

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

1. PURPOSE

- 1.1 This IT Service Continuity Plan (ITSCP) is in effect for the critical IT service and technology components under the control of Canadian Medical Center & Group - IT in Abu Dhabi - UAE.
- 1.2 The main objective of this document is to provide a means of mitigation, preparation, response and recovery in the event of a disaster or serious disruption. The ITSCP will provide seamless failover for mission critical IT services.
- 1.3 The IT Service Continuity Plan is a plan defining the steps required to recover one or more IT Services. The Plan also identifies the triggers for invocation, people to be involved, communications etc. Business Impact Analysis and Risk Analysis should be conducted to support this plan.

2. POLICY STATEMENT:

- 2.1 The goal of CMC IT Service Continuity Policy is to ensure business critical services are operational in the event of a disaster and information processing services are recovered within agreed timescales.

3. SCOPE:

- 3.1 This policy applies in reference to the inputs received from business, below items are covered under the scope of IS Service Continuity. All Canadian Medical Center Group of Companies are under scope of BCP for HIS, ERP, Network & IT Desks
 - 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 business continuity plan for CMC network owned under Canadian Medical Center facilities by CMC IT team.

5. RESPONSIBILITY

- 6.1 The Information Technology Department is responsible for development, maintenance, enforcement and endorsement of the policy.
- 6.2 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.
- 6.3 All Users are responsible to read, understand and adhere to this policy in their day-to-day activities.
- 6.4 Top management is responsible for compliance to this policy within their area(s) of concern.

6. PROCEDURE:

6.1 Objective

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

6.1.1 To provide a means of mitigation, preparation, response and recovery in the event of a disaster or disruption such as, but not limited to

6.1.1.1 Loss of, serious damage to, or inability to access premises.

6.1.1.2 Loss of a large number of staff (eg. pandemic).

6.1.1.3 Loss of key equipment/services.

6.1.1.4 Loss of voice & data communications.

6.1.1.4.1 The document defines the steps required to recover critical IT services. It also identifies the triggers for invocation, people to be involved, communications etc. Business Impact Analysis and Risk Analysis shall support this plan.

6.1.2 Responsibilities

6.1.2.1 Senior Management

6.1.2.1.1 Approve scheduled IT service continuity drills

6.1.2.1.2 Provide suggestions for IT service continuity plan

6.1.3 Service Continuity Manager/IT Support

6.1.3.1 At time of disaster – Invoke IT service continuity plan and coordinate with teams and senior management

6.1.3.2 Plan and coordinate IT service continuity exercises.

6.1.3.3 Review and update the IT Service continuity policy document.

6.1.3.4 Report exercise and test results to senior management.

6.1.3.5 Make decisions about the need for testing, and activation of the recovery plan.

6.1.4 Change Manager/ IT Manager

6.1.4.1 Assess the impact on changes to the IT service continuity policy document.

6.1.4.2 Notify Service Continuity Manager about major changes which could affect the plan.

6.1.4.3 Approve changes to the policy document

6.1.4.4 Approval for mock IT service continuity tests.

6.1.5 Service Desk

6.1.5.1 Communicate with users as instructed by Service Continuity Manager/IT Manager.

6.1.5.2 Function Heads/IT Support

6.1.5.2.1 Execute documented continuity and recovery procedures.

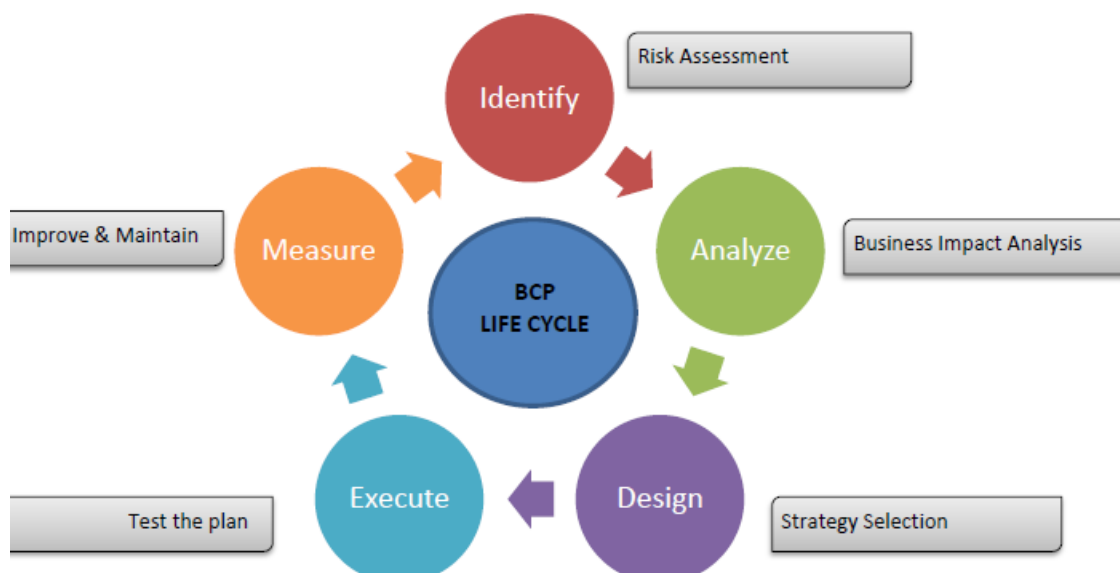
6.1.5.2.2 Inform Service Continuity Manager of any disruptions.

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

- 6.1.5.2.3 Monitor and track status of technical recovery procedures during an exercise or a disaster.
- 6.1.5.2.4 Ensure adequate backups for critical system components are periodically taken.
- 6.1.5.2.5 Vendor
- 6.1.5.2.6 Participate in continuity drills if required.
- 6.1.5.2.7 Work with appropriate teams in the event of a disruption to execute the continuity plan.

6.1.6 BCP Life Cycle



6.1.7 Identify

- 6.1.7.1 List out critical processes and their dependencies.
- 6.1.7.2 Risk Assessment
 - 6.1.7.2.1 A risk assessment is a process to identify potential hazards and analyze what could happen if a hazard occurs. These give an idea to prioritize high impact risks and implement controls to mitigate their impact.
 - 6.1.7.2.1.1 Risk assessment shall be done annually or whenever changes take place in the environment.
 - 6.1.7.2.1.2 Risk assessment shall list all threats, vulnerabilities and emerging risk for every type of asset.
 - 6.1.7.2.1.3 Please refer to ISMS risk assessments & mitigation plan- CMC-IT-008 VER 01

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

6.1.8 Analyze

6.1.8.1 Determine the impact of dependencies on mission critical processes.

6.1.9 Business Impact Analysis

6.1.9.1 A business impact analysis (BIA) is the process for determining the potential impacts resulting from the interruption of time sensitive or critical business processes.

6.1.9.1.1 BIA shall be carried out annually or when changes take place in the environment.

6.1.9.1.2 BIA shall be current and relevant.

6.1.10 Design

6.1.10.1 Draw a plan to mitigate the level of impact on critical processes due to disruption in the dependencies.

6.1.11 Strategy Selection

6.1.11.1 Most appropriate strategy shall be selected to ensure RTO and RPO are within acceptable levels.

6.1.11.2 Strategy shall include technology and people

6.1.12 Execute

6.1.12.1 Implement the plan in a controlled environment.

6.1.13 Test the plan

6.1.13.1 Simulate a disaster and implement the plan to see its effectiveness. Several gaps may be discovered during this exercise.

6.1.14 Measure

6.1.14.1 Determine the success of the plan.

6.1.15 Improve and maintain

6.1.15.1 Identify areas of improvement from the test results. Based on these learnings, strengthen the plan

6.1.16 Approach towards Business Impact Analysis

6.1.16.1 Establish the Criticality & Rating Criteria

6.1.16.2 Consider the following list of consequences of a disruption for each of the Business Functions identified.

6.1.17 Disruption to the Business

6.1.17.1 Loss of assets: key personnel, physical assets, data assets, intangible

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

assets

6.1.17.2 Disruption to the continuity of service and operations

6.1.17.3 Violation of law / regulation

6.1.17.4 Public Perception

6.1.18 Impact on the business

6.1.18.1 Financial

6.1.18.2 Customers and suppliers

6.1.18.3 Public relations / credibility

6.1.18.4 Legal

6.1.18.5 Regulatory requirements / considerations

6.1.18.6 Environmental

6.1.18.7 Operational

6.1.18.8 Personnel

6.1.18.9 Other resources

6.1.19 Loss exposure to the business (*Quantitative*)

6.1.19.1 Property loss

6.1.19.2 Revenue loss

6.1.19.3 Fines

6.1.19.4 Cash flow

6.1.19.5 Accounts receivable

6.1.19.6 Accounts payable

6.1.19.7 Legal liability

6.1.19.8 Human resources

6.1.19.9 Additional expenses / increased cost of working

6.1.20 Loss exposure to the business *Qualitative*

6.1.20.1 Human resources

6.1.20.2 Morale

6.1.20.3 Confidence

6.1.20.4 Legal

6.1.20.5 Social and corporate image

6.1.20.6 Financial community credibility

6.1.21 Business Impact Analysis – 2021

6.1.21.1 BIA was performed for business processes and functions handled CMC to determine their criticality to business. Business owners listed all critical services in their units and prioritized them according to their criticality of not being available to the business.

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

#.	Service Name	Criticality rating	RTO Recovery time objective	RPO Recovery point objective	Business Units
1	Insta HIS	Critical	30 minutes	10 minutes	All licensed facilities – CMC at Abu Dhabi
2	Network	Critical	30 minutes	10 minutes	All Units All licensed facilities – CMC at Abu Dhabi
3	Service Desk	Major	30 minutes	10 minutes	All Units All licensed facilities – CMC at Abu Dhabi

6.1.22 IT Continuity Plan

No.	Service	Service Owner	Continuity Option
1	Insta HIS	IT Manager-Mr. Yahiya	Mirroring (DR Site) Server Redundancy server
2	Network	IT support – Mr. Shifas	Auto failover
4	IT Service Desk	IT Software-Mr. Zeeshan	Call rerouting

6.1.23 Backups

6.1.23.1 **Daily Backup:** Daily full database backup of Insta HMS database is taken every day at 12:01 AM to a shared storage. These daily backup as retained for One week.

Host	Policy Name	Backup Location	Schedule	Start Time	Retention Period
	Daily full Backup	/Share/dbbackup/hms	Daily	12:01 AM	One week

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

6.1.24 Roles & Responsibilities - BCP

IT Manager/ IT Supervisor	- Decide /Declare BCP invocation - Keep Sr.Management/Key business stakeholders informed
IT Continuity Manager /IT Support	- Notify IT Head - Oversee BCP invocation - Liasion between different teams - Monitor situation
Functional Manager / IT Manager/IT Supervisor	- Initiate BCP - Recovery actions - Monitor situation
IT Desk/ Software Support	- Notify Users - Follow directions given by Continuity & Functional Managers
End Users CMC	Follow IT team directions

6.1.25 Business Continuity Plan Exercises and Testing

6.1.25.1 Business continuity exercises are essential to establish appropriate preparedness levels during an actual disaster and effectiveness of existing continuity plan. The exercises also highlight potential areas of improvement that can strengthen the BCP

6.1.25.1.1 Test dates shall be decided to ensure minimal impact on business.

6.1.25.1.2 Testing requires change management approval. CAB approval is mandatory.

6.1.25.2 Service Continuity Manager along with Function Managers shall plan the BCP drill at least once per year. A change request is created for BCP drill and shall be approved by Change Advisory Board before proceeding. Associate Vice President IT shall be updated about the drill. Business stakeholders shall be notified to ensure they are well prepared.

6.1.25.3 Change request for BCP drill shall contain the following:

6.1.25.3.1 Business approval

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

6.1.25.3.2 Affected Services

6.1.25.3.3 Affected business units

6.1.25.3.4 Timeline of activities including which IT groups were involved

6.1.25.3.5 Length of outage

6.1.25.3.6 Risk analysis

6.1.25.3.7 Impact analysis

6.1.25.3.8 Rollout plan

6.1.25.3.9 Backup plan

6.1.25.3.10 Implementation Checklist

6.1.25.3.11 Scheduled start time

6.1.25.3.12 Scheduled end time

6.1.25.3.13 Actual start time

6.1.25.3.14 Actual end time

6.1.25.3.15 Business confirmation

6.1.25.3.16 Incidents encountered (if any)

6.1.25.4 After completion of the drill, the results are analyzed to determine effectiveness & areas of improvement.

6.1.26 Information Security Requirements in IT Service Continuity

6.1.26.1 During an IT service continuity situation, following information security requirements are to be followed.

6.1.26.1.1 Access to information/information assets shall continue to follow as per Access Control Policy.

6.1.26.1.2 Access logs on applications, network devices, databases, servers shall be recorded.

6.1.26.1.3 Information processing assets shall be protected as per Physical and Environmental security policy (example: CCTV, HVAC, fire suppression system, visitor register etc..)

6.1.26.1.4 DR site to be configured exactly the same as data center.
Examples:

6.1.26.1.5 Ports open on the firewall in DR site should be the same as the data center.

6.1.26.1.6 Anti-virus version running at both locations shall be the same.

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

6.1.27 Key Contacts

6.1.27.1 The following staff/functions are responsible for responding to those procedures or ensuring the procedures are taken care of and recording any issues or problems encountered.

6.1.27.2 Contact will be made via the normal escalation procedures.

Role	Name	Contact Details	Extn #
IT Manager/IT Supervisor	Mr. Yahiya Manooparambil	0526552116	225
IT Support	Mr. Muhamed Shifas Avudiyil	0527824304	225
Human Resources - Rep	Ms. Aprilia	0547729321	220
IT Desk	Mr. Zeeshan	0555918166	225

7. DEFINITIONS AND ABBREVIATIONS:

SI No	TERMS	DEFINITIONS AND ABBREVIATIONS
7.1	Business Continuity Plan (BCP)	A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans.
7.2	Business Impact Analysis (BIA)	BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recover Time Objective (RTO), Recovery Point Objectives (RPO) and minimum Service Level Targets for each IT Service
7.3	Crisis Management	The Process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for Strategic issues such as managing media relations and shareholder confidence and decides when to invoke Business Continuity Plan.

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

7.4	Information Damage	A sudden, unplanned event that creates an inability for an organisation or entity to provide the critical business functions for some predetermined period of time which results in great damage or loss.
7.5	Disaster recovery	Activities and programs designed to return the technology of an organisation to an acceptable condition after a disaster has occurred.
7.6	IT Service Continuity Plan	The documentation that defines the resources, actions, tasks and data required to manage the business and IT recover process in the event of a disaster.
7.7	Emergency Response	The processes required to respond to the earliest stage of an event, including life safety, protection of property, and containment of the situation and minimization of further impact. Multiple teams with specific skill sets may be deployed during this phase
7.8	Exercises	An activity that is performed for the purposes of validation of documentation and procedures training and formalization and conditioning of team members to improve performance in the event of a disaster. Types of exercises include: Peer review, structured walkthroughs, individual team table tops, combined team table tops, simulation exercises, operational exercises and mock simulation exercises.
7.9	Risk assessment	A formal document that is used in conjunction with a BIA to validate the MTO and RPO of an application and determine an appropriate technology strategy to be implemented.
7.10	Recovery strategy	An approach implemented by an organisation, system, piece of hardware or service to ensure the recovery of that entity within the required MTO and with the required RPO in the event of a disaster. Different hardware, systems or components may utilize different recovery strategies, which generally fall into

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

7.11	Risk Mitigation	The implementation of measures to deter specific threats to the continuity of business operations.
7.12	Threats	Events that have a potential of becoming a disaster. For example any natural events such as smoke, fire or any other event which could either have impact on material of the back and/or impact on human being.
7.13	ADHICS	Abu Dhabi healthcare information and cyber security standards

8. DISTRIBUTION LIST:

On shareholder Policies IT

9. SPECIAL INSTRUCTIONS:

9.1 The IT Department reserves the right to check the compliance of this plan as & when required.

9.2 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 Code of conduct Canadian Medical Center & Group: CMC-HR-006

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

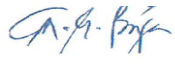
13. APPENDIX:

NA

Department:	CMC- IT-ADHICS- 015
Issue Date:	01/07/2020
Revision Date:	01/07/2022
Next Revision Date:	01/07/2022
Version :	01

BUSINESS CONTINUITY PLAN

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. 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