COAST INVESTMENT & DEVELOPMENT CO. K.S.C.P

شــركة الساحـــل للتــنميـة والاســتثمار ش.م.ك.ع

Since 1975 منذ

COAST INVESTMENT & DEVELOPMENT COMPANY K.S.C.P

Business Continuity Plan Policies and Procedures

	BUSINESS CONTINUITY PLAN POLICIES AND PROCEDURES	ISSUE DATE: FEBRUARY 2012
COAST INVESTMENT & DEVELOPMENT CO. K.S.C.P Since 1975		VERSION:
		APPROVED BY:

TABLE OF CONTENTS

1. Introduction

The following is a Coast disaster recovery plan. Please note that this plan is provided to generate ideas only on the creation of an organization's plan. It is not intended to be a complete work. Plans can be developed using many different formats this represents just one. Additionally, not every recovery function is represented and not every plan component is presented.

1.1 Policy Statement

It is the Policy of Coast Investment and Development Company ("Coast") to maintain a comprehensive Business Continuity Plan for all critical organization functions. Each department head is responsible for ensuring compliance with this policy and that their respective plan component is tested no less than annually. Coast's Disaster Recovery efforts exercise reasonable measures to protect employees, safeguard assets, and client accounts.

1.2 Introduction

This document is the Business Continuity Plan for Coast located at Sharq, Al Shuhada Street Area 1, Kuwait. It has been developed in compliance with the Ministry of Interior, Kuwait Fire Service Directorate Prevention Sector.

This plan was specifically designed to guide the Company through a recovery effort of specifically identified organization functions. At the onset of an emergency condition, Coast employees and resources will respond quickly to any condition, which could impact Coast's ability to perform its critical organization functions. The procedures contained within have been designed to provide clear, concise and essential directions to recover from varying degrees of organization interruptions and disasters. For this task KD 50,000/- reserved budget will be allocated.

1.3 Confidentiality Statement

This manual is classified as the confidential property of Coast. Due to the sensitive nature of the information contained herein, this manual is available only to those persons who have been designated as plan participants, assigned membership to one of the Coast recovery teams, or who otherwise play a direct role in the recovery process. This manual remains the property of Coast and may be repossessed at any time. Unauthorized use or duplication of this manual is strictly prohibited and may result in disciplinary action and/or civil prosecution.

1.4 Manual Distribution

Each plan recipient will receive and maintain a soft copy of the disaster recovery manual; one copy will be kept in the plan recipient's work area; the second copy will be kept at the plan recipient's residence or cloud storage. Each manual has a control number to track its distribution. The additional copies may be obtained from Coast's Disaster Recovery Manager/Compliance group. Backup copies of all recovery documentation are maintained in safety locker at Coast premises as well as in the cloud storage.

1.5 Manual Reclamation

Plan recipients who cease to be an active member of a disaster recovery team or an employee of **Coast** must surrender both copies of their disaster recovery manual to the Disaster Recovery Manager. **Coast** reserves all rights to pursue the return of these manuals.

1.6 Responsibility

1.6.1 The Board of Directors (BOD) bears the responsibility of establishing and endorsing the comprehensive framework of the Business Continuity Plan (BCP). This framework provides clear directives for the implementation of effective emergency response and business continuity measures, in strict adherence to the policies and procedures delineated within the manual.

1.6.2 The respective heads of departments are entrusted with the responsibility of executing the prescribed policies and procedures meticulously. Their actions are to be aligned with the overarching objectives and strategies established by the Board of Directors.

1.6.3 The Risk Management Unit assumes an active role in providing oversight and support to the departmental heads in the implementation of the BCP. This includes conducting thorough risk assessments aimed at identifying potential threats and vulnerabilities to the organization.

1.7 Plan Revision Date

The latest manual revision date appears in the Appendix 2 - Revision Manual. This date indicates the most published date of the manual.

1.8 Defined Scenario

A disaster is defined as a disruption of normal organization functions where the expected time for returning to normalcy would seriously impact Coast's ability to maintain customer commitments and regulatory compliance. Coast's recovery and restoration program is designed to support a recovery effort where Coast would not have access to its facilities and data at the onset of the emergency condition.

1.9 Recovery Objectives

The Business Continuity Plan was written with the following objectives:

- To ensure the safety and wellbeing of all Coast employees during the emergency situations, disaster declaration, and throughout the recovery process.

- To re-establish the essential organization related services provided by Coast within their required recovery window as identified in the recovery portfolio in Section 2 at the declaration of disaster.

- To suspend all non-essential activities until normal and full organization functions have been restored.

- To mitigate the impact to Coast's customers through the rapid implementation of effective recovery strategies as defined herein.

- To reduce confusion and misinformation by providing a clearly defined command and control structure.

- To consider relocation of personnel and facilities as a recovery strategy of last resort.

1.10 Plan Exclusions

The Coast Business Continuity Plan was developed with the following exclusions:

- Succession of Management

- Restoration of the Primary Facilities

1.11 Plan Assumptions

Coast's Business Continuity Plan was developed under certain assumptions for the plan to address a broad spectrum of disaster scenarios. These assumptions are:

- Coast's recovery efforts are based on the premise that any resources required for the restoration of critical organization functions will reside outside of the primary facility.

- Any vital records required for recovery can be either retrieved or recreated from an off-site location and moved to the recovery facility within 24 hours.

1.12 Declaration Initiatives

Coast's decision process for implementing any of the three levels of recovery strategies to support the restoration of critical organization functions are based on the following declaration initiatives:

- Every reasonable effort has been made to provide critical services to Coast's customers by first attempting to restore the primary facility and / or operate using intra-day procedures.

- After all reasonable efforts have failed to restore the primary facility, and using manual procedures severely degrades client support, Coast would invoke a recovery strategy that requires the relocation of personnel and resources to an alternate recovery facility.

- If the outage will clearly extend past the acceptable period identified in the Recovery Portfolio, (Section 2) a declaration of disaster will immediately be made.

1.13 Recovery Strategies

1.13.1 In order to facilitate recovery regardless of the type or duration of disaster, Coast has implemented multiple recovery strategies. These strategies are categorized into three (3) levels. Each level is designed to provide an effective recovery solution equally matched to the duration of the emergency condition.
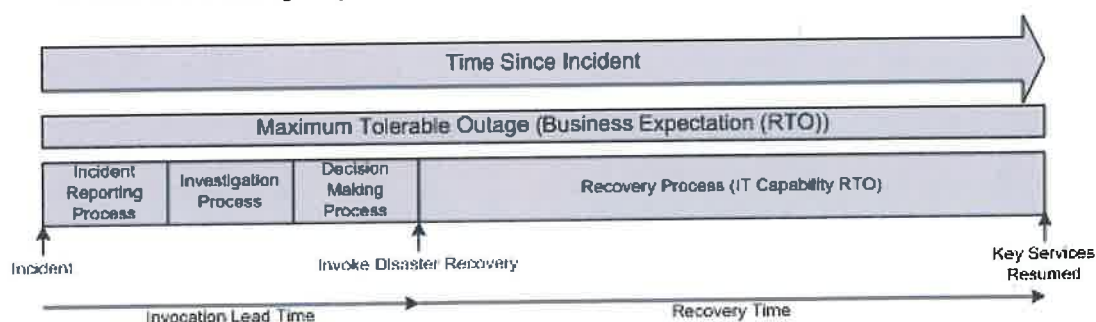
- **LEVEL 1: SHORT-TERM OUTAGE (RIDE-OUT) – INTRA-DAY**

  A short-term outage is defined as the period Coast does not require computerized operations, or where an outage window of the same day or less would not allow adequate time to restore / utilize automated recovery operations.

- **LEVEL 2: MEDIUM-TERM OUTAGE (TEMPORARY) – UPTO SIX WEEKS**

  A medium-term outage is defined as the period that Coast will execute its formal disaster recovery strategy, which includes declaring a disaster. A disaster may either be declared companywide or only for the effected department or building. The decision to declare a disaster will be based on the amount of time / expense

that is required to implement the formal recovery and the anticipated impact to Coast's organization over this period.

- **LEVEL 3: LONG-TERM OUTAGE (RELOCATION) – 6 WEEKS OR MORE**

A long-term outage is defined, as the period of time that Coast will exceed the allowed occupancy time of its primary recovery strategy. During this phase of recovery Coast will initiate a physical move of personnel and resources.
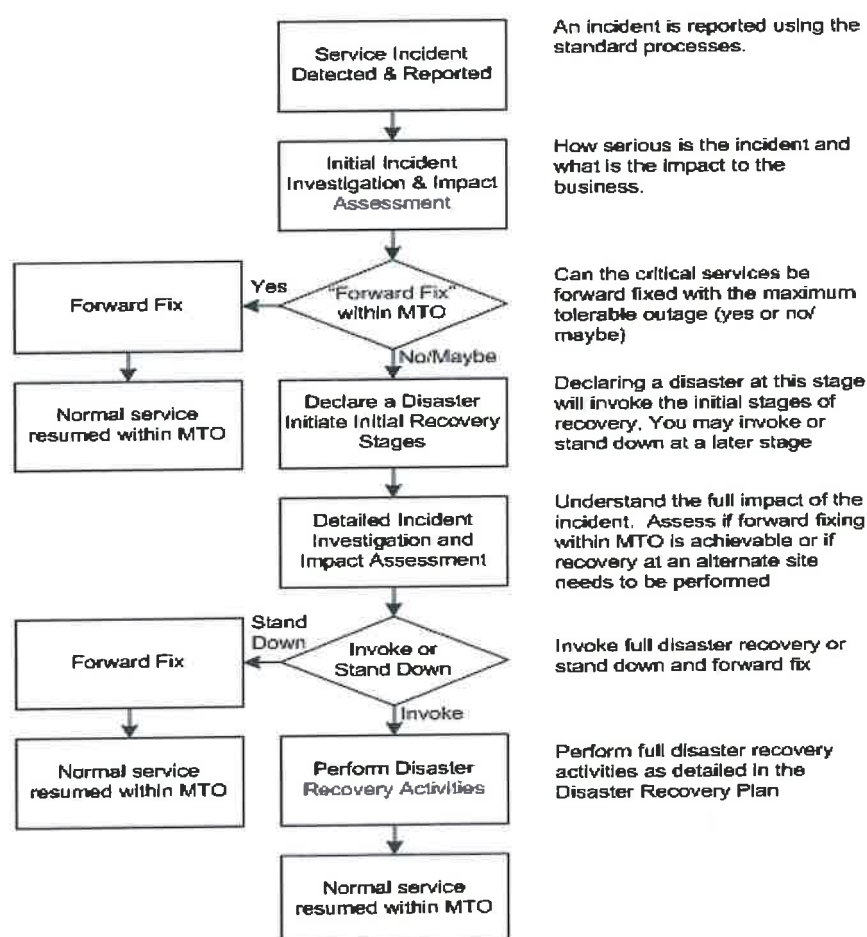
1.13.2 The proper records relating to arrangements of business continuity shall be maintained for minimum 5 years after discontinuity of using or updating thereof ".

1.14 Team Overview

During an emergency each team member contributes the skills that they use in their everyday work to the overall response.

1.15 Team Charters

Crisis Management Team - The CMT is comprised of senior Coast management and is responsible for authorizing declarations of disaster, emergency investment strategy, approving public release of information, and ensuring volunteers and assignees and constituents are informed.
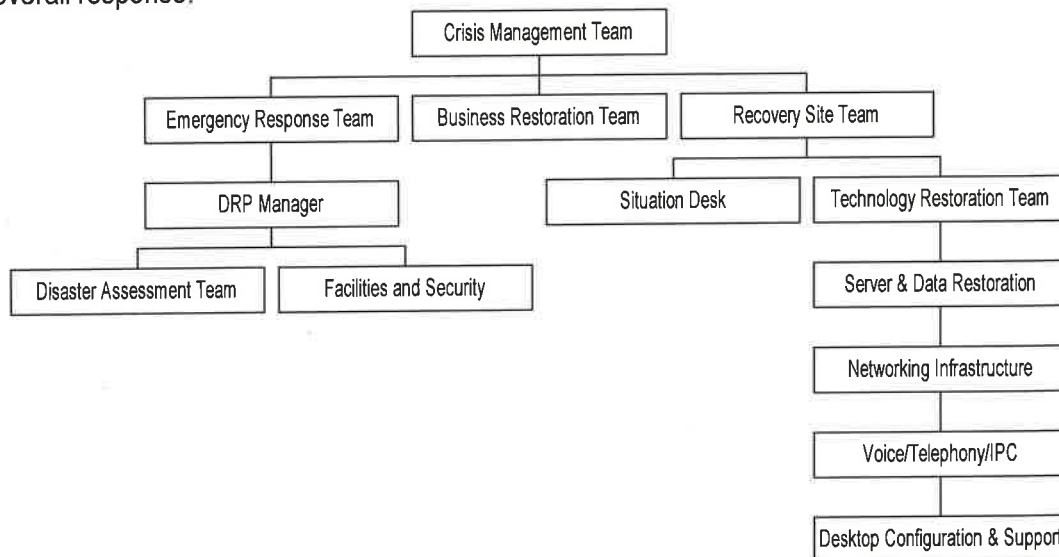
1. Chief Executive Officer
2. Senior Vice President - Support
3. Asst. IT Manager

Emergency Response Team - The ERT is first on scene to assess the damage caused by the disaster or ensure precautionary measures are taken in light of any imminent disaster (e.g. inclement weather, etc.) Once the ERT determines the extent of the disaster, they will either order an evacuation of the facility or work with facilities to mitigate the effects to Coast.

1. Senior Vice President - Support
2. Asst. IT Manager

Recovery Site Team - The RST provides enterprise-level support for both the physical site and technology issues. The members of this team will ensure that the alternate site is ready, and adequate for arriving recovery personnel. The RST will be the first at a meeting point or alternate site in order to register arriving personnel.

1. Asst. IT Manager
3. Vendor or Application Provider - External Party

Business Restoration Team – The BRT'S consist of personnel from each Coast area deemed critical to the continuation of business. The head of the BRT gets updated status from the ERT and the RST to pass on to their team members to ensure prompt recovery of each department.

1. User Department Head
2. User Department 2nd In charge

2. Recovery Strategies

The following are the identified recovery strategies for the organization:

Recovery Area:	Primary Strategy:	Backup Strategy:
Office Space	Mobilization Time: (1 Day)	Mobilization Time: (4 Days)
Phone System	Mobilization Time: (2 Days)	Mobilization Time: (3 Days)
Network Recovery	Mobilization Time: (1 Day)	Mobilization Time: (3 Days)
Server Recovery	Mobilization Time: (1 Day)	Mobilization Time: (3 Days)
Desktop Recovery	Mobilization Time: (1 Day)	Mobilization Time: (4 Days)
Office Furniture	Mobilization Time: (1 Day)	Mobilization Time: (4 Days)

Recovery Area:	Primary Strategy:	Backup Strategy:
Office Equipment	Mobilization Time: (1 Day)	**Mobilization Time: (3 Days)**
Applications	Mobilization Time: (1 Day)	**Mobilization Time: (3 Days)**
Databases	Mobilization Time: (1 Day)	**Mobilization Time: (3 Days)**
Service Providers	Mobilization Time: (1 Day)	**Mobilization Time: (3 Days)**
Employees	**Mobilization Time: (1 Day)**	**Mobilization Time: (7 Days)**

2.1 Emergency Phone Numbers

Complete the following to ensure that you have identified all the contact numbers in case of emergency

Emergency services

1. Police: 112

2. Fire: 112

3. Ambulance: 112

4. Alarm Company: (+965) 24317028 - Universal Project Co.

Communications

1. Local Telco: (+965) 22410000

Weather information

1. Radio station: AM KUNA 120

2. Weather channel: https://www.weather.com
                        https://www.met.gov.kw/forecasts/kuwait.php

Maintenance & repair

1. HVAC: (+965) 1802255 - Gulf Engineering Company

2. Electrical: (+965) 66118442

3. Carpentry: (+965) 66932246

4. Plumbing: (+965) 97810983

Logistics

1. Travel agent: (+965) 22424115/6 Barakat Travels

2. Express shipping: (+965) 1820011 - ARAMEX

3. Taxi service: (+965) 66237417

Utilities

1. Electrical: (+965) 24847329

2. Water: (+965) 24847329

Employee assistance

1. Childcare: (+965) 22450005 Al- Ameri Hospital

2. Elderly care: (+965) 22450005 Al- Ameri Hospital

	ISSUE DATE: FEBRUARY 2012
BUSINESS CONTINUITY PLAN POLICIES AND PROCEDURES	**VERSION:**
	APPROVED BY:

COAST INVESTMENT & DEVELOPMENT CO. K.S.C.P
Since 1975

2.3 Threat Profile

2.3.1 Hazard: Freezing Rain
Profile of Hazard:
Freezing rain is rain occurring when surface temperatures are below freezing. The moisture falls in liquid form, but freezes upon impact, resulting in a coating of ice glaze on exposed objects. This occurrence may be called an ice storm when a substantial glaze layer accumulates. Ice forming on exposed objects generally ranges from a thin glaze to coatings about an inch thick. A heavy accumulation of ice, especially when accompanied by high winds, devastates trees and transmission lines. Sidewalks, streets and highways become extremely hazardous to pedestrians and motorists. During the winter citizens should be prepared to shelter themselves at home for several days, possibly without power. Local shelters can be opened in areas where power is not affected but transportation to a shelter may be difficult.
Response:
Step 1: Monitor weather advisories
Step 2: Notify on-site employees.
Step 3: Call local radio and TV stations to broadcast weather closing information for employees at home.
Step 4: Place closing sign on all Coast doors.
Step 5: Arrange for snow and ice removal.

2.3.2 Hazard: Tornadoes
Profile of Hazard: Tornadoes are violent rotating columns of air, which descend from severe thunderstorm cloud systems. They are normally short-lived local storms containing high-speed winds usually rotating in a counterclockwise direction. These are often observable as a funnel-shaped appendage to a thunderstorm cloud. The funnel is initially composed to nothing more than condensed water vapour. It usually picks up dust and debris, which eventually darkens the entire funnel. A tornado can cause damage even though the funnel does not appear to touch the ground.
Response:
Step 1: Monitor weather conditions
Step 2: Notify employees of potential of severe weather
Step 3: Power off equipment
Step 4: Shut off utilities (power and gas)
Step 5: Instruct employees to assume protective posture.
Step 6: Assess damage once storm passes.
Step 7: Assist affected employees

2.3.3 Hazard: Floods

Profile of Hazard:

In several areas of Coast Co., unusually heavy rains may cause "flash" floods. Small creeks, gullies, dry streambeds, ravines, culverts or even low lying round frequently flood quickly. In such situations, people are endangered before any warning can be given.

Response:

Step 1: Monitor flood advisories

Step 2: Determine flood potential to Coast

Step 3: Determine employees at risk

Step 4: Pre-stage emergency power generating equipment

Step 5: Assess damage

2.3.4 Hazard: Hurricanes

Profile of Hazard:

Coast's Co. is considered as coastal area and also hurricanes do affect our area.

Response:

Step 1: Power-off all equipment

Step 2: Listen to Hurricane advisories

Step 3: Evacuate area, if flooding is possible

Step 4: Check gas, water and electrical lines for damage

Step 5: Do not use telephones, in the event of severe lightning.

2.3.5 Hazard: Earthquakes

Profile of Hazard:

An earthquake is the shaking, or trembling, of the earth's crust, caused by underground volcanic forces of breaking and shifting rock beneath the earth's surface.

Response:

Step 1: Shut off utilities

Step 2: Evacuate building if necessary

Step 3: Account for all personnel

Step 4: Determine impact of organization disruption

2.3.6 Hazard: Power Failures

Profile of Hazard:

Power failures occur in many parts of the Co. throughout the year. They can be caused   by winter storms, lightning or construction equipment digging in the wrong location.

For whatever the reason, power outages in a major metropolitan area can severely impact the entire community.

Response:

Step 1: Wait 5-10 minutes.

Step 2: Power-off all Servers after soft shut down procedure.

Step 3: Shut down the main circuit located on the bottom floor.

Step 4: Use emergency phone line to make outgoing phone calls.

Step 5: Call power company for assessment

Step 6: Locate sources of mobile power.
Step 7: Contact electrical company.
Step 8: Re-energize building.
Step 9: Power-on equipment

2.3.7 Hazard: Urban fires

Profile of Hazard:
In metropolitan areas, urban fires can, and do, cause hundreds of deaths each year and Coast's Co. is no exception. Even with strict building codes and exceptions, citizens still parish needlessly in fires.

Response:
Step 1: Attempt to suppress fire in early stages.
Step 2: Evacuate personnel on alarm, as necessary.
Step 3: Notify fire department.
Step 4: Shut off utilities.
Step 5: Account for all personnel
Step 6: Search for missing personnel
Step 7: Assess damage.

2.3.8 Hazard: Pandemic/Epidemic

Profile of Hazard:
Possible effects on business from a pandemic/epidemic can include reduced labor supply, including your regular workers or availability of contractors or temporary workers. Restrictions on travel (regional, national, or international) and movement of people from one area to other area Reduced availability of health care In more severe situations, disruptions in services such as telecommunications, financial/banking, water, electricity, gasoline/fuels, medicine, or the food supply.

Response:
Step 1: Identify critical processes, operations, and functions and identify key minimal resources to run the business. Also keep it ready the second line of resources as an
alternate. It can be from existing staff or outsourced.
Step 2: Identify key internal and external dependencies – those things, people, or other business you rely on.
Step 3: Identify what else can affect your business:
Location – Identify alternate location for operational use due to resource movement restrictions to company. If the pandemic situation is very long and location is not available for use more than 6 weeks. Move the data center to an alternate location.
Personnel – Identify and train backups for essential functions, including chain of command (management). Be sure you have consulted with staff, including any applicable union or collective agreements.
Equipment – Make sure the available equipment meets the identified needs.
Availability of assets – Make sure that facilities, utilities, computers, machinery, or tools also meet the company needs, availability of internet bandwidth for employees to work from home. (e.g., access to internal systems by staff working from home).

Business commitments – Research legal implications for level of service arrangements (e.g., for non-performance or late delivery).

Accounting – make sure you can continue your payroll, finances payment, accounting etc.

2.3.9 Hazard: Political Violence / Wars

Profile of Hazard:

Companies need to prepare for more political disturbances and Violence as well as war in coming period. A significant increase in the number of riots, demonstrations, and vandalism, as terrorism events decline, means civil unrest is now the main political risk exposure for companies, resulting in significant losses and insurance claims. Impact of political violence can cause business disruption beyond physical property damage. CIDCO which is headquartered in the State of Kuwait, does not have any chance of political violence scenarios but should be ready for facing any such incidents.

Response:

It is important for businesses to minimize presenting their facilities as a soft target for opportunistic criminal activity. Having a proactive plan in place to deter criminal activity will aid in protecting employees and assets.

Risk Assessment:

Local news and media coverage should be monitored to stay up to date on protests and any breaking events, trending social and/or racial injustice mentions and hashtags, or any protest announcements and/or updates.

Conduct a comprehensive assessment of geopolitical risks in the country of operation. Analyse historical data and current political climates to understand potential threats.

Scenario Planning:

Enable/ activate the essential services until the situation settles. Develop scenarios outlining various levels of political violence and conflicts. Assess potential impacts on infrastructure, staff, clients, and operations for each scenario.

Critical Function Identification:

Identify core functions critical to operations (e.g., transaction processing, accounting, client services) and readily available for use in work from home facility as prioritized in this manual.

Redundancy and Backup Systems:

Establish redundant systems and data backups at geographically distant locations. Ensure redundancy in communication channels and technology infrastructure. Make sure that all the data is backed up and shifted to alternative cloud-based services that are primarily and readily available for use in a work-from-home facility.

Employee Safety Protocols:

Develop and communicate safety protocols for employees in high-risk areas. Implement procedures for evacuation or relocation if necessary. Evacuate the employees and safeguard CIDCO company employees where we are facing a potential danger i.e. of a petrol bunk nearby, just 200 meters away. Transportation routes should be reviewed, and contingency plans made with alternative routes, particularly if the primary route travels through areas likely to encounter civil unrest. This is especially the case when moving people or assets. A formalized plan should include built-in redundancies for primary and alternate communication methods if various digital and cellular systems are disrupted.

Establish and maintain communication. Ensure there is an established communications plan that provides positive communication processes for use during critical incidents. This will facilitate effective emergency notifications and responses among employees, executives, and clients.

Supplier and Partner Assessment:
Evaluate the resilience of suppliers and partners to withstand geopolitical disruptions. Diversify suppliers or have alternate arrangements in place.

Regulatory Compliance and Contingencies:
Understand legal and regulatory requirements during times of crisis. Develop contingency plans to meet regulatory obligations in disrupted environments.

Communication and Crisis Management:
Establish clear communication channels internally and externally. Provide training staff on crisis communication protocols to maintain transparency and trust.

Testing and Training:
Regularly test the BCP through simulations and drills (if the need arises). Provide comprehensive update to employees on BCP procedures.

Adaptability and Flexibility:
Continuously review and update the BCP based on changing geopolitical situations. Remain flexible to adapt strategies and responses to evolving threats.

Insurance and Financial Preparedness:
Consider appropriate insurance coverage for political risks, violences and Wars. Maintain sufficient financial reserves to withstand disruptions. Assess damage, account and claim the damage with insurance agents.

Plan for recovery:
Make the necessary arrangements in advance for repair and recovery resources to clean up and restore damaged sites and bring them back to full operation quickly.

Government and Security Liaison:
Establish relationships with relevant government agencies and security forces and wait for the advisory. Stay informed about security updates and alerts in the areas of operation.

2.4 Recovery Strategy Overview

Coast's Business Continuity Recovery is based on the organization surviving the loss of facilities and/or key personnel and systems during a disaster. Once Coast's ERT has determined that a declaration of disaster is required, the following sequence of events will occur:

Steps:	Instruction:
1: Evacuate affected facility.	If the emergency requires an evacuation of employees, execute evacuation plans contained in the Emergency Procedures section.
2: Go to staging area.	Follow building evacuation instructions.
3: Determine length of outage.	Review written and verbal damage assessment reports from facilities and civil authorities and then estimate the amount of time the facility will be uninhabitable.
4: Select disaster level.	Based on the estimated duration of the outage, declare the disaster event as either a L1 (Less than 48hrs.), L2 (48hrs. to 6 weeks), or L3 (6 weeks or longer).
5: Activate alternate facilities.	Contact alternate facilities identified in the Facilities section. Confirm their availability and alert them of estimated arrival time.
6: Release personnel from the staging area.	Once the disaster level has been selected, release all personnel from the staging area to their assigned recovery location. • Non-essential personnel – Home • Recovery Site Team – Alternate Facility • End Users – Alternate Facility • Command Center Staff – Alternate Facility • Crisis Management Team – Alternate Facility
7: RST establish Command Centre.	RST personnel are the first to arrive at the alternate facility to setup and organize the command centre prior to the arrival of the CMT and support personnel. The following representatives are required at the Command Centre within 1-3 hours: • Crisis Management Team • Emergency Response Team Lead • Business Restoration Team Lead • Recovery Site Team Lead
8: Establish situation desk.	At the command center, establish a dedicated line with operator to field all incoming calls. Announce command center phone number to all recovery participants.
9: Review recovery matrix.	Review the Recovery Matrix Section on a department-by-department basis to determine who is most affected by the disaster. Group departments by recovery resource requirements, time frames, and co-location requirements.
10: Create technology shopping list.	Once the technology requirements of the effected department(s) are known, create a requirements list for the IT support staff.
11: Contact quick ship vendors.	Using the vendor quick-ship contacts or local sources located in the LAN Restoration section order replacement technology indicated on requirements list.
12: Retrieve electronic/hardcopy vital records,	Retrieve vital records from Iron Mountain or other locations as indicated in the Vital Records section. Have vital records shipped and staged at the alternate facility.
13: Setup replacement LAN.	The priority of Coast Server restoration to support all other Coast Business functions is: • Core technology • End-user servers
14: Activate short-term recovery strategies.	Instruct each department to initiate their short-term recovery strategies. These strategies will be used while the replacement LAN/WAN circuits are implemented.
15: Populate alternate facility.	Once the replacement LAN/WAN is functional, notify the BRT that departments can now begin executing their L2 recovery strategies.

2.5 Plan Participants

The following presents the Coast plan participants and their associated recovery function. At the time of a disaster, these individuals will be among the first to be contacted.

Team Members	Recovery Role
Name: Mr. Asaad Al-Banwan Title: **Chief Executive Officer** Office: +965 22230502 Cell: +965 99606060 Home: +965 E-mail: asaad.albanwan@coast.com.kw	**Crisis Management Team**
Name: Mr. Christy Kulathooran Title: **Senior Vice President** Office: +965 22230553 Cell: +965 97799159 Home: +965 24896405 E-mail: christy.kulathooran@coast.com.kw Email 2: christykulathooran@gmail.com	**Crisis Management Team** **Emergency Response Team**
Name: Mr. Suresh BS Title: **Asst. IT Manager** Office: +965 22230545 Cell: +965 97194693 Home: +965 25613942 E-mail: suresh.shetty@coast.com.kw Email 2: sureshabs@hotmail.com	**Crisis Management Team** **Emergency Response Team** **Recovery Site Team**
IT Staff/Vendor/Application Provider **(Available in each Task)**	**Recovery Site Team**
User Department Head/In charge **(Available in each Task)**	**Business Restoration Team**

Recovery Role:	Primary:	Alternate:
Network Recovery	Name: Mr. Suresh BS Title: Assistant IT Manager Office: +965 22230545 Cell: +965 97194693 Home: +965 25613942 E-mail: suresh.shetty@coast.com.kw Email 2: sureshabs@hotmail.com	Name: Burhan Tech Support Title: Outsourced Technicians Office: +965 22498923 Others: +965 22616127/28/29 E-mail: helpdesk @burhantec.com Email 2: techhelp@burhantec.com
Administrative Support (Purchasing)	Name: Mr. Christy Kulathooran Title: Senior Vice President - SG Office: +965 22230553 Cell: +965 97799159 Home: +965 24896405 E-mail: christy.kulathooran@coast.com.kw Email 2: christykulathooran@gmail.com	Name: Mr. Yaser Al-Aryan Title: Supervisor Accounting Office: +965 22230544 Cell: +965 99776682 Home: +965 25658927 E-mail: yaser.alaryan@coast.com.kw
Administrative Support (Premises)	Name: Mr. Christy Kulathooran Title: Senior Vice President-SG Office: +965 22230553 Cell: +965 97799159 Home: +965 24896405 E-mail: christy.kulathooran@coast.com.kw	Name: Mr. Noor Jamal Title: Admin Officer Office: +965 22230546 Cell: +965 60491700 Home: +965 0444783 E-mail: noor.jamal@coast.com.kw
Business Restoration Users Department Asset Management Group	Name: Mr. Jassem Al-Zaid Title: Senior Vice President – AMG Office: +965 22230400 Name: Christy Kulathooran Title: Senior Vice President – Support Office: +965 22230553 Cell: +965 97799159 E-mail: jassem.alzaid@coast.com.kw E-mail: christy.kulathooran@coast.com.kw	Name: Mr. Thampi Paul Title: Vice President - AMG Office: +965 22230538 Cell: +965 69994349 Home: +965 24349730 E-mail: thampi.paul@coast.com.kw
Recovery Role:	Primary:	Alternate:

Business Restoration Users Department Support Group	Name: Mr. Christy Kulathooran	Name: Mr. Ahmed Al-Huneidi
	Title: Senior Vice President - SG	Title: Manager - Finance & Accounts
	Office: +965 22230553	Office: +965 22230554
	Cell: +965 97799159	Cell: +965 66906006
	Home: +965 24896405	Home: +965
	E-mail: christy.kulathooran@coast.com.kw	E-mail: ahmed.elhuneidi@coast.com.kw

2.6 Alternate Site Setup

Once the alternate site has been secured, the RST's will work with the event staff to configure appropriate command enter and recovery space.

The following provides Coast configurations for general work areas and the command centre.

Recovery Area:	Configuration:
Command Center	- Occupancy – 15 - Room – private, 750-sq. ft. - Conference table - Phones – 15 - Facsimile – 2 - Office Equipment – copier, typewriter, PC, printer, folding tables - Office supplies – flip charts, stationary, writing supplies - Communications – Walkie-talkies, tape recorder, cellular phones
Work Area Recovery	- Occupancy – 50 - Room – 5000- sq. ft. - Folding Tables- each workstation needs to be 3ft apart - Phones – 50 - Facsimile – 3 - Office Equipment – copier, typewriter, tape recorder, 15 pre-configured laptops - Office supplies – flip charts, stationary, writing supplies - Communications – 3 fax lines, 10 modem lines, 50 voice lines
Mail Room	- Occupancy – 2 - Room – 250-sq.ft. - Phone – 1 - Office Equipment – scale, postage meter - Supplies – Mailing/shipping supplies
Vital Records Staging	- Occupancy – 2 - Room – private, 300 sq. ft. - Office Equipment – folding tables, metal racks

3. Recovery Ranking

The following organization processes will be recovered within the sequence specified below:

Priority Rank:	Organization Process:	Potential Impact:	Allowable Downtime:
1	Active Directory	All applications are working on access rights through active directory and mails are also integrated to active directory.	24 Hours
2	Mail Server	The company relies primarily of email service for its core business communications	1 Day
3	Portfolio Management System (BNIS)	This should be enabled immediately as daily client transactions must be updated and relevant information promptly communicated to clients	1 Day
4	Microsoft Dynamics - Great Plain	Company is using this application as core Finance & Accounting module	2 Days
5	HRMS and TAMS	Company is using this application for HR activities, Payroll process, Time and Attendance Module	3 Days
6	Asset Tracker	Company is using this application for Asset Tracking	3 Days
7	AML, CFT and CBK Blacklist Module	Company utilizes this application for AML, CFT and monitoring entities listed CMA and Central Bank of Kuwait	3 Days
8	KSE Market Analysis (BOURSA)	Company is using this application for MIS purpose	3 Days
9	Company Website	Company website is published on www.coast.com.kw	4 Days
10	Reuters Services, KSE Feeds and Internet	As these services are depending on external parties' decision must be made to change them	5 Days
11	VEEAM Agent (Back Up)	Utilized to ensure proper back up for all user data	6 Days

3.1 Risk Assessment and Business Impact Analysis

Scope:

The method of information security risk assessment applied throughout the Company in respect of business activities.

Responsibilities:

The IT Manager is primarily responsible for undertaking risk assessments wherever they are required by Coast Investment and Development Company and communicated with the Risk Management Unit as and when required.

Procedures:

Identify the risks

- The assets within the scope of each risk assessment are identified and listed in line with the business requirements of the organization.

- When new information assets are acquired, or existing assets in any way change, those assets are added to the inventory of the organization and are treated in line with the requirements below.

- Threats to each of those assets shall be identified [how is this done, and by whom?] under the headings of threats to availability, confidentiality and integrity and are documented [in the asset risk log].

- Vulnerabilities that might be exploited by each of these threats are identified [how, and by whom?] and documented with each risk assessment

- Where new vulnerabilities or weaknesses are identified, the risk log shall be updated and, where appropriate, the risk assessment procedure set out here shall be repeated and any changed controls implemented.

- The effect that losses of availability, confidentiality and integrity might have on the assets themselves [i.e., what is the actual harm to the asset itself that might occur?] are identified and documented [by whom and how?].

Assess the risks

- Impacts – the business harm - that might result from the loss of availability, confidentiality or integrity, for each of these assets, is assessed [how, by whom?]

- The realistic likelihood that each of these failures might occur is assessed [how, by whom?]

- The risk levels are assessed [how, by whom?]

- A decision is made, for each of the risks, as to whether it is acceptable or if it must be controlled in line with criteria established [by whom, how?].

Identify and evaluate options for the treatment of risks

- For each of the risks, identify [how and by whom?] the possible options for treating it in line with the decision made.

- For each of the risks, document which treatment action (accept, reject, transfer or control) is going to be taken [how and by whom?] and document in the [organisation name] risk treatment plan [how and by whom?] the reasons for each choice.

Select control objectives and controls for treatment of the risks.

- Appropriate control objectives should be adopted

- These control objectives and controls are then summarized into the organisation's information security management system.

The organization assets/processes will be maintained as per the table below:

No.	Step	Description	Output	Status	Notes
1	System Characterization	Define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system.	Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary		
2	Threat Identification	Identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.	A threat statement containing a list of threat-sources that could exploit system vulnerabilities		
3	Vulnerability Identification	Develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.	A list of the system vulnerabilities (observations) that could be exercised by the potential threat sources		
4	Control Analysis	Analyse the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.	List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event		
5	Likelihood Determination	An overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment,	Likelihood rating		
6	Impact Analysis	The adverse impact resulting from a successful threat exercise of a vulnerability.	Magnitude of impact (High, Medium, or Low)		
7	Risk Determination	the level of risk to the IT system.	Risk Level (High, Medium, or Low)		
8	Control Recommendations	Reduce the level of risk to the IT system and its data to an acceptable level.	Recommendation of control(s) and alternative solutions to mitigate risk		
9	Results Documentation	A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.	Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation		

3.2 Backup Procedures and Disaster Recovery Points

Coast has already established detailed backup procedures in functional document as follows.

Method 1

Important Servers replication is in SAN automatically.

Frequency: Hourly

Method 2

Users' backups are scheduled by using Servers and DLO Backup Tools and storing in Network Access Storage (NAS). 15 days backup can be restored at any point of time and in the same manner servers have disaster recovery solution to keep backup with recovery points are stored in the NAS and it is in different floor. All server's backup and DLO backups are moved to Azure Cloud Storage. These backups are remotely available for alternate stage to download.

Frequency: Daily

3.3 Detailed/Specialized Disaster Recovery Procedures as per ranking and level of outage

Disaster recovery procedure is one of the key elements of business continuity plan. Traditionally business continuity and disaster recovery (DR) planning have always been separated between the business and the information technology department.

Scenario I
- **LEVEL 1: SHORT-TERM OUTAGE (RIDE-OUT) – INTRA-DAY**
- **LEVEL 2: MEDIUM-TERM OUTAGE (TEMPORARY) – UPTO SIX WEEKS**

Maintain detailed recovery procedures in case of disaster affecting IT systems in case of all or individual system fails.

Scenario II

- **LEVEL 3: LONG-TERM OUTAGE (RELOCATION) – 6 WEEKS OR MORE**

Maintain detailed recovery procedure in case of disaster affecting and Coast location is not available for IT Staff.

Note: Detailed Recovery Plan is available in functional document

4. Recovery Team Checklists

Checklist for each recovery function:

Recovery Function:	Administration	Primary:	Company Premises
		Alternate:	KEMS Data Centre
Alternate Locations:	Primary Staging Area: Coast Investment and Dev. Co. Sharq, Al-Shuhada Street, Area 1 Kuwait City Kuwait		Alternate Staging Area: KEMS Data Centre Kuwait
	Primary Work Area: Coast Investment and Dev. Co. Sharq, Al-Shuhada Street, Area 1 Kuwait City Kuwait		Alternate Work Area: KEMS Data Centre Kuwait
Charter:	Responsible for all of the administrative aspects of the recovery effort. This includes maintaining the plan currency, activating the command centre and providing logistics and employee assistance support during the recovery effort.		
Retrieval List:	The following items should be removed from your work area if you are evacuated from the building: 1. Calling List and Vital Records 2. Servers, Desktops and Printers 3. Network Accessories 4. Applications media and license information 5. Disaster Recovery Plan 6. _____		
Recovery Resources:	In order to perform your recovery efforts, you will need access to the following resources: Phone: _____ PC: _____ Network _____ Internet _____ Fax _____		

Recovery Steps:	The following are the recovery tasks to be followed:
	1. Retrieve important items form work area
	2. Evacuate building
	3. Go to primary staging area
	4. Wait for all clear or activation notice
	5. Go to designated recovery location
	6. Execute calling tree
	7. Further details are available in functional document on task basis_____
	8. _____
	9. _____
	10. _____
	11. _____
	12. _____
	13. _____
	14. _____
	15. _____
	16. _____
	17. _____
	18. _____
	19. _____
	20. _____

Calling List:	You are responsible for calling the following employees and/or companies:
	1. Details are available in functional document on task basis_____
	2. _____
	3. _____
	4. _____
	5. _____
	6. _____
Vital Records:	The following documents and/or electronic media will be required for your recovery effort:
	1. Building Plan on Civil, Pipelines and Electrical Diagram
	2. Network diagram
	3. Employee List and Access Rights List for each application
	4. Applications installation guide
	5. Server Details and Disaster Recovery Plan
	6. Contact details of emergency numbers, vendors and all the teams

5. Emergency Contacts

5.1 Vendor Dependencies

All plans require a comprehensive listing of external contacts:

Provider:	Contact:	Purpose:
KEMS Help desk **Sales Team**	1821821 1820820	**Internet Service Provider and KSE Feed**
STC **Sales Team**	1804466 1804444-29	**Internet 3rd**
Zain Help desk	1804804	Wireless Internet
Burhan Tec Help desk	22498923	**Computer Hardware Vendor** **Lenovo Servers**
Mayura Traders Mr. Firoz Ansari	50711004	**Software Vendor (Microsoft Dynamics)**
Path Solutions	24824600	**Software Vendor (IMAL Application)**
Marsoft **Khaled Araby**	99712218	**Client & Portfolio Management Application** **Software Vendor (PMS)**
Al-Yousifi Systems Help desk **Sales**	24812123-385 24812123-354	**Computer Hardware Vendor** **IBM Servers and DLO**
KDCC Sales - Syed Mohsin	22449590 97698385	**Computer Hardware and Network Accessories Vendor**
Human Dream Co.	24752355	**HRMS - Software Vendor**
Burhan Technologies	22498923	**Servers, Veeam Backup and DR Solutions, VM, Azure, Firewall & Security Systems and MS Office 365**
Al-Farkad- Rejy Koshy	22405100 22405150	**TAMS system/Access Control**
Hadeed Hashem Hadeed	22441647/8 99712981	**UPS**
Burgan Systems (BNIS) Fadi Muhtadi Senior Systems Engineer	2247 8858 9980 8048	**BNIS – Portfolio & Client Management Software** **Maintenance & Support**
Middle Eastern Trading Co. (METCO) Jatin Lamba	9098483 1813300	**IP Telephony** **Sales & Help Desk**
Enhanced Engineering & Multi-Technologies Co. (EEMC) Juzer Tapiya, Manager, Corporate	94068430 1866661	**Network Switches** **Sales & Help Desk**

Appendix 1- Certification form

I certify that:

1.   I have carefully read Business Continuity Planning (BCP) on (date) _____
and I understand my role in this BCP and its importance for the Company. I understand that if I
have questions concerning the BCP, I shall communicate with my superior and/or the
Information Technology department to obtain explanations.

Signature: _____ **Date:** _____

Name (in block letters):_____

Please return the present form duly signed and filled out to the IT Department and keep your copy of
this to BCP to get into your role and responsibilities in case of crisis/disaster recovery planning.

Appendix 2 - Revision History Form

Policy Ref. No.	Issue No.	Revision No.	Date of Revision	Approved By	Approver's Signature
		1	4/3/2012	BOD	
		2	4/3/2013	No changes	
		3	4/3/2014	" "	
		4	28/12/2015	BOD	
		5	4/3/2016	No changes	
		6	30/3/2017	BOD	
		7	4/3/2018	No changes	
		8	4/3/2019	" "	
		9	28/10/2020	BOD	
		10	24/5/2021	No changes	
		11	14/5/2022	No changes	
		12	14/5/2023	BOD	
		13	14/5/2024	"	
		14	24/5/2025	"	