless otherwise specified by the license agreement.
- 6.3.8 Installed Software or data: All software packages that reside on computers and networks within CMC must comply with applicable licensing agreements and restrictions and must comply with CMC acquisition of software policies.

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

6.3.9 All identified risks related to information security shall mitigate with appropriate control measures to avoid the risks or severity of the risks.

6.3.10 An ISMS risk analysis conducting biannually by IT team and concerned stakeholder's involvement (CMC ISMS risk register reference No: CMC-IT-008 VER 01)

### 6.4 Virus Protection

6.4.1 Virus checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses.

6.4.2 Users are not authorized to turn off or disable virus checking systems.

### 6.5 Access Controls Types:

6.5.1 Physical and electronic access to PI, Confidential and Internal information and computing resources is controlled.

6.5.2 To ensure appropriate levels of No Distribution and dissemination of any part of this correspondence without expressed written consent is a violation.

6.5.3 Confidential and Internal information include (but are not limited to) the following methods:

6.5.4 Authorization: Access will be granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner. Any of the following methods are acceptable for providing access under this policy:

6.5.4.1 Context-based access: Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The "external" factors might include time of day, location of the user, strength of user authentication, etc.

6.5.4.2 Role-based access: An alternative to traditional access control models (e.g., discretionary or non- discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role

6.5.4.3 User-based access: A security mechanism used to grant users of a system access based upon the identity of the user.

6.6 Identification/Authentication: Unique user identification (user id) and authentication is required for all systems that maintain or access PI, Confidential and/or Internal Information.

6.6.1 Users will be held accountable for all actions performed on the system with their user id.

6.6.2 At least one of the following authentication methods must be implemented:

6.6.3 Strictly controlled passwords

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

6.6.4 The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

6.6.5 An automatic timeout re-authentication must be required after a certain period of no activity (maximum 60 minutes).

6.6.6 The user must log off or secure the system when leaving it.

6.6.6.1 Data Integrity

6.6.6.2 CMC must be able to provide corroboration that PI, Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity

6.6.6.2.1 Transaction audit

6.6.6.2.2 Disk redundancy (RAID)

6.6.6.2.3 encryption of data in storage

6.6.6.2.4 digital signatures

### 6.7 Transmission Security

6.7.1 Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks.

6.7.1.1 The following features must be implemented:

6.7.1.1.1 Integrity controls and

6.7.1.1.2 Encryption, where deemed appropriate

6.7.2 Remote Access: Access into CMC network from outside will be granted using CMC approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further, PHI, Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the ECIPS network.

6.7.3 Physical Access: Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals. The following physical controls must be in place:

6.7.3.1 Mainframe computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

- 6.7.3.2 File servers containing PI, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individual.
- 6.7.3.3 Workstations or personal computers (PC) must be secured against use by unauthorized individuals.
- 6.7.3.4 Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:
  - 6.7.3.4.1 Position workstations to minimize unauthorized viewing of protected health information.
  - 6.7.3.4.2 Grant workstation access only to those who need it in order to perform their job function.
  - 6.7.3.4.3 Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected health information (PHI).
- 6.7.3.5 Information Disposal / Media Re-Use of:
  - 6.7.3.5.1 Hard copy (paper and microfilm/fiche)
  - 6.7.3.5.2 Magnetic media (floppy disks, hard drives, zip disks, etc.) and
  - 6.7.3.5.3 CD ROM Disks
- 6.7.3.6 Accountability: Each entity must maintain a record of the movements of hardware and electronic media and any person responsible, therefore.

### 6.8 Data backup and Storage

- 6.8.1 When needed, create a retrievable, exact copy of electronic PI before movement of equipment. F. Other Media Controls:
  - 6.8.1.1 PI and Confidential Information stored on external media (diskettes, cd rom, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as PI or Confidential Information. Further, external media containing PI and Confidential Information must never be left unattended in unsecured areas.
  - 6.8.1.2 PI and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum-security requirements implemented:
    - 6.8.1.2.1 Power-on passwords
    - 6.8.1.2.2 Auto logoff or screen saver with password c. Encryption of stored data or other acceptable safeguards approved by Information Security Officer

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

Further, mobile computing devices must never be left unattended in unsecured areas.

6.8.1.2.3 If PI or Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of AHS Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with CMC.

### 6.9 Data Transfer/Printing

#### 6.9.1 Electronic Mass Data Transfer

6.9.2 Downloading and uploading PI, Confidential, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for research purposes that include PI must be approved through the Internal Review Board (IRB). All other mass downloads of information must be approved by the Application Owner and include only the minimum amount of information necessary to fulfill the request. Applicable Business.

### 6.10 Information Classification

6.10.1 Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

6.10.1.1 The following levels are to be used when classifying information – Secret, Confidential, Restricted & Public.

6.10.1.2 Secret is information, Information that requires substantial and multilevel protection due to its highly sensitive nature. Disclosure of such information could have a serious and sustained impact upon the government, national security, social cohesion, economic viability and health of the country. Information disclosure could potentially threaten life or seriously prejudice public order(eg: VIP health information, Critical health information, Credit Card Details, IP addresses, Network and Infrastructure Diagrams IT etc)

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

6.10.1.3 Confidential information that requires robust protection due to its critical support to decision-making within the Entity, and across health sector and government. Information that could disclose designs, configurations or vulnerabilities exploitable by those with malicious intent. Information that the Entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody (e.g., critical personal information, health/healthcare information, government information, financial information etc.).

6.10.1.3.1 Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for CMC, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner. (eg : Strategic/Critical Projects Contracts, payroll data, employee private records (medical records), audit reports, risks registers, assets registers, financial details in relation to projects or proposals, strategic/critical projects RFPs, Information Security Incident Reports etc.)

6.10.1.4 Restricted information that must be afforded limited confidentiality protection due to its use in the day-to-day operations. Disclosure of such information could have limited adverse impact on the functioning or reputation of Canadian Medical Center facilities Information that relates to the internal functioning of CMC and will not have general relevance and applicability to a wider audience. Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary, if they were to be revealed (eg: External Government Correspondences, Policies, Procedures, Standard Operating Procedures, Internal Circulars, contract of non-critical projects, projects charters, check lists etc.)

6.10.1.5 Public information destined to be used in public domain or public use, and has no legal, regulatory or organizational restrictions for its access and/or usage. Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping citizens, patients and other stakeholders understand better the

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

country's/governmental/organizational vision and values. (eg: Website information, news articles, marketing disseminations, education leaflets for patients /visitors published in Medical centers etc.)

### 6.10.2 Internal Information

6.10.2.1 Internal Information is intended for unrestricted use within CMC, and in some cases within affiliated organizations such as CMC business partners. This type of information is already widely-distributed within CMC, or it could be so distributed within the organization without advance permission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

6.10.2.2 Any information not explicitly classified as Secret, Confidential, Restricted or Public will, by default, be classified as Internal Information.

6.10.2.3 Public Information has been specifically approved for public release by a designated authority within each entity of CMC. Examples of Public Information may include marketing brochures and material posted to medical centers, entity internet web pages. Information Services must be deployed using a multi-layered are secure the system when leaving it.

6.10.2.4 Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

6.10.2.5 Access Control and Validation – Documented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

6.10.2.6 Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

### 6.11 Emergency Access

6.11.1 Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned custodian or owner is unavailable during an emergency.

6.11.1.1 Procedures must be documented to address:

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

- 6.11.1.1.1 Authorization,
- 6.11.1.1.2 Implementation, and
- 6.11.1.1.3 Revocation

### 6.12 Equipment and Media Controls

- 6.12.1 The disposal of information must ensure the continued protection of PI, Confidential and Internal Information.
- 6.12.2 Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain PI into and out of a facility, and the movement of these items within the facility.
- 6.12.3 The following specification must be addressed: unauthorized manner. Listed below are some methods that support data integrity.

### 6.13 Emergency Mode Operation Plan

- 6.13.1 A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
- 6.13.2 Testing and Revision Procedures: Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.
- 6.13.3 Applications and Data Criticality Analysis: The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.
- 6.13.4 Compliance Information Security Policy applies to all users of CMC information including: employees, medical staff, students, volunteers, and outside affiliates. Failure to comply with Information Security Policies and Standards by employees, medical staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable CANADIAN MEDICAL CENTER procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with CMC procedures. Further, penalties associated with state and federal laws may apply.
  - 6.13.4.1 Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

6.13.4.1.1 Unauthorized disclosure of Secret or Confidential Information as specified in Confidentiality Statement.

6.13.4.1.2 Unauthorized disclosure of a sign-on code (user id) or password.

6.13.4.1.3 Attempting to obtain a sign-on code or password that belongs to another person.

6.13.4.1.4 Using or attempting to use another person's sign-on code or password.

6.13.4.1.5 Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.

6.13.4.1.6 Installing or using unlicensed software on CMC computers.

6.13.4.1.7 The intentional unauthorized destruction of CMC information.

6.13.4.1.8 Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

### 6.14 Information Security Incident Management System

6.14.1 All CMC & CMC Group will use Incident Reporting Form – CMC-QDF-001VER 02 for reporting any information Security Incidents.

6.14.2 Upon receiving the incident, Quality Personnel shall acknowledge the submitted incident report and it will be provided to Information security officer's investigation & action completion.

6.14.3 The CMC & Group quality & IT team will ensure the compliance of this procedure.

6.14.3.1 The established incident reporting system will include incident identification, incident response, incident notification and learnings from incident which are shared with involved team members for their reference & preventing further occurrence.

## 7. DEFINITIONS AND ABBREVIATIONS:

| 7.1 | TERMS                | DEFINITIONS AND ABBREVIATIONS                                                                                                                                                                                                                                                 |
|-----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.2 | Information Security | Information Security- The preservation of confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved the processes to deal with security breaches |

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

|     |                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.3 | High Level Information Security. | High Level Information Security is a framework for third parties and facility staff to adhere to the promotion of security and guidance and advice where appropriate.                                                                                                                                                                                                                                                                                                                                                                                                               |
| 7.4 | Disciplinary action procedures   | The Disciplinary action procedures set out in CMC are designed to deal with misconduct or indiscipline, or allegation thereof. The procedures do not apply to matters relating to an employee's professional competence which is dealt with through the performance appraisal. The object of the procedures is to encourage improvement in the conduct of an individual employee and should not be viewed primarily as a means of imposing sanctions. All information's security violations are also subjected to include with disciplinary procedures of CMC Human Resources dept. |
| 7.5 | CMC                              | Licensed facilities in Abu Dhabi where ADHICS standards are applicable:<br>Canadian Medical Center LLC<br>Canadian Medical Center LLC Branch -2<br>Canadian Medical Center LLC Branch - 3<br>Canadian Medical & Rehabilitation Center LLC<br>CMC First Aid Clinic                                                                                                                                                                                                                                                                                                                   |
| 7.6 | User                             | Anyone who holds a valid account on the facility's network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 7.7 | ADHICS                           | Abu Dhabi Healthcare Information and cyber security standards                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### 8. DISTRIBUTION LIST:

On shareholder Policies IT

### 9. SPECIAL INSTRUCTIONS:

9.1 Violation or Any 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.

### 10. CROSS REFERENCE, RELATED LEGISLATION, FORMS, POLICY & DOCUMENTS:

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

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](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      | 23/12/2020    | 6.14 updated              | Page no 12 |

### 13. APPENDIX:

13.1 CMC-HR-F-038 Information Security acknowledgement form V1

13.2 Incident Report Form CMC

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

## INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY

### CMC-HR-F-038 Information Security acknowledgement form V1



Canadian Medical Center Group  
Human Resource Department

INFORMATION SECURITY ACKNOWLEDGMENT FORM  
CMC-HR-F-021

I acknowledge that during my employment or service with CMC Group and or subsidiaries, I may see or have access to documents, records, or data that include confidential and sensitive information. I understand that this Information may be confidential and sensitive by virtue of the organization's Acceptable Use Policy.

Under this policy, I shall not disclose Information about patients, employees or any personally, identifiable financial, health or medical Information, computer passwords and user IDs or account names unless explicitly given authorization. This applies whether the Information is in paper, digital, or other format or media.

Regarding patient records, I understand I may have access to patient records only as required in performing my assigned duties.

For access to IT security systems, understand I may have access to IT system(s) only as required in performing my assigned duties. I shall, in no way, play a part to compromise these systems or disclose information to unauthorized entities.

If in doubt about the confidentiality of any record or my ability to legally disclose information, agree to consult in writing with my supervisor (who in turn may consult with Information Security Manager) before disclosing any information.

If I become aware of any breach or suspected breach of information security, I will promptly report it in writing to my supervisor. Supervisors should in turn report the matter to Information Security Manager.

In addition, I acknowledge my responsibility to secure all data and information that may contain confidential information from the view of or access by unauthorized persons.

My signature on this form is to acknowledge that I have read and understood the 'Acceptable Use Policy' and various policies including 1. ISMS Information Security Management System, 2. Security Policy 3. Social Media Usage Policy 4. Access Control Policy 5. laptop- Desktop Policy which was given to me on my date of Joining, and that I have an obligation to fully adhere to these policies. I hereby confirm that:

- I have read the policy, familiarized myself with its contents and acknowledge that I am governed by it.
- The policy contains Important information on IT systems, their acceptable usage, rules, and regulations in relation to my employment with the organization. These have been explained to me during the induction / orientation session by the concerned authority.
- In case of any query regarding this policy, I shall make reasonable effort to contact the responsible authority for clarification.
- I hereby agree to comply with the policies, rules, and regulations. In case I am found in violation of this policy, the organization may take appropriate disciplinary action against me, or any other legal action that may be required as per the United Arab Emirates.

| 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:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

**INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY**

13.2 Incident Report Form CMC



**INCIDENT REPORTING FORM**

Unit /Medical Center Name:

Incident Report Reference Number: .....

**AN ACCIDENT / UNSAFE INCIDENT REPORT IS HIGHLY CONFIDENTIAL AND NOT A PART OF MEDICAL OR OTHER RECORDS**

General Guidelines: (1) Use black /blue ink (2) Write in clear, legible handwriting (3) Write objective view/comments and avoid personal opinions.

1. (4) Other details refer to – Policy on CMC/IRP/P1003/19 Incident Reporting & Investigation Procedures.  
Policy and Procedures

**Part A: (To be filled in by the Reporter)**

**DETAILS OF ACCIDENT/INCIDENT**

Prepared by:

(Name/Signature)

Date of Incident:

Time:

Department

Involved:

Location of Incident:

Incident Witnessed by:

**TYPE OF INCIDENT:** CMC/IRP/P1003/19 Policy on Incident Reporting for Medical Centres

- ☐ Clinical Incident ☐ Medication Incidents ☐ Health ☐ Radiation Incidents  
☐ Fire Incidents ☐ Security Incidents ☐ Vehicle Incidents ☐ Information Security Incidents  
☐ Personal Accidents & Dangerous Occurrences ☐ Other specify: .....

**Part B: Description of Accident/Incident (To be filled in by the Reporter) NOTE: Use Separate Paper If Applicable**

Person Involved in the Incident/Accident: ☐ Staff ☐ Visitors ☐ Contractor ☐ Subcontractor ☐ Outpatient ☐ Other(s):

Does it present a Patient / Staff / Visitors / Contractor / Subcontractor at risk? ☐ Yes ☐ No

**Details of Risks Present: (Give details of risks present and to whom)**

Received by Quality Department Representative (Print Name & Signature):

Date: ..... / ..... / ..... Time: .....

Feedback from Staff Involved/Concerned Staff in the Incident Report: NOTE: Use Separate Paper If Applicable

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

**INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY**



**Part C: Feedback of Concerned Department Head & Immediate Corrective Action Taken (To be filled in by the Initiating Department))**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Feedback of: Medical Manager Administrator QM Manager OTHER(S):

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

(This page below is to be filled in by Quality Representative only):

**Part D: Nature of Variance**

☐ STAFF RELATED   
 ☐ PATIENT RELATED   
 ☐ INFECTION CONTROL   
 ☐ OCCUPATIONAL H & S   
 ☐ FACILITY SAFETY  
☐ ENVIRONMENTAL   
☐ SECURITY VARIANCE   
☐ OTHER(S): \_\_\_\_\_

**Part E: Accident / Incident Investigation**

Is this Near Miss: ☐ Yes ☐ No \*What is the Accident Severity Levels? ☐ Level 1 ☐ Level 2 ☐ Level 3 ☐ Level 4

Does the Incident fall under Sentinel Event Class? (Level 4/5 are considered Sentinel Events) ☐ Yes ☐ No If YES, copy of report will be forwarded to concerned committee.

**Root Cause Analysis:**

MAN MATERIAL METHOD MACHINE MEASUREMENT MOTHER NATURE

Has this happened before? ☐ Yes ☐ No Last IR Code Number: \_\_\_\_\_ Date: \_\_\_\_/\_\_\_\_/\_\_\_\_  
(If applicable)

**Part F: Action Verification and Report Closing**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Signature: \_\_\_\_\_

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

**INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY**



**INCIDENT CLASSIFICATION AS PER DEPARTMENT OF HEALTH:**

☐ Level 1 – No harm, ☐ Level 2 – Required Minimal Interventions, ☐ Level 3 – Required Intensive analysis & actions,  
☐ Level 4 – Resulted in Serious, harm to patient, visitors & clients, ☐ SENTINEL EVENTS – As per DOH Guidelines.

Remarks from Quality & Accreditation Department :

**PREVENTIVE ACTION TAKEN**

| Policy & Procedure                                       | Instructions/ Counseling            | Facility/ Equipment                       | STATUS                          |                         |
|----------------------------------------------------------|-------------------------------------|-------------------------------------------|---------------------------------|-------------------------|
| <input type="checkbox"/> Evaluate                        | <input type="checkbox"/> To Staff   | <input type="checkbox"/> Evaluate         | <input type="checkbox"/> Closed | Date: ...../...../..... |
| <input type="checkbox"/> Recommend Change                | <input type="checkbox"/> To Patient | <input type="checkbox"/> Recommend Change | Name/ Signature                 |                         |
| <input type="checkbox"/> Changed                         | <input type="checkbox"/> To Others  | <input type="checkbox"/> Changed/ Removed |                                 |                         |
| <input type="checkbox"/> Enforced (Compliance/ Training) |                                     |                                           |                                 |                         |

**PREVENTIVE ACTION APART FROM ABOVE IF ANY:**

.....

.....

.....

.....

.....

.....

**FOLLOW UP /ACTION CLOSED:**

.....

.....

.....

.....

.....

| Department Head: | Quality Manager: |
|------------------|------------------|
| Signature:       | Signature:       |
| Date:            | Date:            |

Note: To be returned back to quality department within 24 hours of Incident, all information security incidents will be intimated to Information security Officer for their final action. Occupational Health Safety incidents required to submit as per OSH incident classification time frame.

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

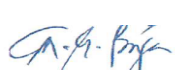
**INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY**

**14. APPROVAL:**

**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. Yahiya 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       |
| Manager Human Resources /Chief Administration Officer | Mr. Sallam Mohammed Naji |  | 01/07/2020 |
|                                                       | Name                     | Signature                                                                             | Date       |

|                     |                     |
|---------------------|---------------------|
| Department:         | CMC- IT-ADHICS- 003 |
| Issue Date:         | 01/07/2020          |
| Revision Date:      | 23/12/2020          |
| Next Revision Date: | 20/12/2022          |
| Version :           | 02                  |

**INFORMATION SECURITY HIGH LEVEL & RISK MANAGEMENT POLICY**