BUSINESS CONTINUITY POLICY

STAR HFL

VERSION 1.0

PREPARED BY:
APPROVED BY:
BOARD OF DIRECTORS
On behalf of Board of Directors: **Ashish Jain** Managing Director DIN: 02041164

Title	Star Business Continuity Policy
Date of Latest Release	
Version	1.0

1. Overview

1.1 Purpose

The purpose of the Business Continuity Plan (BCP) is to clearly lay out the roles, responsibilities and tasks of staff and resources to resume business operations in response to events that interrupt normal business operations.

1.2 Document Structure

This document has ten sections:

- **Business Continuity Overview:** Outlines the scope, goals, basic assumptions and function of this plan.
- **Business Continuity Governance:** Outlines who sits on the Business Continuity Steering and Working Committees.
- **Business Impact Analysis (BIA):** Identifies the organization's mandate and critical services or products, ranks the order of priority of services or products for continuous delivery or rapid recovery and identify internal and external impacts of disruptions.
- **Plan, Measures and Arrangements for Business Continuity:** These plans and arrangements detail the ways and means to ensure critical services and products are delivered at minimum service levels within tolerable down times.
- **Readiness Procedures:** Business continuity plans can be smoothly and effectively implemented by providing training (drills) and exercises (table top) to Staff and the BCP Governance Committees.
- **Quality Assurance Techniques:** Review of the BCP should assess the plan's accuracy, relevance and effectiveness. It should also uncover which aspects of the BCP require improvement as well as identify gaps. Continual appraisal of the BCP is essential to maintaining its effectiveness.
- **Glossary of Terms:** Incorporated terms utilized by the nation-wide Incident Command System.
- **Appendix A - Project Roles and Responsibilities:** The defined roles and responsibilities of project Steering and Working Committee members and the reporting relationships between those members as identified in the Governance chart.

1.3 Scope

This document contains business continuity plans that include:

- **What must be done:** The steps that must be taken to resume business functions after an interruption to business operations.
- **Who will do it:** Personnel responsible for performing tasks to resume functions.
- **When it must be done:** A timeline for executing the tasks in the plan.

This plan may require the activation of other plans to be fully effective (e.g. Emergency Response Plan).

1.4 Assumptions

- The department's Emergency Response Plan has addressed immediately threats to life and safety.
- Plans are living documents and can be scaled as needed depending on the severity of the interruption.
- Staff is aware that they can receive information updates, instructions and status reports via our mass text communication system.

1.5 Comprehensive Emergency Management Approach

A comprehensive emergency management approach ensures a coordinated response to any incident.This methodology involves strong communication between the Business Continuity and Emergency Response Plan to ensure the linkages between them are lucid and complementary.

2. BCP Governance

A BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities.

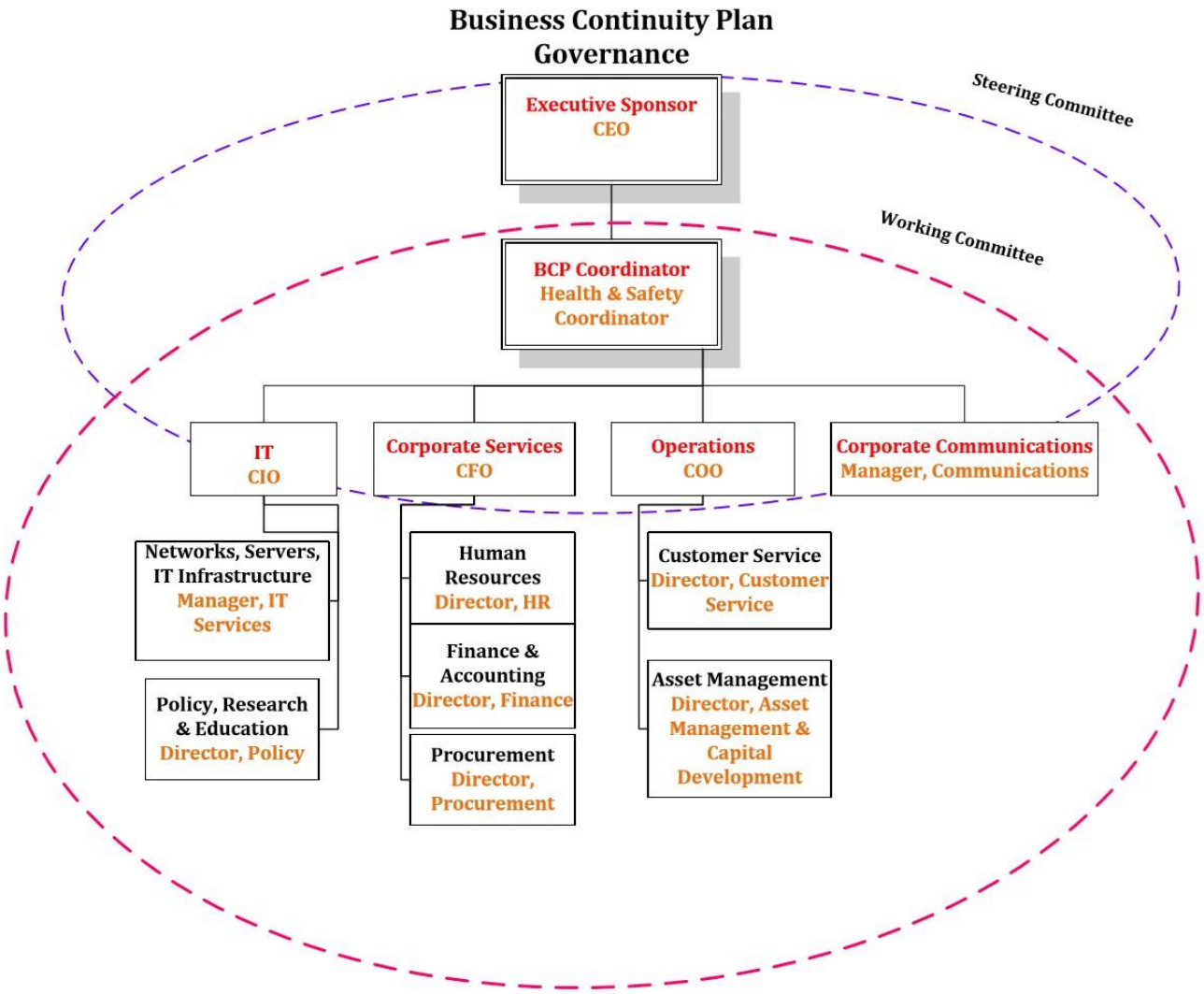
The BCP Steering Committee is responsible for the oversight, initiation, planning, approval and testing of the BCP. This Steering Committee is commonly co-chaired by the Executive Sponsor and the Coordinator.

Steering Committee would normally:

- approve the governance structure;
- clarify their roles and those of participants in the program;
- provide strategic direction and communicate essential messages;
- approve the results of the BIA;
- review the critical services and products that have been identified;
- approve the continuity plans and arrangement;
- monitor quality assurance activities; and
- resolve conflicting interests and priorities.

2.1 Governance Model

The following is the BCP Governance structure which identifies the Steering and Working Committees.



3. Business Impact Analysis

The purpose of the Business Impact Analysis (BIA) is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

BUSINESS IMPACT ANALYSIS

Critical Function					
BIA Owner					
Assessment Date		Review Date			
CRITICAL FUNCTION PRIORITY:					
Impact on Business					
Time	Impact				
First 24 Hours					
24-48 hours					
Up to 1 week					
Up to 2 weeks					
Requirements for Recovery					
Time	People	Premises	Technology	Information	Suppliers & Partners
First 24 Hours					
24-48 Hours					
24-48 Hours					
Up to 1 Week					

Identify the mandate and critical aspects of an organization

This step determines what goods or services must be delivered. Information can be obtained from the mission statement of the organization, and legal requirements for delivering specific services and products.

Prioritize critical services or products

Once the critical services or products are identified, they must be prioritized based on minimum acceptable delivery levels and the maximum period the service can be down before severe damage to the organization results. To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

Identify impacts of disruptions

The impact of a disruption to a critical service or business product determines how long the organization could function without the service or product, and how long clients would accept its unavailability. It will be necessary to determine the time period that a service or product could be unavailable before severe impact is felt.

Identify areas of potential revenue loss

To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue. If these processes and functions are not performed, is revenue lost? How much? If services or goods cannot be provided, would the organization lose revenue? If so, how much revenue, and for what length of time? If clientscannot access certain services or products would they then to go to another provider, resulting in further loss of revenue?

Identify additional expenses

If a business function or process is inoperable, how long would it take before additional expenses would start to add up? How long could the function be unavailable before extra personnel would have to be hired? Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties?

Identify intangible losses

Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations. Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards.

Insurance requirements

Since few organizations can afford to pay the full costs of a recovery; having insurance ensures thatrecovery is fully or partially financed.

When considering insurance options, decide what threats to cover. It is important to use the BIA to helpdecide both what needs insurance coverage, and the corresponding level of coverage. Some aspects of an operation may be over-insured or underinsured. Minimize the possibility of overlooking a scenario, and to ensure coverage for all eventualities.

Ranking

Once all relevant information has been collected and assembled, rankings for the critical businessservices or products can be produced. Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause. Minimum service levels and maximum allowable downtimes are then determined.

Identify dependencies

It is important to identify the internal and external dependencies of critical services or products, sinceservice delivery relies on those dependencies.

Internal dependencies include employee availability, corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and support services such as finance, human resources, security and information technology support.

External dependencies include suppliers, any external corporate assets such as equipment, facilities,computer applications, data, tools, vehicles, and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service.

4. Plans, Measures and Arrangements for Business Continuity

Plans for business continuity

This step consists of the preparation of detailed response/recovery plans and arrangements to ensure continuity. These plans and arrangements detail the ways and means to ensure critical services and products are delivered at a minimum service levels within tolerable down times.

CRHC has mapped out process flow charts for the following incidents (see Appendix B & C):

1. *Corporate Services*
   a. Office Power Outage <24 hrs.
   b. Cannot Access the Office Building – undefined time

2. *Information Technology*
    a. Office Power Outage >24 hrs.
    b. Office Power Outage + 24 hrs.
    c. Internet Down > 24 hrs.

3. *Operations*
    a. Office Power Outage > 24 hrs.
    b. Office Power Outage > 24 hrs. (Rent Subsidies)
    c. Office Power Outage > 24 hrs. (Property Development)
    d. Office Power Outage + 24 hrs. (Asset Management)
    e. Alternate Location up to 6 months

Mitigating threats and risks

Threats and risks are identified in the BIA or in a full-threat-and-risk assessment. Moderating risk is an ongoing process and should be performed even when the BCP is not activated. For example, if an organization requires electricity for production, the risk of a short-term power outage can be mitigated by installing stand-by generators.

Another example would be an organization that relies on internal and external telecommunications to function effectively. Communications failures can be minimized by using alternate communication networks or installing redundant systems.

Analyse current recovery capabilities

Consider recovery arrangements the organization already has in place, and their continued applicability. Include them in the BCP if they are relevant.

Response preparation

Proper response to a crisis for the organization requires teams to lead and support recovery and response operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

The number and scope of teams will vary depending on organization's size, function and structure, and can include:

- Command and Control Teams that include a Crisis Management Team, and a Response, Continuation or Recovery Management Team.
- Task Oriented Teams that include an Alternate Site Coordination Team, Contracting and Procurement Team, Damage Assessment and Salvage Team, Finance and Accounting Team, Hazardous Materials Team, Insurance Team, Legal Issues Team, Telecommunications/ Alternate Communications Team, Mechanical Equipment Team, Mainframe/ Midrange Team, Notification Team, Personal Computer/ Local area Network Team, Public and Media Relations Team, Transport Coordination Team and Vital Records Management Team

The duties and responsibilities for each team must be defined, and include identifying the teammembers and authority structure, identifying the specific team tasks, member's roles and responsibilities, creation of contact lists and identifying possible alternate members.

For the teams to function despite personnel loss or availability, it may be necessary to multitask teamsand provide cross-team training.

Alternate locations

There are three types of alternate locations:

1. Cold site is an alternate facility that is not furnished and equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and a substantial time and effort is required to make a cold site fully operational. Cold sites are the least expensive option.
2. Warm site is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. Warm sites are more expensive than cold sites.
3. Hot site is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds. Hot sites are the most expensive option.

5. Readiness Procedures

Training

Business continuity plans can be smoothly and effectively implemented by:

- Having all employees and staff briefed on the contents of the BCP and aware of their individual responsibilities (drills).
- Having Committee members with direct responsibilities trained for tasks they will be required to perform and be aware of other teams' functions (table top exercises).

Table Top Exercises

After training, table top exercises should be developed and scheduled in order to achieve and maintain high levels of competence and readiness. While exercises are time and resource consuming, they are the

best method for validating a plan. The following items should be incorporated when planning an exercise:

Goal

The part of the BCP to be tested.

Objectives

The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely.

Scope

Identifies the departments or organizations involved, the geographical area, and the test conditions and presentation.

Artificial aspects and assumptions

Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed and equipment availability.

Participant Instructions

Explains that the exercise provides an opportunity to test procedures before an actual disaster.

Exercise Narrative

Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and anyexternal conditions.

Communications for Participants

Enhanced realism can be achieved by giving participants access to emergency contact personnel who share in the exercise. Messages can also be passed to participants during an exercise to alter or createnew conditions.

Testing and Post-Exercise Evaluation

The exercise should be monitored impartially to determine whether objectives were achieved. Participants' performance, including attitude, decisiveness, command, coordination, communication and control should be assessed. Debriefing should be short, yet comprehensive, explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation.

Exercise complexity level can also be enhanced by focusing the exercise on one part of the BCP instead of involving the entire organization annually.

6. Quality Assurance Techniques

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. It should also uncover which aspects of a BCP need improvement as well as identify gaps. Continuous appraisal of the BCP is essential to maintaining its effectiveness. The appraisal can be performed by an internal review, or by an external audit.

Internal review

It is recommended that organizations review their BCP:

- On a scheduled basis (annually or bi-annually)
- when changes to the threat environment occur;
- when substantive changes to the organization take place; and
- after an exercise to incorporate findings.

External audit

When auditing the BCP, consultants nominally verify:

- Procedures used to determine critical services and processes
- Methodology, accuracy, and comprehensiveness of continuity plans

What to do when a disruption occurs

Disruptions are handled in three steps:

A. Response
B. Continuation of critical services
C. Recovery and restoration

6.1 Response

Incident response involves the deployment of teams, plans, measures and arrangements. The following tasks are accomplished during the response phase:

a. Incident Management
b. Communications Management
c. Operations Management

Incident Management

Incident management includes the following measures:

- notifying management, employees, and other stakeholders;
- assuming control of the situation;
- identifying the range and scope of damage;
- implementing plans;
- identifying infrastructure outages; and
- coordinating support from internal and external sources.

Communications Management

Communications management is essential to control rumors, maintain contact with the media, emergency services and vendors, and assure employees, the public and other affected stakeholders. Communications management requirements may necessitate building redundancies into communications systems and creating a communications plan to adequately address all requirements. The Mass Text service will be used to update Staff on incident status.

Operations Management

An Incident Command Post (ICP) can be used to manage operations in the event of a disruption. Having a centralized ICP where information and resources can be coordinated, managed and documented helps ensure effective and efficient response.

6.2 Continuation

Ensure that all time-sensitive critical services or products are continuously delivered or not disrupted for longer than is permissible.

6.3 Recovery and Restoration

The goal of recovery and restoration operations is to, recover the facility or operation and maintain critical service or product delivery. Recovery and restoration include:

- Re-deploying personnel
- Deciding whether to repair the facility, relocate to an alternate site or build a new facility
- Acquiring the additional resources necessary for restoring business operations
- Re-establishing normal operations
- Resuming operations at pre-disruption levels

7. Glossary of Terms

Base – All primary logistics and administration functions are coordinated/administered and is established/managed by the Logistics Section (only one base per incident).

Branch – Used when the number of Division or Groups exceeds the span of control. Can be either geographical or functional and can be activated for any Section.

Camp – Temporary locations within the general incident area that have equipment and are staffed to provide sleeping, food, water and sanitary services to incident personnel.

Chain of Command – Orderly line of authority within the ranks of an ICS organization.

Check-In – Officially logs incident personnel and provides important basic information.

Command – The act of direct ordering or controlling by virtue of explicit statutory, regulatory ordelegated authority.

Communications Specialist – Provide active radio information from a scene to an ambulance dispatch ora hospital emergency radio and is part of the Operations Section.

Communications Unit – Provide effective communications planning including acquiring, setting up, maintaining and accounting for communications equipment and supervises the incident communication centre.

Compensation/Claims Unit – Responsible for financial concerns resulting from property damage,injuries or fatalities at the incident.

Comprehensive Resource Management – An accurate and up-to-date picture of resource use.

Cost Unit – Responsible for tracking costs, analyzing cost data, making estimates and recommendingcost saving measures.

Demobilization Unit – Ensures orderly, safe and efficient demob of resources through demob release priorities and procedures.

Deputy – Assumes responsibility for a specific portion of a primary position.

Director – In charge of the Branch.

Division – Responsible for operations within a defined geographical area.

Documentation Unit – Collects, records and safeguards all documents relevant to the incident including providing duplication services and maintaining/archiving documentation.

Doers – Is the Operations Section and first to be set up. Directs all tactical operations and expands from the bottom up.

EOC – Emergency Operations Centre is a multi-agency/site/service coordination entity that provides support and coordination to the on-scene responders.

Facilities Unit – Sets up, maintains and demobilizes all facilities used in support of incident operationsand provides maintenance and security services.

Finance/Administration Section Chief – Monitors contracts, tracks personnel and equipment time,insurance claims and procurement.

Food Unit – Determine food and water requirements, plan menus, order food, provide cooking facilities, cooks, servers, maintains food service areas and manages food security/safety concerns for incident personnel (*Food needs for people affected by the incident are handled by Operations).

Getters – Provide food, water and medical for responders and arrange communication equipment, computers and transportation.

IAP – **Incident Action Plan** – Verbal or written plan containing general objectives reflecting the overall strategy for managing an incident.

IC – Incident Commander provides overall leadership for the management of an incident or event (is usually the Senior Person but in some situations, a lower ranking but more qualified person may be designated).

ICS – Incident Command System is a control structure that enables organizations to respond to any incident, regardless of cause, size, location or complexity.

Incident – An occurrence, either caused by humans or natural phenomena, that requires a response to present or minimize loss of life or damage to property and/or the environment (e.g. traffic accident, flood, medical emergency or hazardous materials release).

Incident Command Post – Location from which primary command functions are performed and where the IC is located.

ITP - Incident Transportation Plans

Integrated Communications – Common communication plan.

Ground Support Unit – Provides all ground transportation during an incident and is responsible for maintaining and supplying vehicles.

Group – Established to divide the incident management structure into functional areas of operation.

Logistics Section Chief – Provides resources and services required to support incident activities and developing logistics.

Management by Objectives – Is an approach used to communicate functional actions through the entire ICS organization.

Medical Unit – Effective and efficient provision of medical services to incident personnel.

Modular Organization – Is adaptable and can shrink or grow to address the needs of the incident.

Operations Chief - Responsible for developing and implementing strategy and tactics to accomplish the incident objectives.

Payers – Responsible for contract negotiation, recording personnel/equipment time, documenting and processing insurance claims and tallying costs.

Planners – Prepare and disseminate the IAP, track status of incident resources, ensure responders have accurate information and provide resources (e.g. maps/floor plans).

Planning Section Chief – Oversees the collection, evaluation and dissemination of operationalinformation

and ensures plans comply with the IAP.

Procurement Unit – Responsible for financial matters concerning vendor contracts, leases and fiscal agreements.

Responders – Incident personnel.

Resource Unit – Responsible for all check-ins and tracking the status of all resources and plays a significant role in preparing the written IAP.

Security Officer - Works with the Coordinator to ensure that all aspects of the BCP meet the security requirements of the organization and ensures the protection of the location and people within the CRHC office building and managed properties.

Section Chief – Assigned to Sections and reports directly to the IC.

Single Command – Defined as one person who holds a position.

Single Resource – An individual, a piece of equipment and its personnel complement, or a crew or team of individuals with an identified supervisor that can be used at an incident.

Situation Unit – Collects, organizes and analyzes incident status information as it progresses.

Span of Control – Number of individuals or resources that one Supervisor can manage effectively during emergency response incidents.

Staging Area – A temporary location at an incident where personnel and/or equipment are kept while awaiting tactical assignments.

Staging Area Manager – Supervises Staging Area and reports to the Operations Section Chief (should be located close enough to incident for a timely response but far enough away to be out of the immediate impact zone).

Strike Team – A set number of resources of the same kind and type with common communications.

Strike Team Leader – Supervises the Strike Team.

Supervisor – The person in charge of each Division or Group.

Supply Unit – Services non-expendable equipment, places all resource orders and maintains aninventory of supplies/equipment.

Task Force – A combination of mixed resources with common communications.

Technical Specialist – May be required to provide specialized expertise (e.g. Enviro Health Officer when a contaminant has been released).

Time Unit – Responsible for recording time for incident personnel and hired equipment.

Transfer of Command – The process of moving the responsibility for incident command from one IC to another.

Unified Command – An ICS application may have a single IC or multiple IC's (for larger incidents or

events) working together as a single entity in setting objectives and organizing the response.

Unity of Command – Each individual reports only to one other person.

8. Appendix A – Project Roles and Responsibilities

The following are the roles and responsibilities of project team members and the reporting relationships between those team members, as identified in the Governance table.

Steering Committee

The Steering Committee oversees strategic matters for all phases of the project using the following Terms of Reference:

- Provides strategic advice and recommendations at project initiation and planning on:
    - The content of the Final Project Charter, e.g., Scope, Schedule, Budget, Risks and Contingency plans, Project Structure, Project Staffing, Communications and OCM plans, etc.
    - Regular Reporting
    - Stakeholder Communications
    - Organizational Change Management (e.g., business process mapping and reengineering, stakeholder readiness, training, etc.).
    - Benefits realization and measurement (as appropriate to the project)
    - Ongoing post-project maintenance and support of the solution
- Monitors project execution and provides input and recommendations on:
    - Significant changes to plans for any of the project components listed above.
    - Significant risks and issues that have been escalated. The Steering Committee focuses on issues and risks impacting Stakeholders.
    - Advancement of the project to its subsequent phases.
- Provides strategic advice for the ongoing post-project maintenance of the solution, including the assignment of necessary staff resources.

Membership

Name	Title	Representing Areas
MD	CEO - Executive Sponsor	CRHCC
Executive Asst.	BCP Coordinator	CRHCC
CIO	CIO – Information Systems Unit	CRHCC
CFO	CFO - Corporate Services Unit	CRHCC
COO	COO – Operations Unit	CRHCC
Sr. Comm Adv.	Sr. Communications Advisor – Corporate Communications	CRHCC
Head – Corp Planning & Strategy	Head – Corp Planning & Strategy	CRHCC

BCP Coordinator

The BCP Coordinator, accountable to the Executive Sponsor, works with Unit Leaders and external stakeholder(s) to manage all activities of the project. The BCP Coordinator:

- Conducts and manages the **overall activities** of the project, within the approved plans and budget.
- Plans, schedules and assign project **resources** as required.
- Ensures **activities** are coordinated across the project teams.
- Initiate **corrective action** for deviations in the approved plans.
- Drives project to meet **milestone & completion** dates.
- Guides analysis & processes.
- Controls scope of project to ensure on-time, on-budget delivery.
- Manages **day-to-day** tasks & issues, budgets and risks.
- Ensures an appropriate level of **documentation** is developed and maintained.
- Consolidates **progress updates** from the Project Teams and prepares overall project status report for the Project Steering Committee.
- Meets with the Executive Sponsor and Leadership Team to present the project **status reports** and addresses **specific issues** as required.

Membership

Name	Title	Representing Areas
Executive Asst.	Executive Assistant	CRHC

Information Systems (IT) Unit

The IT Unit, reporting to the BCP Coordinator, plans and delivers the technical environment for the system and the project team. The Technical Team:

- Coordinates with the project team to ensure technical requirements are met, e.g. desktop/lap top requirements, network access, remote access, access control, etc.
- Procures hardware and software if required.
- Ensure system is configured for CRHCC and available.
- Ensures Testing and Training environments are available.
- Prepare for go-live activities.
- Documents major issues requiring decisions for submission to the Project Manager.
- Provides post go-live warranty service for any break/fix and issues resolution.

Membership

Name	Title/Role	Representing Area
CIO	Chief Information Officer	Information Systems

Manager IT	Manager, Information Systems	Networks, Servers, Rest of the Infrastructure

HR, Finance and Procurement Unit

The HR, Finance and Procurement Unit provide all-related Staffing and Finance for the project, including:

- Identify an alternative staffing plan to allow for operations when greater than 25% of the unit's staffing is unable to work for more than 72 hours, including a list of staff who can be cross-trained to perform essential functions, a line of succession, managerial and essential contacts, and a full department staff contact list.

Membership

Name	Title/Role	Representing Area
CFO	Chief Financial Officer	HR, Finance, Procurement
Director, HR	Director, Human Resources	Human Resources
Director, Finance	Director, Financial Services	Finance & Accounting

Operations Unit

Responsible for all aspects of property operations, including overseeing property management, tenant relations, capital maintenance programs, business development, business planning, and strategic priorities outlined by the CEO and Board.

Membership

Name	Title/Role	Representing Areas
COO	Chief Operating Officer	Operations
Director, Customer Ser	Director, Customer Services	Customer Services

Corporate Communications Unit

The Corporate Communications Unit plays an operational role by communicating with staff, board, government, media and any other outside stakeholders regarding facility closings, supply limitations or any other change in typical business operations including:

- Identify primary, secondary and alternate forms of communications
- Addresses the necessary information needs of employees, tenants and their families and the Command Centre as it may be activated.
- A plan to promote personal preparedness for staff, tenants and families.

Membership

Name	Title/Role	Representing Areas
Sr. Comms Advisor	Senior Communications Advisor	Corporate Communications

Working Committee

The fundamental task in business impact analysis (BIA) is understanding which processes in your business are vital to ongoing operations and to understand the impact the disruption of these processeswould have on your business.

The Working Committee determines which processes are critical to the Organization's ongoing success, and understanding the impact of a disruption to those processes (business impact analysis - BIA):

- Obtain an understanding of the organization's most critical services, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.
- Analyze and provide the resource information from which an appropriate recovery strategy can be determined/recommended.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

Membership

Name	Title	Representing Areas
Executive Assistant	BCP Coordinator	Overall
CIO	Chief Information Officer	Information Systems
Manager IT	Manager, Information Systems	Networks, Servers, Rest of the Infrastructure
Director, Policy & Research	Director, Policy, Research & Education	Policy, Research & Education
CFO	Chief Financial Officer	HR, Finance, Procurement
Director, HR	Director, Human Resources	Human Resources
Director, Finance	Director, Financial Services	Finance & Accounting
COO	Chief Operating Officer	Operations
Director, Customer Services	Director, Customer Services	Customer Services
Sr. Comms Advisor	Senior Communications Advisor	Corporate Communications

Emergency Response Plan

In the event of the following situations these protocols shall be followed by all Star Housing Finance Limited Staff.

Situation Description:

1. Any form of electronic communication received directly or indirectly to the CRHC office by anyone threatening to cause or which can potentially cause any form of physical harm to anyone in the building.
2. Letter type mail received directly or indirectly by CRHC office from anyone threatening to cause or which can potentially cause any form of physical harm to anyone in the building.
3. Verbal statement received directly or indirectly from anyone threatening to cause or which can potentially cause any form of physical harm to anyone in the building.
4. Anyone stating that they have a firearm or any type of weapon, displaying a firearm or any type of weapon, or any other object that can / is used as a weapon which can potentially cause any form of physical harm to anyone in the building.
5. Suspicious package; some of the factors that may cause an item to be suspicious are:
    a. Item contents cannot be readily identified and left unattended in one place for a period of time. For example: a backpack, duffle bag, box, large style envelope or briefcase.
    b. Item left by itself with no apparent owner.
    c. Item appears to be leaking, sweating, omitting a mechanical sound or giving off an odour.

The following procedure shall be utilized for the following situations as noted:

1. *Any form of electronic communication received directly or indirectly to the CRHC office by anyone threatening to cause or which can potentially cause any form of physical harm to anyone in the building.*

2. *Letter type mail received directly or indirectly by CRHC office from anyone threatening to cause orwhich can potentially cause any form of physical harm to anyone in the building.*

- Remain calm and advise your direct manager immediately or in the case of their absence any other manager as well as the Security Manager
- Do not erase/delete/discard the message
- If it is in the form of a handwritten letter/typed letter other than received in electronic format do not continue to handle/touch the letter. Secure the letter from further contamination. (**Fingerprints may be obtainable by police**)
- The manager will secure the letter without excessive handling and after determining the threat potential decide whether the police need to be notified as well as senior management.

- If it is determined that there is a threat potential that is present the office should proceed into lockdown mode where all clients are asked to exit, and all exterior doors are locked and remain secure until police arrival on scene.
- Staff will be notified by a management or designate to remain at their workstations depending upon the situation and subsequent lock down procedure.
- Once police have arrived to investigate the incident the CEO or designate will decide whether the office will remain open to the public.

The following procedure shall be utilized for the following situations as noted:

3. *Verbal statement received directly or indirectly from anyone threatening to cause or which can potentially cause any form of physical harm to anyone in the building.*

4. *Anyone stating that they have a firearm or any type of weapon, displaying a firearm or any type of weapon, or any other object that can / is used as a weapon which can potentially cause any form of physical harm to anyone in the building.*

- Staff should remain calm without doing anything that could potentially escalate the situation.
- Security may be involved to de-escalate the situation and interact with the individual.
- The Manager of the area where the incident has occurred as well as the Security Manager should be notified at this time when it is safe to do so.
- Police will be notified via a 100 call by either the Manager or staff member.
- The manager will confirm the validity of the situation by cautiously responding to the immediate area to observe the potential threatening situation without becoming directly involved in the situation unless it is absolutely necessary.
- Upon confirmation that the situation is of a threatening nature as described in #3 and/or #4 the above mentioned steps shall be taken.

Be prepared to give as much detail of the event and description of the individual/s and circumstanceswhen notifying police dispatch.

Note: Under no circumstances should other staff venture to the area of the potential threat or wander about the building unless given specific instructions by a Manager or designate.

The following procedure shall be utilized for the following situation as noted:

5. *Suspicious package; some of the factors that may cause an item to be suspicious are:*

a. Item contents cannot be readily identified and left unattended in one place for a period of time. For example: a backpack, duffle bag, box, large style envelope or briefcase.
b. Item left by itself with no apparent owner.
c. Item appears to be leaking, sweating, omitting a mechanical sound or giving off an odor. Note: Suspicious package/s are never to be touched, kicked, prodded or moved by any staff member.

If the item is observed anywhere within the interior of the office public or "staff only" area and/or immediate interior or exterior parking area on the building property staff should notify their Manager as well as security regarding the suspicious item.

- Be able to provide its description, location, approximate time that it has been at the location and any other pertinent information regarding any individual associated with the item.
- The Security Manager will be notified about the item so that CCTV footage can be viewed to provide more information regarding the circumstances of the item.
- If the item is deemed to be suspicious the immediate area surrounding the item will be cleared of any persons.

The police will be notified by Management to respond and investigate.

Announcing Emergency Code

When a violent incident or threat is reported, the Manager needs to obtain as much detail about the incident or threat from the initial observer/s or by their own observations.

The priority is to confirm that an incident is occurring or has occurred, if anyone has been hurt/injured or may be hurt/injured and activate the Lockdown ERP which will initiate the Shelter in Place procedure then be able to contact and direct police quickly to the correct location.

After confirming that a violent incident is in progress or has occurred the manager will immediately initiate Lockdown / Shelter in Place by communicating the **Emergency Code.**

Note: This **Emergency Code** may be a simple inconspicuous phrase that all staff is aware of and is communicated by person/s designated to do so. An example of one is "Tango Tango Front Lobby" This phrase will advise all staff there is presently an incident involving a threat as described in #3 and/or #4 occurring or has just occurred and the area where the incident has occurred.

Either the staff member or Manager shall activate the **Emergency Code and call 100 as quickly as possible when it is safe to do so.** A call to 100 will initiate assistance from police services, as well as fireand ambulance services.

Lockdown Procedure

When staff become aware that the emergency code has been activated, they are to follow the Lockdown Emergency Response Plan immediately:

1. Staff members will go directly to a **safe location** and advise anyone who is not CRHC staff who are at the time within the secure "staff only" area of the building to a **safe location** such as:
    a. A designated **shelter in place** location within the building on the floor they are presently on.
    b. The **nearest exit** only if it does not put them in close proximity to the incident by doing so.

Shelter in place

Has a deadbolt lock which can be easily engaged (if the door does not lock properly, or there is nosystem to prevent entry, it will not be designated as a safe area)

Has blinds on any window to prevent anyone from viewing into the room from within the building interior.

2. The staff member(s) must remain at this secure location and **remain as quiet as possible**. Thevolume on cellular phones should be turned down and phone ringer turned off.

3. Staff members will assess whether anyone is injured and the severity of the injuries and takeappropriate measures to **assist the injured without jeopardizing their own safety** or that of others.

4. Curtains or blinds will be pulled, and the lights turned off. **Move away from doors and windows.** If possible, furniture and chairs can be placed to further barricade the door and window from the inside. In consideration of sight lines into the room, individuals are usually safest when positioned away from the entrance to the room. Everyone must remain quiet and follow staff or police instructions. The room should appear quiet and empty to anyone from the outside.

5. If **gunshots** are heard, **everyone should lie on the floor** if able to safely do so within the shelterin place room.

6. **Cell phones** are **NOT** to be used by the staff, residents or visitors unless communicating vitalemergency information. A ringing cell phone may alert an intruder to a particular location.

7. Staff, residents and individuals are to stay in lockdown until given the All Clear by managementor emergency services personnel. **(Use of a specific code word to indicate "All Clear")**