HUMAN RESOURCES SECURITY POLICY

1. PURPOSE

1.1 To ensure right resources are hired and utilized to support secure delivery of organizational objectives and services and are relieved in a manner that does not impact organizational assets, value, reputation and financial conditions any time current or in future.

2. POLICY STATEMENT:

2.1 Prior to employment, Canadian Medical center & Group ensures that employees and contractors understand their responsibilities in terms of organizational security system standards.

2.2 During employment, employees shall ensure that they are aware of and fulfil their information security responsibilities.

2.3 At termination or change in employment, to protect the government's interests as part of the process of changing or terminating employment as mentioned in this policy.

2.4 All the above laid down statements are depicted in procedure part of this policy also employee's awareness & adherence.

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.

5. RESPONSIBILITY

5.1 Canadian Medical Center Group of Companies Information Technology Department responsible for development, maintenance, enforcement and endorsement of the policy.

5.2 Canadian Medical Center Group of Companies Information Technology Department is responsible in implementation of the defined controls and ensuring compliance with this policy.

5.3 All Canadian Medical Center Group of Companies Users are responsible to read, understand and adhere to this policy in their day-to-day activities.

5.4 The Canadian Medical Center Group of Companies Information Technology Department is responsible to conduct awareness about the policy to Users.

5.5 Human Resource assigned personnel's & ADHICS Steering Committee are responsible for compliance to this policy within their area(s) of concern.

5.6 The IT Department is responsible to support the relevant business unit / section in implementation of the defined controls and ensuring compliance with this policy.

5.7 CMC HR Department is responsible to implement the defined security controls and ensure compliance of this policy.

6. PROCEDURE:

6.1 Screening

6.1.1 Human Resources Department / Administrative Unit shall establish a formal process for hiring, resigning and terminating of all CMC employees.

6.1.2 Human Resources Department / Administrative Unit or appropriate third parties shall carry out appropriate background verification checks "Screening" for all candidates for employment, contractor status or third-party user status. Such screening process shall take into consideration the level of trust and responsibility associated with the position and where permitted by UAE labour laws:

6.1.3 Canadian Medical Center facilities business needs, and relevant legal-regulatory and requirements.

6.1.4 Classification/sensitivity of the information, system, service, and infrastructure to be accessed and the perceived risks.

6.1.5 Privacy, protection of personal information and other relevant employment legislation where appropriate, components such as:

6.1.5.1 Proof of person's identity (e.g., Emirates ID, passport).

6.1.5.2 Proof of academic qualifications (e.g., certificates) by acquiring original documents or through direct verification with the relevant institution.

6.1.5.3 Proof of work experience (e.g., resume/CV and references).

6.1.5.4 Verification of two business references.

6.1.5.5 Criminal record checks.

6.1.5.6 Recruitments agencies or third parties providing contractors / consultants directly to CMC shall perform at least the same standard of personnel background verification checks as those indicated in the Human Security Policy (i.e., as part of the agency's responsibilities).

6.2 Terms and Conditions of Canadian Medical Center & Group Employment.

6.2.1 The employee's legal responsibilities and rights relevant to employment shall be made clear to all CMC employees at the beginning of employment and shall be clearly stated in the signed agreement.

6.2.2 All CMC employees shall sign an appropriate confidentiality agreement at the time of joining / engagement.

6.2.3 All CMC employees shall sign & understand the applicability of Information Security acknowledgement form (CMC-HR-F-038) as well as Acceptable Use Policy acknowledgement form (CMC-HR-F-039) upon their joining with CMC facilities.

6.2.4 This agreement shall require the employee to comply with all applicable CMC information security policies and procedures.

6.2.5 Contract staff or contract agency providing staff visiting sensitive areas (e.g., main datacenter and server rooms) shall be required to sign a confidentiality agreement as required.

6.2.6 The terms and condition of employment shall include all responsibility of the users towards information security.

6.3 Management Responsibilities:

6.3.1 All Department Managers shall require all employees, who work under their area of concern, to apply security in accordance with CMC information security policies and procedures.

6.3.2 All Department Managers/In charges/Supervisors shall ensure that employees are:

6.3.2.1 Appropriately brief on their information security roles and responsibilities.

6.3.2.2 Encouraged to fulfill CMC information security policies.

6.3.2.3 Continue to have the appropriate skills and qualifications.

6.3.3 All the employees shall orient on a regular basis (especially on information security aspects)

6.3.4 Managers/Immediate Supervisors /HODs shall be aware of the personal circumstances of their employee/staff; and shall be on the lookout for any behavioral change that may lead to security breach or violation.

6.3.4.1 Employee vacations and leave of absences shall not affect the availability and performance of service provision at CMC.

6.3.4.2 When applying for a leave of absence, the following shall be considered:

6.3.4.3 Leave request shall be sent before enough time for processing.

6.3.4.4 Employee shall specify the followings in his leave request:

6.3.4.4.1 List of duties and activities during his leave period (Vacation handover form: CMC-HR-F-F041)

6.3.4.4.2 Name(s) of employee(s) that will be responsible to take care of these duties and activities in his absence.

6.3.4.4.3 Employee shall ensure that business will continue during his absence.

6.4 Background Verification

6.4.1 Background verification of general / non-clinical staff will be done with the provided reference(s) from the candidate. Supporting documents must be placed in employee personnel file.

6.4.2 Background verification of clinical staff will be done through dataflow verification report provided by the employee. Otherwise, HR – Licensing will verify the required documents through dataflow group; supporting documents must be placed in employee personnel file.

6.4.3 Department HOD / HR Team are the sole authorized personnel who can perform background verifications.

6.4.4 Below are the certifications which require verification:

6.4.4.1 Qualification(s)– Verification will be done through attestation of UAE Ministry of Foreign Affairs or through Dataflow Group

6.4.4.2 Experience(s) - Verification will be done through provided experience certificates for non-clinical and dataflow group for clinical staff; If additional verification is required, this can be done telephonically.

6.4.4.3 Health License(s) – Applicable to only clinical staff, verification will be done through dataflow group

6.5 Information Security Awareness, Education and Training

6.5.1 Suitable information security awareness, training and education shall be provided to all CMC employees, clarifying their responsibilities relating to CMC information security policies and procedures and all relevant obligations defined in job description.

6.5.2 The security awareness may include, but not be limited to:

6.5.2.1 A formal induction process that includes security training, prior to being granted access to CMC network and systems.

6.5.2.2 Ongoing training in security control requirements, legal-regulatory responsibilities and generally accepted information security procedures, suitable to the employees' roles and responsibilities.

6.5.3 Information security awareness shall cover general aspects such as:

6.5.3.1 CMC Management commitment to information security objectives.

6.5.3.2 Basic information security procedures (e.g., information security incident reporting) and security standards (e.g., password security, assets handling protection, antivirus controls, and clean and clear desks)

6.5.3.3 Personal accountability and responsibilities towards protecting CMC assets.

6.5.3.3.1 Annual information security awareness program and training plan.

6.5.3.3.2 Issue awareness material (e.g., information printouts or email communications) in order to keep all CMC employees aware of their information security roles and responsibilities.

6.5.3.4 Management shall allocate sufficient on-the-job time for CMC employees to familiarize themselves with CMC information security policies, procedures and the relevant ways of conducting business.

6.5.3.5 Every CMC employee shall attend an information security awareness session within three months of the hiring date. Each employee shall sign a statement that he has attended such sessions, understood the material presented, had an opportunity to ask questions, and agree to perform his work according to CMC information security policies and procedures.

6.6 Disciplinary Process

6.6.1 Disciplinary process shall provide a gradual response taking into consideration factors such as:

6.6.1.1 Nature and severity of the security breach.

6.6.1.2 Impact on the business

6.6.1.3 If it is a repeated offence.

6.6.1.4 Whether or not the violator was properly trained.

6.6.1.5 Relevant legislations.

6.6.2 A formal disciplinary action shall be taken in accordance with CMC personnel policies, procedures, guidelines and instructions memos.
(Reference: CMC- HR- 007 CMC Disciplinary code policy)

6.6.3 CMC information and infrastructure (e.g., network, systems and services) shall not be used for purposes other than CMC business needs. Any such fraudulent activities detected shall be dealt as per CMC personnel disciplinary action procedure.

6.7 Termination or Change of Employment Responsibilities

6.7.1 Responsibilities and practices for performing employment termination or change of employment shall be clearly defined and assigned. This may include, but not be limited to:

6.7.1.1 Termination processes that ensure removal of access to all information resources.

6.7.1.2 Changes of responsibilities and duties within CMC processed as a termination (of the old position) and re-hire (to the new position), using transfer policy controls for those processes unless otherwise indicated.

6.7.1.3 Processes ensuring that employees are appropriately informed of a person's changed status; and any post-employment responsibilities are specified in the terms and conditions of employment, or contractor's or third party's contract.

6.7.1.4 Human Resources Department / Administrative Unit in cooperation with employee's supervisors shall promptly inform about employee transfers or job duty changes, so that all necessary measures are taken with regard to the revocation or change of access rights (logical and/or physical) to assets.

6.7.2 In the event an employee is terminated, the followings shall be considered:

6.7.2.1 Releasing the employee of all CMC related duties and terminating all work-related privileges at the time of termination. (Employee Handover Form CMC-HR-F-041)

6.7.2.2 Ensuring all CMC property and information in the concerned employee's custody is returned before the employee leaves CMC premises.

6.7.2.3 Notifying all administrators handling user accounts used by the employee as soon as the termination is known.

7. DEFINITIONS AND ABBREVIATIONS:

Sl No	TERMS	DEFINITIONS AND ABBREVIATIONS
7.1	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.
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	Screening	A process to verify facts about individuals related to their identity, professional credentials, previous employment, education and skills
7.4	ADHICS	Abu Dhabi healthcare information and cyber security standards

8. DISTRIBUTION LIST:

On shareholder Policies HR

9. SPECIAL INSTRUCTIONS:

9.1 Human resources management shall in compliance with relevant HR Law and its amendments, or any other regulations the entity follows in this context.

9.2 The Human Resource department assigned personnel reserves the right to check the compliance of this policy on a periodic basis.

9.3 Any exceptions to this policy with valid justification require approval from IT Manager on a case-to-case basis any matters involved with ADHICS requirements.

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

10.3 BSI IT security baselines https://www.bsi.de • Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management https://www.axelos.com/best-practice-solutions/iti

10.4 ISD Strategy https://portal.uea.ac.uk/information-services/strategy-planning-andcompliance/isd-strategy

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	21/01/2021	Addition of Background Verification	Page 4

13. APPENDIX:

14. APPROVAL SHEET:

Document Developed By:			
Licensing Officer	Ms. Aprilia Ariesia		21/01/2020
	Name	Signature	Date
IT Support	Mr. Muhamed Shifas Avudiyil		21/01/2020
	Name	Signature	Date
Document Developed & Reviewed By:			
IT supervisor/IT Manager	Mr. Yahiya Mannooparambil		21/01/2020
	Name	Signature	Date
Nurse Manager & Quality Control Supervisor	Ms. Monina Baja		21/01/2020
	Name	Signature	Date
Document Approved By:			
Chief Operating Officer/Chief Financial Officer	Mr. Imran Saleem		21/01/2020
	Name	Signature	Date
Manager Human Resources /Chief Administration Officer	Mr. Sallam Mohammed Naji		21/01/2020
	Name	Signature	Date