Board Paper No : 2024 / 811 / 09 / S Date : 27 / 09 / 2024

Board Meeting No : 77

BUSINESS CONTINGENCY & CONTINUITY PLAN

Policy Owner : Chief Risk Officer

BIRMC Presented Date : 14 / 05 / 2024

Board Approved Date : 27 / 09 / 2024

Version : 01

COPYRIGHT

CONFIDENTIALITY

DOCUMENT DETAILS	
Area	Description
Title	**BUSINESS CONTINGENCY & CONTINUITY PLAN (BCCP)**
Date	**27 / 09 / 2024**
Version	**1**
Owner	**Risk management Department**

DOCUMENT CHANGE CONTROL			
DATE	REASON / CHANGE	CHANGE AUTHOR	RECCOMENDED BY

BOARD APPROVAL	
DATE OF APPROVAL:	27 / 09 / 2024

Table of Contents

1 Executive Summary

The Business Contingency & Continuity Plan (BCCP) is of supreme importance in today's business scenario and has vital significance in the management of risks. The aim of the BCCP is to ensure that LCB Finance PLC (LCB) is able to maintain the highest level of service possible in the event that a disaster affects the infrastructure.

The Business Contingency & Continuity Plan provides a set of steps, procedures and information in order to ensure the continuity of the business during and following any critical incident that results in disruption to the operations / services provided by the company.

Business continuity planning focuses on sustaining the ability to deliver services in the event of a serious interruption to normal business operations. It is multi-faceted and covers all areas of the organization.

Generally, Systems are vulnerable to operational caused by failure of internal processes, systems and external events i.e. variety of disruptions, ranging from mild (Such as short-term application failure, power outage, disk drive failure) to severe (Such as Equipment destruction, major power sabotage, fire) from a variety of sources such as natural disasters to criminal / terrorists' activity.

The entity's BCCP is to address the planning and reaction in a coordinated approach in order to eliminate vulnerabilities through technical and operational solutions.

This document will focus on five key phases of the entity's BCCP, namely

1. Guiding Principle

The policy defines the scope, purpose and the commitment towards the BCCP adopted by the entity.

2. Assessment & Analysis

Under analysis the following main aspects are considered;

- Business Impact Analysis to assist the entity to prioritize critical systems and components by identifying the potential impact of business disruptions.

- Evaluation of Maximum allowable downtime (Maximum Tolerable Downtime - MTD) and acceptable level of loss, associated with the business functions and processes; and the Estimation of the Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and work recovery time.

- Risk assessment consists of the evaluation of risk in which assumptions and uncertainties are clearly considered and also prioritizing potential business disruptions based upon their severity and their impact on the entity's operations and probability of occurrence.

-Vulnerability and Interdependency assessment of critical support areas such as telecommunication, transportation services, support for hardware & software and third-party vendors.

3. Risk Management

The entity will address the risk of business disruptions by formulating Crisis Management Teams (CMT), Secondary sites (DR Site) and Crisis Management Process Development and Implementation based on the assessment and analysis Business Continuity. (i.e. Business Impact Analysis and Response)

- BCCP Teams and Responsibilities

This document will define the teams behind the BCCP Activities and their tasks towards crisis management.

i. Information Security Management Committee (ISMC) – Board / Corporate Level) will conduct Business Continuity Steering Meetings. Responsible for strategy formulations and financial resources. BCCP Recommendations and approvals.

ii. Disaster Recovery Management Committee (DRMC) - Responsible for BCCP Development, Implementation, Testing & Maintenance

iii. Disaster Recovery Operational Team (DROT)

- Geographical Site for Disaster Recovery (DR) to facilitate BCCP

The entity will have a secondary site namely Disaster Recovery site which is to handle systems replications (Physical location to maintain the DR Servers and equipment) and a Disaster Recovery operational site which facilitates relevant DR officials to operate the DR site. In addition, the Contingency operational sites to handle the operations.

The BCCP enables the entity to formulate a recovery strategy for critical systems. The recovery strategies will assist LCB to ensure a superior decision-making process and systems recovery process during the event of a disaster.

-Business Continuity Strategy & Implementation

This document will discuss the design including the network diagram development and implementation process / strategies for the entity's critical systems and functions. Further, illustrate the architecture / methodology of replication of Systems & Databases and the recovery / resumption actions.

- Crisis Management

This document will define activities involved following a major disruption or disaster. The activities will consist of disaster declaration, Crisis communication, Emergency notification and emergency response including staff transportation and telecommunication facilities.

4. Risk Awareness & Testing

This document establishes the importance of BCCP training & testing.

- A comprehensive training will be provided to the relevant team members to create awareness of their roles in the implementation /operation of the BCCP.

- The entity will ensure the testing of critical systems and test results will be gathered and documented for review of same by the management.

5. BCCP Acceptance & Maintenance

- The test results will be reviewed by the senior management on a regular basis

- The revision of the BCCP and the testing program will be based upon the changes in business operations, audit recommendations and test results

- The BCCP document will be continually updated to reflect the current operating environment (constantly as a living document)

- The BCCP will be reviewed and approved on an annual basis by the Board

2 Introduction

The purpose of developing a Business Contingency & Continuity Plan is to support the continuity of the business during and following any critical incident, service outage, which results in disruption to the normal operational capability.

A Business Contingency & Continuity Plan will allow the company to continue the business avoiding financial losses, regulatory fines and to maintain compliance with regulations laid by the governing bodies. It also provides security to the staff of the company while providing assurance to the clients of an uninterrupted service.

This document demonstrates the Business Contingency & Continuity Plan for LCB. The contents of the document provide information needed for post interruption decision-making and the entity's response to any disaster or extended interruption of normal operations and services to its customers.

The BCCP represents the Entity's commitment towards the 4R planning of "Risk Assessment", "Response", "Resumption / Recovery" and "Restoration / Return".

In addition, the entity's BCCP encompasses the activities and responsibilities of the Board, Corporate Management and other relevant teams in order to ensure and maintain a feasible and demonstrable business continuity process through a consistent planning methodology. Further this document will focus on the requirements of continuous review and upgrading of the BCCP to keep pace with changes in the environment in which LCB operates.

3 BUSINESS CONTINUITY PLAN

3.1 BCCP General Information & Guiding Principle

3.1.1 BCCP Document Distribution List / Update List

NAME	DESIGNATION	COPY NO.
Mr. K. G. Leelananda	Chief Executive Officer	001
Mr. K. K. Wannige	AGM Finance & Strategic Planning	002
Mr. M. J. H. Perera	Chief Risk Officer	003
Mr. Vajira Jayasinghe	Deputy General Manager – IT	004

Mr. T. M. N. J. Fernando	Deputy General Manager (Credit)	005
Mr. Aruna Vithange	Deputy General Manager (Business Development & Fund Mobilization)	006
Mrs. Thamarika Rodrigo	Company Secretory	007
Mr. H. D. S. K. Jayasinghe	DGM - Recoveries	008
Ms. W. H. A. C. Fernando	Head of Legal	009
Mr. W. V. D. M. H. Wevita	Head of Compliance	010
Mr. R. M. Gnanarathne	Head of Finance	011
Mr. Oswal Sahabandu	Head of Business Development	012
Mr. Srimal De Silva	Manager Human Resources	013
Mr. M. K. R. S. Kumara	Head of Leasing	014
Mr. A. P. Senevirathna	Manager – IT	015
Mr. G.A.M.U.W. Emitiyagoda	Manager – IT	016
Mr. K. Sashi Kumar	Senior Manager - Recoveries	017
Mr. Thilina Bandara	Assistant Manager - Audit	018
Ms. K A C N Kodithuwakku	Assistant Manager - Audit	019
Mr. D. M. W. Bandara	Manager - Administration	020
Mr. H. G. A. Kumara	Senior Manager – Credit	021
Mr. K. T. K. Thiruchchenthuran	Manager – Credit	022
Ms. W P A U Weerasooriya Manike	Manager – Gold Loan	023

3.1.2 Document Approval

APPROVER	DESIGNATION	DATE
Mr. Dushmantha Thotawatte	Chairman of BIRMC (Independent / Non-Executive Director)	
Mr. Ashwin Nanayakkara	Independent / Non-Executive Director	
Mr. Mahesh Katulanda	Independent / Non-Executive Director	
Mr. J.P.G. Jayalath	Independent / Non-Executive Director	

3.1.2.1 References and related documents

- Disaster Recovery Plan
- List of employees with contact details
- Contact details of vendors

- Building site plan
- Latest stock and equipment inventory
- Maintenance Agreements

3.1.3 Revision Control

This document should be reviewed annually by LCB Finance.

VERSION	DATE	SUMMARY OF CHANGES MADE	CHANGES MADE BY (NAME)

3.1.4 Key Recovery Team Members

Name of the Contact Option	Contact Details	
Mr. K G Leelananda CEO	Work	200
	Mobile	777724761
	Home Address	No. 564, Isuru Uyana, Baaswatta, Narawala, Poddala
	Email Address	leelananda@lcbfinance.lk
Mr. K K Wannige – AGM Finance & Strategic Planning	Work	209
	Mobile	760988089
	Home Address	No. 12/546, Himburawa Road, Galle
	Email Address	kelum@lcbfinance.lk

Mr. M. J. H. Perera – Chief Risk Officer	Work	205
	Mobile	773421215
	Home Address	No. 05, Base work shop area, Ampara
	Email Address	jayalal@lcbfinance.lk
T M N J Fernando – GDM Credit	Work	245
	Mobile	771859996
	Home Address	2/2, Palliya Road, Diyalagoda, Maggona.
	Email Address	nishantha@lcbfinance.lk

3.1.5 External Contact List

Services	Vendor	Address	Contact Person	Mobile Contacts	Telephone	Email
SLT Voice & Data Links	SLT Mobitel PLC	Lotus Rd, Colombo 10	Lahiru Kularathna	710119642	112864314	lahirus@slt.com.lk
Secondary Data Link & Voice Package	Dialog Axiata PLC	475 Union Pl, Colombo 2	Malinda Wijesinghe	777331662	777678700	Malinda.Wijesinghe@dialog.lk
End Point Security	AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 2	Damitha Anuradha	775071078	117439208	damitha@acsysnetworks.com
HP Servers / SAN	VS Information Systems (Pvt) Ltd	7 Sulaiman Terrace, Colombo 005	Dithika Jayakody	773448335	112038568	dithika@vsis.lk
NAS	DMS Electronics (Pvt) Ltd	Pagoda Rd, Sri Jayawardenepura Kotte	Dhanushka Madushanka	773959577	114732100	dhanushka.madushanka@dmselectronics. com

Backup Appliance	Ultrium Technologies (Pvt) Ltd	RVH9+5F3, Dehiwala-Mount Lavinia	Lahiru Kariyawasam	768203620	115882933	lahiru@ultryum.com
Server Room Maintenance	Assidua technologies (Pvt) ltd	149 Galle Rd, Dehiwala-Mount Lavinia	Nadeepa Silva	767634666	112710088	nadeep@assiduasolutions.com
Branch Centralize UPS	Asiacom Engineering Services (Pvt) Ltd	No.123, Bauddhaloka Mawatha, Colombo 04	Manjula Madurapperum a	765788944	117444125	manjula@asia.com.lk

3.1.6 Glossary

Business Continuity Planning: a process that helps to develop a plan document to manage the risks to a business, ensuring that it can operate to the extent required in the event of a crisis/disaster.

Business Continuity Plan: a document containing all of the information required to ensure that your business is able to resume critical business activities should a crisis/disaster occur.

Business Impact Analysis: the process of gathering information to determine basic recovery requirements for your key business activities in the event of a crisis/disaster.

Recovery Time Objective (RTO): the time from which you declare a crisis/disaster to the time that the critical business functions must be operational in order to avoid serious financial loss.

Risk Management: is the process of defining and analyzing risks, and then deciding on the appropriate course of action in order to minimize these risks, whilst still achieving business goals.

Business Unit: smallest organizational unit, one carrying out one or more business operations.

Damage: the cost of repairing or replacing an asset, plus any consequential cost or loss.

Damage Assessment: Superficial assessment of impact, by the Business Continuity Team to decide if the Business Contingency & Continuity Plan should be invoked. Full assessment of physical damage to premises by the Premises Manager to determine restoration needs.

Disaster: any unwanted significant incident, which threatens personnel, buildings or the organizational structure of an organization which requires special measures to be taken to restore things back to normal.

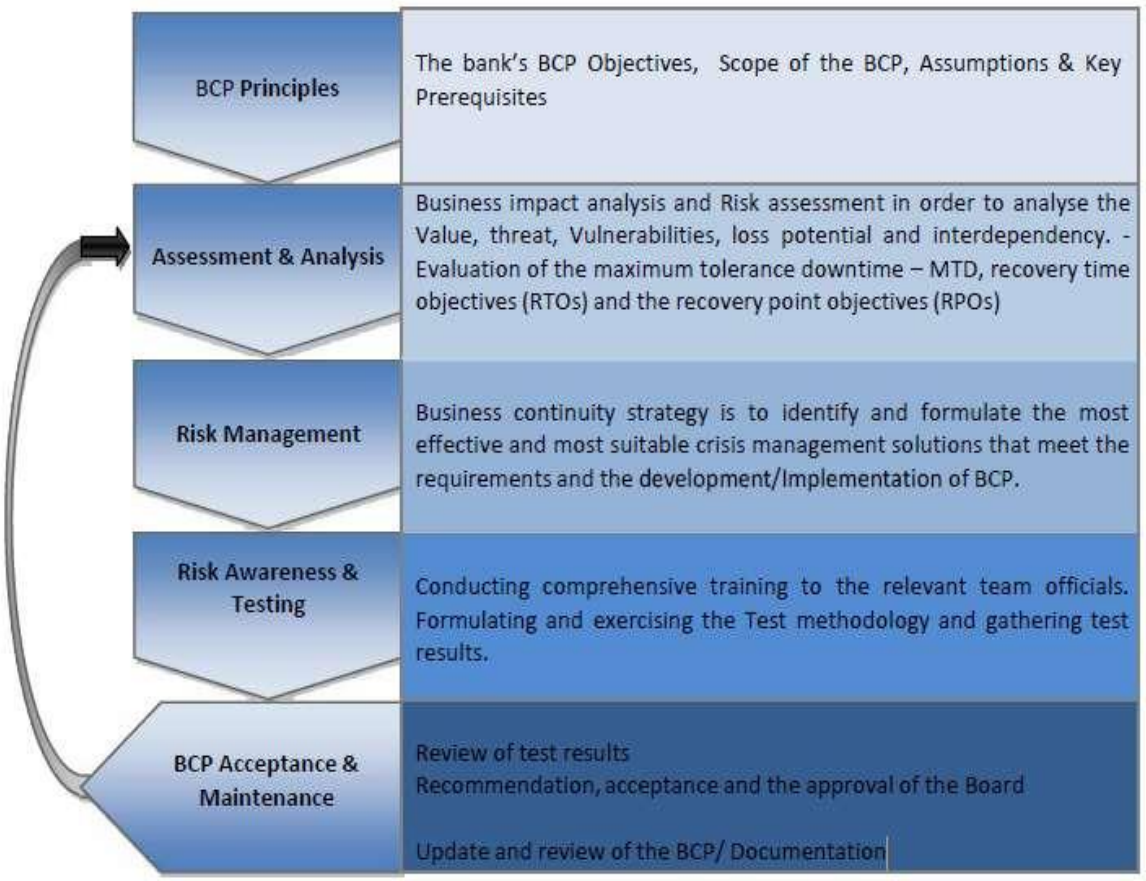
Critical Business Operations: those operations carried out at the premises for which there are compelling reasons why they should restart rapidly.

Incident: an event, which may become disastrous.

4 Business Continuity Policy

The entity is committed to its customers, employees and shareholders. The Business Contingency & Continuity Plan supports business operations and provisioning of service to ensure the availability of essential products and services offered by the company in the event of a disaster/ interruption.

4.1 BCCP Overview



4.2 Approach to Business Continuity Planning

LCB Finance approach to Business Continuity is one of systematic analysis and implementation of a well thought out plan, supported by the management. Its ambit includes information, information processing assets and supporting assets.

The approach is based on:

- The existence and maintenance of facilities, infrastructure and network that provide for adequate redundancies in critical components
- The existence and implementation of security and administrative policies and procedures
- The use of appropriate technology and tools ensuring business continuity is fine-tuned to client needs

The BCCP is based on the two-pronged approach consisting of "prevention" and "recovery". Under Prevention the aim is to attempt to control all that is controllable and prevent the occurrence of events that can lead to interruption. If in spite of these controls, an event or a disaster outside our control happens, then the effort is to recover the operations through well-designed and implemented recovery measures.

i. **Prevention** – The implementation of preventive controls against a number of threats seeks to ensure that the occurrence of events and conditions that could result in any interruptions to business is prevented right at the outset of the occurrence.

ii. **Recovery** – The design and implementation of a number of recovery controls seeks to ensure that in the occurrence of an event that causes an interruption to business, recovery happens at the earliest with the restoration of operations through multiple options using various implemented recovery mechanisms.

4.3 Policy Objectives

- To ensure the existence and availability of a well-documented Business Continuity Plan
- To define and prioritize the functions critical to the business
- To determine the Recovery Time Objective (RTO) of all information systems, data and other resources have been clearly defined.
- To detail recovery strategies and response to critical incidents to ensure continuity of business
- To ensure that the Business Contingency & Continuity Plan has been tested in full and amendments are made where necessary.

4.4 Scope

This applies to all users of LCB Finance, including the LCB employees, employees of temporary employment agencies, consultants, vendors, business partners, and contractors

Each department is responsible for current and comprehensive Business Continuity Planning (BCCP). When implemented, the Plan should include those procedures and support agreements, which ensure on-time availability and delivery of required products and services.

The BCCP will provide failover solutions and DR Solutions to the critical IT Systems & other processes with adequate technology and same will be facilitated to recover according to the time period (i.e. Recovery Time Objective - RTO), within which they must be recovered in order to meet the organizational objectives.

4.5 Plan Objectives

- To serve as a guide for LCB recovery teams.
- Minimize Financial, Legal and other risks
- Provides procedures and resources needed to assist in recovery.

- Identifies Individuals that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Minimize the probability (likelihood) and impact (risk) of interruptions
- Identifies alternate sources for resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

4.6 Assumptions

- Key people (Team Leaders or Alternates) will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.
- The replication of the databases / systems between the Primary site (Production)
- Secondary Site (DR) take place according to the required standard.
- Network connectivity between the following multiple locations are in order
    - Primary Site (Production) and the Secondary Site (DR)
    - Secondary Site (DR) and the DR Operational Site
    - Secondary Site (DR) and Branch network
- All relevant patch updates/bug fixes are carried out concurrently to both the Primary Site and the Secondary Site
- The DR volume support is limited to the delivery of essential business services
    - Number of concurrent user accesses to DR from the Branch in order to deliver essential business services
    - Total number of concurrent user accesses to DR

4.7 Key Prerequisites for Business Continuity

- The DR Site, DR Operational sites and the DR Infrastructure are in place
- All relevant officials are given comprehensive training and they will be in position to handle their own respective roles independently and prudently in order to assure the accuracy of the team responsibilities and resumption procedures
- The appropriate risk assessment is carried out
- All appropriate materials and checklists are in place and available at all times

- The BCCP is periodically tested and test results are in compliance with the BC Requirements
- All Backup media are properly labelled and securely stored (for additional contingency)
- The BCCP is kept up to date

4.8 Office Locations

Apart from the main locations stated below we have branches located.

A. Head Office

Head Office is located at No. 76, S. De. S Jayasinghe Mawatha, Kohuwala, Nugegoda. Its main telephone number is 011 2825404. We engage in all banking and finance functions in this location.

B. DR Site

DR Site is located at No. 155, High level Road, Maharagama. Its main telephone number is 011 2840244. We engage in all banking and finance functions in this location.

4.9 Emergency Operating Centers

In the event of any situation where access to a building housing a system is denied, personnel should report to closest alternate location at No.155, High Level Road, Maharagama. (LCB Maharagama Branch)

4.10 Customers Access to Funds and Securities

Documents related to customer's funds or securities are maintained at the branches in physical form and signature and identification card in digital form. In the event of a disaster, if telephone service is available, the registered people will take customer queries and forwarded to the Deputy General Manager – Business Development & Fund Mobilization on 076 0988088.

5 Disaster Classification and Management

5.1 Disaster Classification & Business Impact

Any loss of utility Services / Public Infrastructure (Power, Road Access), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by LCB operations.

The plan identifies vulnerabilities and recommends measures to prevent extended service outages. There are many potential disruptive threats which can occur at any time and affect the normal business process. Each potential environmental disaster or emergency situation has been examined.

The focus here is on the level of business disruption which could arise from each type of disaster. The classification of a disaster will dictate the level of response by the company. Essentially, there are two assessments involved in classifying a "disaster".

- Extent of the damage
- Expected duration of the interruption

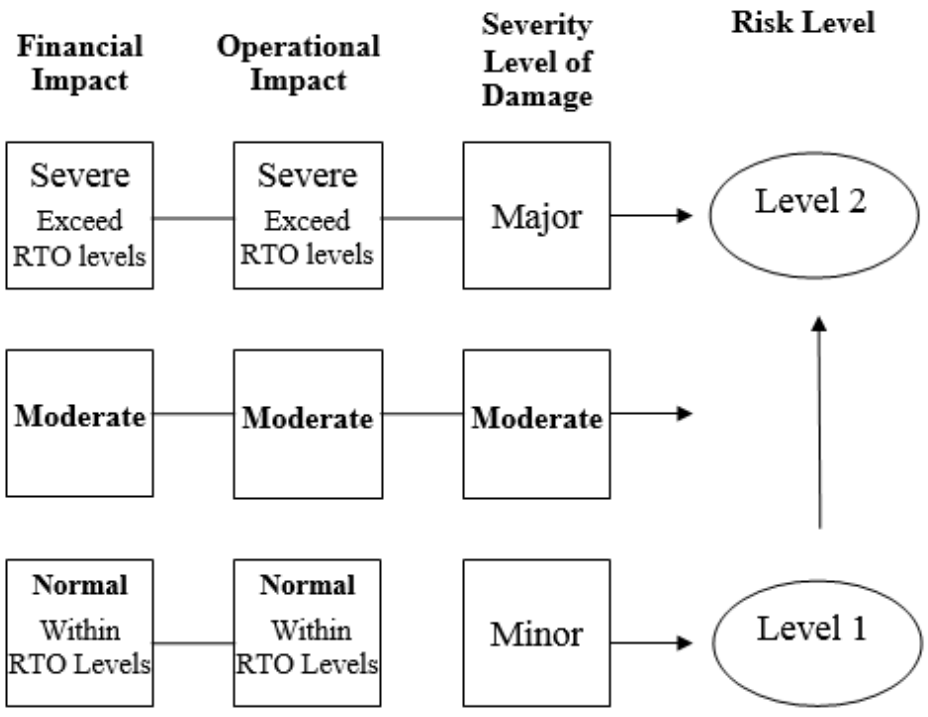
As used in the business unit recovery procedures, the extent of the damages is termed:

- Major
- Minor

Similarly, the expected duration of the interruption is an important consideration. In most physical disasters such as fire, flood, etc. the extent and duration are fairly obvious. While the precise duration may not be known, it is usually obvious that the required recovery time frame has been exceeded and the recovery plan must be activated. However, in other types of interruption, most usually associated with supply of utilities or hardware failure, the duration of interruption is frequently less obvious. For these situations, uses the following terminology.

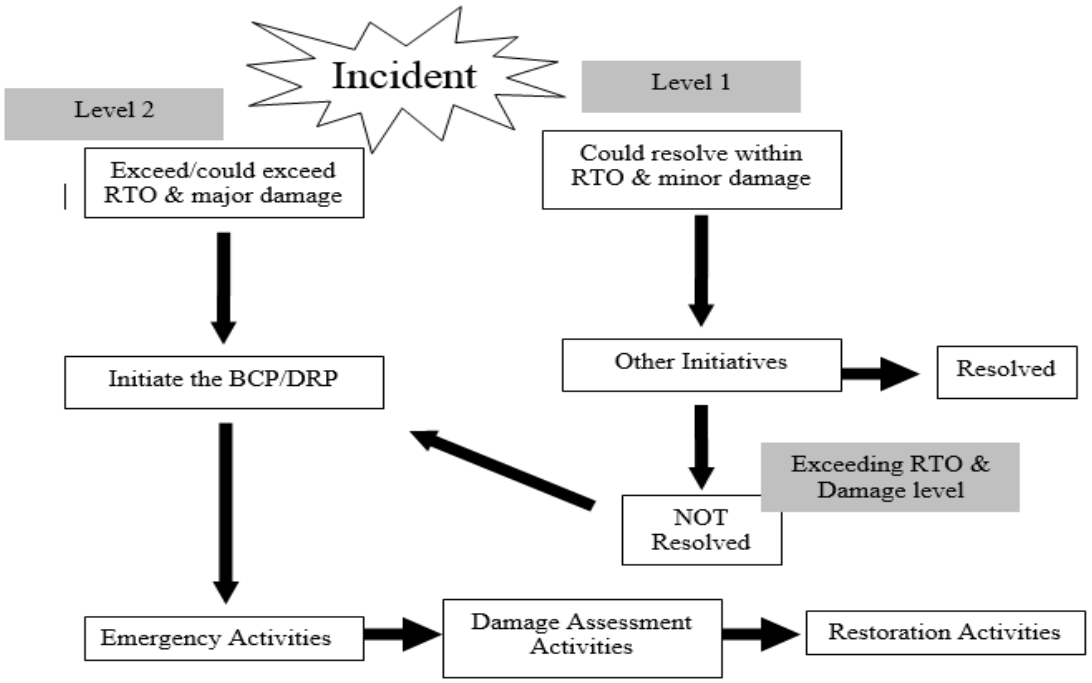
Level 1 – Within RTO time frame

Level 2 – Exceeding RTO time frame



Note: The terminology and precise definition and examples may be modified based on each individual situation.

Disaster/incidents are described from both business impact and operational level. From a business standpoint, an interruption of services within RTO levels and a minor damage (Level 1) for the entity impact the business to a lesser extent then level 2.



Potential disasters have been assessed as follows:
Calamities or Disasters on a Large Scale

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor Interruption

POTENTIAL DISASTER		PROBABILITY RATING	BUSINESS IMPACT	REMEDY
Natural Disaster	Flood	5	1	Insurance Coverage
Natural Disaster	Fire / Explosions	3	1	Insurance Coverage
Technology Disruption	Electrical power Failure / shortage	2	1	Power Generator
Technology Disruption	Loss of communications network services	4	4	Service Provider assistance
Technology Disruption	IT system failure	4	1	Obtain vendor support
Natural Disaster	Tsunami	5	1	-
Technology Disruption	Malware Attacks	3	2	Obtain vendor support
Technology Disruption	Termination of Service by the vendor	4	3	Escrow agreements
Disruption due to Human Activity	Terrorist Attack	5	1	-
Natural Disaster	Cyclones	5	1	Insurance Coverage
Disruption due to Human Activity	Theft or Vandalism	4	2	Insurance Coverage
Disruption due to Human Activity	Restricted Access to Premises	3	1	Relocate to DR Site / Alternate Location
Disruption due to Human Activity	Loss or Illness of Key Staff	2	2	Training of Alternate personnel to take over responsibilities
Reputational Crisis	Loss of Goodwill	5	1	-
Strategic Risk	Tightening of Regulations / High Risk Ventures	4	1	Diversification of Portfolio / Products

5.2 Instructions for using the plan

5.2.1 Invoking the plan

This Business Contingency & Continuity Plan becomes effective when a disaster occurs and will remain in effect until operations are resumed at the original location, or a replacement location and control is returned to the appropriate functional management.

5.2.2 Disaster Declaration

The CEO is responsible for declaring a disaster for Business interruption and activating the various recovery teams as outlined in this plan. In the absence of the CEO, the Deputy General Manager - Administration & Operations/Operations Manager will make this decision.

At branch level disasters the Branch Manager shall consult the CEO or in his/her absence the Deputy General Manager - Administration & Operations who will then declare a disaster. If time permits and based on the level of disruption a meeting of the emergency management team shall be convened.

NAME	CONTACT OPTION	CONTACT NUMBER
Mr. K G Leelananda **CEO**	Work	200
	Mobile	777724761
	Home Address	564, Isuru Uyana, Baaswatta, Narawala, Poddala.
	Email Address	leelananda@lcbfinance.lk
In the absence of CEO, the Deputy General Manager - Administration & Operations will declare the disaster.		
Mr. H. D. S. K. Jayasinghe **DGM – Operations**	Work	234
	Mobile	773587781
	Home Address	55/1, Orutota Road, Gampaha
	Email Address	jayasinghe@lcbfinance.lk
Main Branch - Head Office		
Mr. M. J. H. Perera – Chief Risk Officer	Work	205
	Mobile	773421215
	Home Address	No. 05, Base work shop area, Ampara
	Email Address	jayalal@lcbfinance.lk
Mr. W. V. D. M. H. Wevita – Head of Compliance	Work	207
	Mobile	760988086
	Home Address	No.06 Field Mawatha, Kohuwla, Nugegoda.
	Email Address	mangala@lcbfinance.lk
All other branches		

Location Head	In the event of disaster in any branch, the Location Head should inform the level of disaster to the CEO. The location head is attached as an annexure.
In the absence of Location Head	
Branch Assistant Manager	In the absence of location head, the Branch Assistant Manager should inform the level of disaster to the CEO immediately.

The Emergency Management Team and Location Response Coordinator are responsible for handling the operations when a disaster is declared for Technical Services/Business interruption and activating the various recovery teams as outlined in this plan.

5.3 Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the Emergency Management Team (EMT) must be activated immediately in the following cases:

- One (1) or more systems and/or sites are down concurrently for five (5) or more hours
- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur

5.3.1 Evacuation Procedure

A floor plan of the building is attached to this Business Contingency & Continuity Plan [Refer Annexure 3 – Floor plan of the building]

Assembly Point:

Where the premises need to be evacuated, the BCCP identifies an evacuation assembly point: Refer Annexure 3 for assembly points.

1. Once an incident is declared as a Disaster the Business Contingency & Continuity Plan will be activated.

2. The following steps (a./ b./ c.) should be followed only if time permits:

- Get personal items from desk (keys, purse, etc.)
- Turn off computers, copiers and other electrical devices
- Forward phones to voice mail or remote location

3. Exit the building through nearest exit door. If the nearest door is close to the emergency, go to another exit door

4. After exiting building, report to designated assembly area location.

5. Perform a roll call to ensure everyone has safely evacuated the building.

5.3.2 Items to be picked up

In the event of a disaster where the building should be evacuated, and the operations need to be carried out at an alternate site, the following items may be taken

Documents:

- Business Continuity Plan
- Disaster Recovery Plan
- List of employees with contact details
- Lists of customer and agent details
- Contact details for emergency services.
- Contact details for utility companies.
- Contact details of vendors
- Building site plan
- Latest stock and equipment inventory
- Insurance company details
- Financial information
- Engineering plans and drawings
- Product lists and specifications
- Formulas and trade secrets
- Stationery, company seals and documents
- Maintenance Agreements
- Copies of agreements and AMC, warranty docs

Equipment:

- Computer back-up tapes/ disks/ USB memory sticks or flash drives.
- Spare keys/security codes
- Any other equipment that may be needed
- Installation media for critical systems
- Network and Systems architecture diagrams and designs

5.3.3 Service Providers

The following information is documented and included in this Business Contingency & Continuity Plan as an annexure

[Refer Annexure 5 – Service Providers]

Specific Providers who need to be contacted to repair or replace equipment or supplies critical to the operation of the data center and required as part of the recovery effort are included.

A. New and Used Hardware Providers

Recovery planning efforts are focused on computing equipment. Detailed descriptions of all installed hardware are maintained in the IT inventory list maintained by the IT officer of LCB.

[Refer Annexure 7 - IT Inventory List]

B. Software Providers

A complete inventory of any special software, whether operating system or application system is maintained and a copy kept in offsite storage. All software is backed up on an ongoing basis as part of the DR procedures.

C. Office Supplies and other Equipment Providers

A list of providers is maintained by the administration division and attached as an annexure to this Business Continuity Plan. [Refer Annexure 8 - List of Agreements/ Crucial Documents/ Registers] Copies of agreements with the above suppliers/ service providers are maintained at offsite storage location.

5.4 Backup Policy & Procedure

Full backups that preserve company information assets and are taken on a regular basis for audit logs and files that are irreplaceable that are considered critical. Backup media are stored in a secondary location to be obtained and restored in the event of a disaster.

Our office maintains its primary hard copy books at the selected branch locations [Refer Annexure 8

- Filing locations of physical records] and its electronic records at the Head office. The Genius Operations of the filing location for physical records and the ICT division for digital information is responsible for the maintenance of these books and records. Our office maintains the following document types and forms that are used for daily operations

- Credit files and agreements
- Deposit applications
- Real estate deeds
- Location lease documents
- Pawning tickets
- HR documents
- Legal documents
- Finance documents
- Cash Deposit / Withdrawal Slips & Vouchers

- Marketing Material
- Risk and compliance

All backup media are stored at the designated backup location. Backup media should be tested at periodic intervals to ensure their continued availability. Back-up logs shall be stored securely.

Refer Disaster Recovery Plan

6 Assessment & Analysis of Risk

6.1 Business Impact Analysis [BIA]

When any of the disasters listed above strike, they are likely to cause some disruption of the business. The disruption can impact the business in many ways. Sometimes the impact can result in financial loss, operational loss, loss of lives, and loss to organization image, regulatory and legal non compliances, customer dissatisfaction, etc., hence it is necessary to analyze the impact of the disruption to assess the severity of impact in order to design appropriate recovery procedures. The design of the recovery solution determines the time by which recovery can take place. The more severe the impact, quicker will have to be the recovery time.

All disasters may not impact all the business activities or all business assets. A clear identification of Business activities and assets and their criticality is necessary before the business impact analysis can be done successfully as stated below:

- Identification of Critical Business Processes for the continuity of operations
- Identification of Critical Resources
- Assessment and Identification of acceptable downtime

The BIA is carried out to identify and prioritize the critical business processes. LCB has carried out an institution-wide systems BIA considering Financial, Operational, Reputational impact. The entity's business function, processes and the related IT Systems have been taken as the key input for the BIA.

The output of the BIA establishes the critical functions of the entity and the corresponding interdependencies between the Systems and the Operations plus the relevant output contributes as inputs to the recovery and business continuity strategy development process. The outcome of the entity's BIA establishes that the following systems are considered to be the most critical in the entity.

01. Level one – Within RTO

02. Level two – Outside RTO

6.1.1 BUSINESS OBJECTIVES FOR THE PURPOSE OF A BIA

Establishing the functions/operations which are deemed as "Business Critical" and "Urgent" is a process that has engaged the CEO/MD, Senior Management and

Middle/Line Management who have a clear view of the operational and functional processes.

The Entity's Vision and Mission provide the basis and direction in determining what's

Critical / important to the organization.

Vision of LCB Finance PLC

To be the Financial Services will be recognized as proactive, results-oriented leaders who work in collaboration with their clients to offer excellence in operational and strategic financial management to support the achievement of our objectives.

Mission of LCB Finance PLC

To be Financial Services provides excellence in client service and compliance through our unwavering commitment to our staff, our understanding of financial operations, and a continued focus on process improvement.

6.1.2 REPRESENTATION OF BIA BY BUSINESS PROCESS PRIORITIZING MODEL

The Business Process Prioritizing Model is based on the BIA which represents a tier-based prioritization of the business processes and establishes the inherent value of the business processes.

TIER CLASSIFICATION	IMPACT RATING OF BUSINESS PROCESS
TIER ONE	VERY HIGH
TIER TWO	HIGH
TIER THREE	MEDIUM
TIER FOUR	LOW

BUSINESS UNIT	CRITICALITY OF BUSINESS ACTIVITIES			
	TIER ONE	TIER TWO	TIER THREE	TIER FOUR
Operations				
Finance				
IT				
Internal Audit				
Legal				
Human Resources				
Administration				
Cash Management				
Compliance				
Recoveries				
Sales & Marketing				
Call Center Operations				
Risk Management				

6.1.3 BUSINESS UNITS & CORRESPONDING CRITICAL FUNCTIONS TO BE PERFORMED IN CASE OF A DISASTER

Name of critical business unit	Short description of current business unit process	Impact of process disruption	Time after which the disruption of this process becomes	
			Urgent	Business Critical
Deposit Unit **Products Offered** Fixed Deposits **Critical Functions** - Placements - Upliftment's (At Maturity & Premature) - Interest Payments - Responding to Inquiries - Filing and storage of Mandates & other lodgments	LCBI accommodates fixed deposits inquiries for placements & other such details from customers via telephone, fax, email, website or in-person. During a Significant Business Disaster, the entity should continue to accommodate responding to customer inquiries, placements & upliftments of fixed deposits through reliable methods available. Further, Interest Payments should also be accommodated. In addition, it is the company policy to inform their clients about the current situation and alternatives to use for FD Placements/Withdrawals. Customers will be informed of alternatives via Short Messaging Services, emails or telephone. If the facility cannot be accommodated at the current branch, customers will be advised to place deposits directly with the	Very High	02 Hours	01 Day
Lending & Advances (Credit) Unit **Products Offered** Personal Loans Finance Leasing Security Loans Hire Purchases **Critical Functions** - Evaluation of Credibility - Granting of Loans - Settlement of Loans	Prompt and hassle-free processing of Loans (Placements & Disbursements) is probably the most widely used indicator by existing/potential clientele to decide if they wish to do business with an entity. Therefore, it is crucial that the company should be able meet the laid down service standards when it comes to Loan processing at all times. Processing involves all steps starting from inquires, placements to settlements and is to ensure that all necessary documents are received by the Company. The Urgency and importance of Loan processing	Very High	02 hours	01 Day
- Release of Security / Collateral - Insurance - Responding to Customer Inquiries -Filing and storage of security documents	depends on the type of Loan which need to be processed. If the facility cannot be accommodated at the current branch, customers will be advised to place deposits directly with the nearest / alternate branch.			

Pawning Unit Products Offered Gold Loans **Critical Functions** -Determining the Authenticity of Collateral - Granting of Loans - Settlement of Loans - Article Redemption -Responding to Customer Inquiries - Storage of security documents & Collateral - Traceability of Articles	Prompt processing of Loans Gold is a crucial function that the company should be able meet the laid down service standards when it comes to processing of Pawning facilities. Processing involves steps starting from inquires, determining the authenticity of collateral or the article, granting of the loan, secure storage of item to settlements & redemption. If the facility cannot be accommodated at the current branch, customers will be advised to place deposits directly with the nearest/alternate branch.	Very High	02 hours	01 Day
Collection and Recoveries Unit **Critical Functions** - Reconciliation of Payments (Direct Bank Transfers) - Responding to Inquiries - Collection of Installment Payments/ Capital / Interest Components	The Collection and Recoveries Unit has to reconcile the daily collections made directly to the Bank by the clients in terms of Lease Installment Payments and transfers executed by agents for RBL and Hire Purchase Facilities. After a reconciliation is performed based on the Bank Statement against the Schedule emailed by the agents, the system is updated to accommodate the payments and reports are spooled to generate Age-wise debtors/Arrears/NPA reports. Other activities include the generation of Reminder Notices every 7 days / 14 days / 2 months and a Termination letter is issues on the day the arrears surpasses 2 months and 7 days after which the facility is handled by the Legal division (Outsourced).	High	01 Day	03 Days

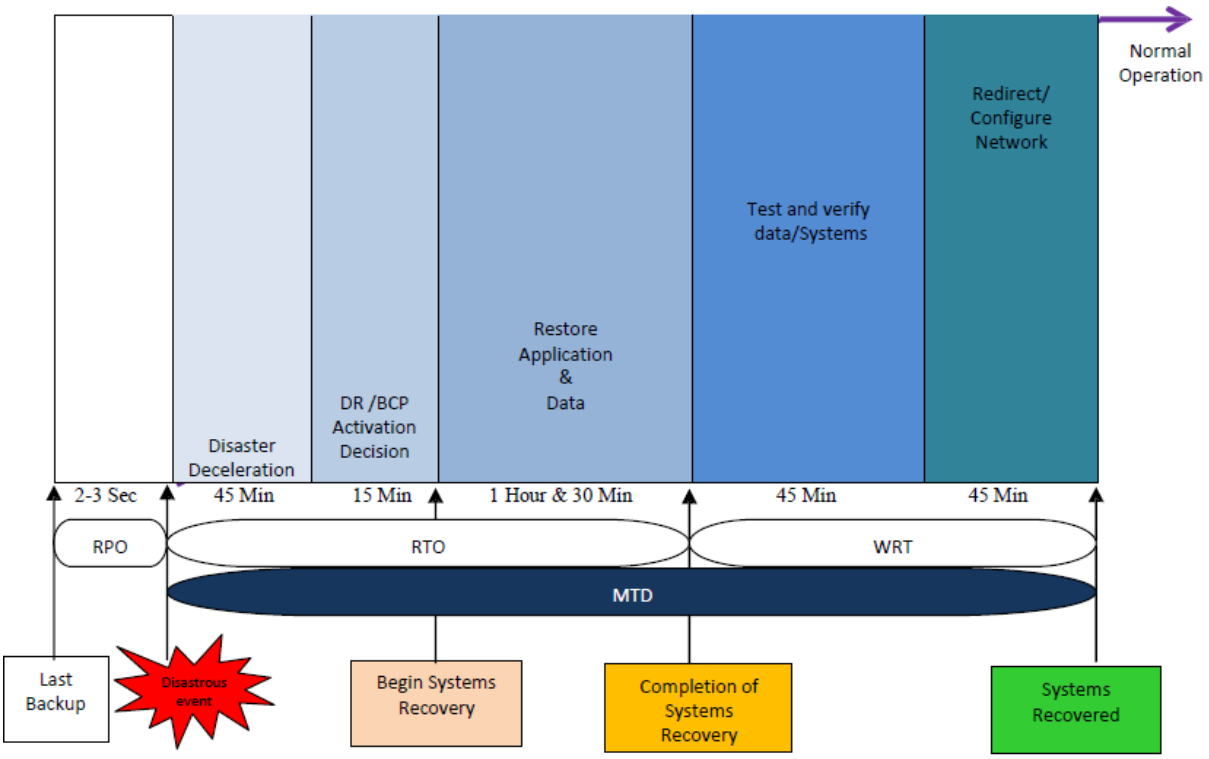
Compliance Unit **Critical Functions** - CBSL Reporting (Fulfilling Statutory Reporting Requirement) -Documentation	Fulfilling Statutory Reporting Requirements & maintaining appropriate documentation of same.	Medium	03 Days	01 Week
Information Communication Technology Unit **Critical Functions** - Purchase of new hardware, setting up, configuring the devices - Installing system & Restoring Backups - Verifying the application And database integrity - Setting up user PCs, networks and other devices required to carry out operations - Data Protection	Delays in updating the system, generating reports critical to operations and recovery. The below listed functions can be considered as crucial activities that need to be performed in case of a disaster. Purchase of new hardware, setting up, configuring the devices. Installing system & Restoring Backups. Verifying the application and database integrity. Setting up user PCs, networks and other devices required to carry out operations and ensuring Data Protection.	Very High	02 Hours	04 Hours
Accounting & Finance Unit Critical Functions -Generating Financial Statements -Reconciliation of Bank Accounts -Handling Payments	The Finance Unit is responsible for the Generation of Financial **Critical Functions** -Generating Financial Statements -Reconciliation of Bank Accounts -Handling Payments	Medium	03 days	

6.1.4 SYSTEMS & VITAL RECORDS NECESSARY FOR CRITICAL FUNCTIONSAL RECORDS NECESSARY FOR CRITICAL

BUSINESS PROCESS	SYSTEM SUPPORT REQUIRED / PROCESSES	REQUIRED DOCUMENTATION	PROCESS OWNER
Fixed Deposits	• Functioning of IT servers • Document Management System, file scanning • E-Financials System • Email Facility	• Fixed Deposit Mandates • Fixed Deposit Certificates • Fixed Deposit Register • Image Repository	Manager – Fixed Deposits
Lending / Advances	• Functioning of IT servers • Document Management System, file scanning • ERP 2 System • I front System • E-Financials System • CRIB System • Email Facility	• Security Documentation • Loan Register • Image Repository • X1 Forms / Demand Promissory Notes / Agreements	Mrs. Nisansala Dias Manager – Main Branch Mr. KTK Thiruchenturan Manager – Credit
Pawning	• Functioning of IT servers • Document Management System, file scanning • E-Financials System	• Pawning Register • Pawning Tickets • Battery Backups • Image Repository	Ms. Anuradha Weerasuriya Head of – Gold Loans
Collection & Recoveries	• Functioning of IT servers • ERP 2 System • I front System • E-Financials System • Email Facility	• Loan Portfolio • NPA Listing • Arrears & Age wise Reports • Customer Contact List • Asset Details	Mr. Sashi Kumar – Credit & Recoveries
Legal	Function Outsourced	- N/A -	Ms. Anusha Fernando Head of Leaga
Cash Management (Operations)	• Functioning of IT servers • E-Financials System	• General Payment and Receipt Vouchers • Cash Tills	Mr. R.M. Gnanarathne Head of Finance
Accounting & Finance	• Functioning of IT servers • E-Financials System • Email Facility	• General Payment and Receipt Vouchers • Bank Statements • E Banking facility credentials • Supplier Payment Register • Financial Statements	Mr. R.M. Gnanarathne Head of Finance
Information Technology	• Functioning of IT servers • E-Financials System • CRIB System • Email Facility • Internet Facility	As per Disaster Recovery Plan	Mr. Athula Senevirathne Manager - IT
Compliance	• Functioning of IT servers • ERP 2 System • I front System	• Financial Statements • CBSL Portal credentials • Weekly Financial Return	Mr. Mangala Wevita Head of Compliance

	• E-Financials System • Email Facility • Internet Facility • Central Bank WAN (Web based) • Central Bank Browser (Web based	Report (Deposit Liabilities) • Monthly Financial Return Report (Classification of Loans & Advances) • Monthly Financial Return Report (Rates of Interest Loans / Deposits) • Loan Advances Report • Loans Secured & Unsecured Large Exposure Report • Loan Age & Maturity Analysis Report	
Human Resources	• Functioning of IT servers • Email Facility • HCM System • Internet Facility • File Server Backup	• Employee attendance, Leave details • Salary & other remuneration details • Bank details • Relevant Finance Dept. Processes	Mr. Sirimal De Silva Manager - HR
BUSINESS PROCESS	SYSTEM SUPPORT REQUIRED / PROCESSES	REQUIRED DOCUMENTATION	PROCESS OWNER

6.1.5 CRITICAL SYSTEMS & MAXIMUM TOLERABLE DOWNTIME - MTD



6.1.5.1 Recovery Point Objective (RPO)

The RPO represents the range of data loss, possible in the event that a disaster affects LCB infrastructure and processes. Based on the available (current) infrastructure, the RPO can be set to15 Minutes. The data replication (uses asynchronous) to update the databases that reside at a DR Site after the primary database has committed a change and with the consideration of primary database performance (Primary application usage), the delay to update the DR Site databases can be set to Maximum 15 Minutes.

6.1.5.2 Recovery Time Objective (RTO)

The RTO is related to the time taken for disaster declaration, BCCP Activation and the time available for the Entity's Disaster Recovery Operational Team to recover data, disrupted systems and resources (System Recovery Time). The estimated RTO is 2 hours and 30 minutes.

6.1.5.3 Work Recovery Time (WRT)

The WRT is associated with the time available for the Disaster Recovery Operational Team and the designated department officials to test and verify the recovered/restored systems prior to releasing the systems (DR Site) to end-users. The network redirection/restoration duration is also considered within the WRT. The estimated WRT is 1 Hour and 30 minutes.

6.1.5.4 Maximum Tolerable Downtime (MTD)

The MTD represents the maximum time that the entity can tolerate without the critical systems recovery time which is RTO and the Work Recovery Time (WRT). MTD = RTO + WRT which is 4 hours.

Business Process	Recovery Time Objectives										
	0-2 Hrs.	4 Hrs.	1 Day	2 Days	3 Days	4 Days	5 Days	2 Weeks	3 Weeks	1 Month	>1 Month
Operations	1	1	1	1	1	1	1	2	2	3	5
Human Resources	-	-	-	-	1	1	1	2	2	2	2
Information Systems	1	1	1	1	2	2	2	2	3	3	3
Compliance	-	-	-	-	1	1	1	1	1	1	1
Administration	-	-	-	-	-	-	-	2	2	2	2
Finance	-	-	-	-	1	1	1	1	2	2	2
Sales & Marketing	-	-	-	-	-	-	-	-	-	1	1
Call Center Operations	-	-	-	-	-	-	-	-	1	2	2
Total Staff	2	2	2	2	6	6	6	10	13	16	18

6.1.6 REQUIRED STAFFING FACILITIES

The following table lists the requirement number of staff to support the initial recovery of key business processes within the entity and the desired time frame within which they are required to be available in a disaster situation.

6.1.7 TABULATION OF A SUMMARY OF BUSINESS PROCESSES TO BE REPLICATED

Critical Business Activity	Priority	Impact of Loss	RTO	RPO
Fixed Deposits:				
Deposit Placements	Very High	Financial Loss Loss of customer satisfaction	08 Hours	02 Hours
Deposit Upliftment's - **Payments on Maturity** - **Premature Withdrawals**	Very High	Loss of customer satisfaction Reputational Loss	08 Hours	02 Hours
Interest Payments	Very High	Loss of customer satisfaction	08 Hours	02 Hours
Renewal of deposits	Very High	Loss of customer satisfaction	08 Hours	02 Hours
Sending reminders/ notice of maturity	Low	Loss of customer satisfaction	02 Weeks	04 Days
Filing and storage of Mandates & other lodgments	High	Loss of crucial information	08 Hours	04 Hours
Responding to Inquiries	High	Loss of customer satisfaction	08 Hours	04 Hours
Issue of FD certificates	Low	Loss of customer satisfaction/customer may consider alternate service providers	02 Weeks	05 Days
Lending / Advances :				
Evaluation of Credibility of facility	Very High	Loss of customer satisfaction	08 Hours	02 Hours
Granting of credit facilities	Very High	Financial Loss	08 Hours	02 Hours
Responding to Customer Inquiries	High	Loss of customer satisfaction/ customer may consider alternate service providers	08 Hours	04 Hours
Making the payments to the agent	High	Loss of satisfaction/ May consider	08 Hours	04 Hours

6.2 Risk Assessment

Risk is exposure to unwanted loss. In terms of Business Continuity, it is the risk of an incident happening which may result in unwanted loss of an asset or delay to operations. Risk Assessment is the systematic identification of all risks, their investigation and grading relevant to each other and to LCB Finance, so that management can be given a clear and full understanding of the risks it faces.

Risk Assessment is an important phase in the development of a Business Contingency & Continuity Plan (BCCP). The aims of Risk Assessment are to:

- Identify the risks that LCB Finance could face;
- Identify essential operations that must be restarted as quickly as possible after a disaster has taken place;
- Re-assess current disaster recovery strategies and established recovery timeframes.
- Simplify decision-making process during a stressful situation.
- Suggest procedural change where necessary.
- Identify legal and regulatory issues related to a business interruption.
- Identify cost-effective measures that could be introduced to prevent risks or lessen their impact, thereby reducing the need for the Incident Control Team (ICT) to be mobilized;
- Provide input for Risk Management.

This has been already conducted from a Confidentiality, Integrity and Availability perspective and is available for viewing at the respective Division.

The objective of the Risk Assessment is to evaluate threats which may potentially disrupt the entity's business activities. The evaluated threats pertain to Natural Disasters, Technical Disasters, Malicious activities, Manmade Disasters.

6.2.1 RISK RATING GUIDELINE

The objective of the Risk Assessment is to evaluate threats which may potentially disrupt the entity's business activities. The evaluated threats pertain to Natural Disasters, Technical Disasters, Malicious activities, Manmade Disasters.

Residual Likelihood	
1 - Rare	Estimated to occur only in exceptional circumstances; probability <10%
2 - Unlikely	Estimated to occur relatively infrequently; probability 10-20%
3 - Moderate	Estimated to occur occasionally; probability 20-50%
4 - Likely	Estimated to occur regularly; probability 50-90%
5 - Almost Certain	Estimated to occur frequently; probability >90%
Impact	

1 – Very Low	No significant impact on any stakeholder, minor non-public criticism by policyholders, no impact on attractiveness of the Company as a business partner, no impact on trust/motivation on employees
2 – Low	Small number of customers/no important corporate clients affected, some media awareness, some negative attention by regulator(s), strong non-public criticism, moderate negative impact on trust/motivation on employees
3 – Medium	Large number of customers/small number of corporate clients affected, public criticism by regulator(s), considerable media awareness, negative perception and as result significant risk of policy lapses, loss of targeted new customers, considerable impact on sensitive business partners
4 – High	Majority of customers/significant number of corporate clients affected, low-scale regulatory action by regulator(s), serious media coverage (cover story), risk of larger number of policy lapses, huge loss of new customers, significant impact on product/service quality, significant loss of attractiveness for major business partners, serious challenge to trust and motivation of majority of mid-management and staff
5 – Very High	Nearly all customers/most important corporate clients affected, very critical articles and cover page media coverage, very high impact on product/service quality, high-scale regulatory action, very huge loss in confidence by mid-management and staff, becomes very unattractive for most important business partners, very high impact on product quality, risk of very large number of policy lapses, very huge loss of new customers
Residual Risk	
1 – 4: Low	Under control at this stage.
5 – 9: Medium	Keep an eye on the exposure. Must regularly assess the Impact and likelihood
10 – 15: High	Either Impact or likelihood of occurrence is high, therefore need to have proper controls in place
16 – 25: Very High	Serious exposure even after controls that are in place as both impact or likelihood of occurrence is high.

SUMMARY – RISK ASSESSMENT MATRIX

Likelihood of occurrence			
High	• Short term or localized disruption to electrical power supplies. • Air conditioning failure		
Medium	• Human error • Programming error	• Water damage • Loss of key individuals • Extended disruption to electrical power supplies. • Interruption to the communications networks	• Fire • Bomb Explosions • Terrorist Attacks
Low	• Utility failure (sewage and water supply) • Smoke damage	• Civil disturbance • Vandalism • Local flooding • Lightning strike	• Complete network interruptions • Complete critical IT systems interruptions
	Low	**Medium**	**High**
	Impact		

6.2.2 ASSET / SCENARIO BASED LEVEL RISK ASSESSMENT

Asset Level Risk Assessment for the most critical systems of the entity establishes the following key factors

- Inherent Vulnerability
- Threat or Exploiting a Vulnerability resulting in Risk
- Impact & Probability of Occurrence

RISK ASSESSMENT

Item No	Threat Name	Threat source	Vulnerability Rating	Likelihood Rating	Impact Rate	Overall Risk Rating
1	Disruption of electrical power supply	Internal / External	Low	High	Medium	High
2	Air conditioning failure	Internal	Low	High	Medium	High
3	Human error	Internal	Medium	Medium	Low	Medium
4	Programming error	Internal	Medium	Medium	Low	Medium
5	Water damage	Internal / External	Low	Medium	Medium	Medium
6	Loss of key individuals	Internal	Low	Medium	Medium	Medium
7	Extended disruption to electrical power supplies	External / Internal	Low	Medium	Medium	Medium
8	Interruption to the communications networks	External / Internal	Medium	Medium	Low	Medium
9	Complete network interruptions	Internal / External	Low	Medium	Medium	Medium
10	Complete critical IT systems interruptions	Internal	Low	Medium	Medium	Medium
11	Fire	Internal / External	Low	Medium	Medium	Medium
12	Bomb Explosions	External	Low	Medium	Medium	Medium
13	Terrorist Attacks	External	Low	Medium	Medium	Medium
14	Utility failure (sewage and water supply)	Internal	Low	Low	Low	Low
15	Smoke damage	Internal	Low	Low	Low	Low
16	Civil disturbance	External	Low	Low	Low	Low
17	Vandalism	External	Low	Low	Low	Low
18	Local flooding	External	Low	Low	Low	Low
19	Lightning strike	External	Low	Low	Low	Low
20	Transportation	External	Low	Low	Low	Low

Refer Annexure 13 for Detailed Risk Assessment

6.3 Scenario Based blueprint for Crisis Management

Based on the threats and vulnerabilities assessment performed for the entity, the impacts for all types of threats and corresponding risks have been mapped to the table below. The chart shows the possible scenarios that could impact the entity in a disaster and the most likely recovery strategy to be adopted by the Business Continuity Team.

Scenario	Facility	Part Facility	IT	Part IT	People	Recovery Strategy
Business as usual	✓	✓	✓	✓	✓	N/A
Primary facility unavailable	▫	▫	✓	✓	✓	Use alternate facility with primary IT and people
Part primary facility unavailable	✓	▫	✓	✓	✓	Use primary site and part of alternate facility
Primary data center unavailable	✓	✓	▫	▫	✓	Use primary site and alternate data center
Part primary data center unavailable	✓	✓	✓	▫	✓	Use primary site and part of alternate IT
Critical people at primary site unavailable	✓	✓	✓	✓	▫	Use back up people from alternate site
Primary facility and primary IT unavailable	▫	▫	▫	▫	✓	Use primary people at alternate facility
All resources at primary site unavailable	▫	▫	▫	▫	▫	Use alternate facility and IT data center

7 Risk Management & Communication

7.1 Call Cascade

The Call Cascade is a mechanism for informing all the staff members of the LCB Finance about the invocation. In the call Cascade, a higher-level staff member is responsible for contacting a group of staff below him,

Important Instructions

The following guidelines should be strictly followed:

- Message should be conveyed effectively by keeping them simple, short and to the point
- Any employee who cannot be contacted must be reported back to the functional Business Continuity Team Leader
- The employee who was unable to contact another member should contact all of the staff under the unreachable member's Cascade
- The functional business continuity team leader should inform the personal and operation team of non – contactable staff
- Periodical attempts should be made to contact unreachable staff until they are reached or satisfactory reasons of unavailability are discovered.
- When a member of the call cascade completes contacting the entire staff listed in the cascade under him, he should inform the business continuity team leader of the completion of the cascade.

Designation/Department	Notification / Contact No.
Deputy General Manager - Business Development and Funds Mobilization	776878000 – EXT. No. 203
Deputy General Manager – Recovery & Operations	773587781 - EXT. No. 234
Deputy General Manager - Credit	760988089 – EXT. No. 245
Deputy General Manager - IT	760988089 – EXT. No. 216
Assistant General Manager - Finance and Strategic Planning	760988089 – EXT. No. 209
Chief Risk Officer	773421215 – EXT. No. 205
Head of Legal	779958148 - EXT. No. 212
Head of Compliance	760988086 – EXT. No. 205
Head of Finance	703738248 – EXT. No. 222
Head of Business Development	703738248 – EXT. No. 222
Manager - IT	779406140 – EXT. No. 216
Manager - IT	766444552 – EXT. No. 217
Assistant Manager - Internal Audit	712841023
Manager - Human Resource	773665131 - EXT. No. 227
Manager - Admin & Operations	772092218 - EXT. No. 204

The following Call Tree Structure would be triggered once disaster is declared. DECLARATION OF DISASTER:

- At Branches : Branch Manager with concurrence of Regional Manager
- At Head Office : DGM with concurrence of BCCP Team. a. Escalation of Disaster:
- At Branches : Branch Manager > Regional Manager > DGM. At Head Office
  : DGM > Executive Director.

7.2 Recovery teams & Responsibilities

LCB Finance recovery organization is a collective group of personnel responsible for maintaining and executing LCB's BCCP. Although the recovery organization is designed for a "worst-case scenario", it is flexible enough to resolve less severe disasters.

The nature of a disaster may indicate specific resources needed for recovery. The nature of disaster and results of the damage assessment shall also indicate the portion(s) of LCB Finance recovery organization to be activated. Regularly scheduled recovery exercises shall increase the effectiveness in the event of a disaster.

The primary duties of recovery teams are as follows:

- Formulate the recovery procedures for the respective area.
- Perform damage assessment.
- Manage recovery activities to protect information assets until normal operations are resumed.
- Assess the appropriate level of disaster with expertise and information, including recommendations for partial or full mobilization of Recovery Teams.
- Accomplish rapid and efficient recovery of critical business processes.
- Take expenditure decisions in the event of a disaster.
- Conduct streamlined reporting of recovery progress from Recovery Teams to Senior Management.

7.2.1 RECOVERY TEAMS

This section provides a description of the teams that will be directly involved in the recovery activities at the time of a contingency. This section lists the personnel, vendors and other parties, who will support the recovery efforts.

As a part of the recovery process, the following teams have a significant role:

- Business Center Manager
- Emergency Management Team
- Local Restoration Team
- Location Response Coordinator

7.2.1.1 Business Center Manager

The Business Center Manager is the highest decision level within the Recovery organization. The Business Center Manager decides the level of disaster to be declared. He relies on the Emergency Management Team to make appropriate decisions regarding the level of disaster. However, he/she reserves the right to exercise the final decision when declaring a disaster and, on the replacement, or restoration of the affected facilities. The Business Center Manager plays a vital role in the recovery process through advice and key decisions.

Name of the Contact Option	Contact Details	
Mr. G.A.M.U.W. Emitiyagoda Manager IT	Work	EXT. No. 216
	Alternate	EXT. No. 217
	Mobile	779406140
	Home Address	284, Balagolle, Kengalle
	Email Address	uditha@lcbfinance.lk

Roles and Responsibilities of BCM

Business Center Manager

Emergency Responsibilities:

- In consultation with other recovery teams, determine whether a disaster should be declared and what Recovery Teams should be activated.
- Assist EMT leader validate priorities throughout the recovery process.
- Assist EMT leader in deciding the level of disaster and mobilization of the Recovery Teams
- Provide necessary approvals for the equipment purchase required for the continuity of operations
- Ensure the clients are informed about the disaster and the time required recovering the process.
- Handle any communication with the media, if need arises.

7.2.1.2 Emergency Management Team [EMT]

The Emergency Management Team (EMT) is responsible for decision making, coordinating the activities in the recovery process, handling legal matters, arranging the finances and handling public relations and media inquiries.

Name of the Contact Option	Contact Details	
Mr. M. J. H. Perera – Chief Risk Officer	Work	205
	Mobile	773421215
	Home Address	No. 05, Base work shop area, Ampara
	Email Address	jayalal@lcbfinance.lk
Mr. W. V. D. M. H. Wevita – Head of Compliance	Work	207
	Mobile	777357134
	Home Address	No.06 Field Mawatha, Kohuwla, Nugegoda.
	Email Address	mangala@lcbfinance.lk
	Work	214

Mr. Oswald Sahabandu – Head of Business Development	Mobile	717694552
	Home Address	582/2/3, Highway Garden, Mahakatuwana, Homagama
	Email Address	oswald@lcbfinance.lk;

Roles and Responsibilities of EMT

Emergency Management Team Leader – Deputy General Manager - Administration & Operations / Operations Manager

Emergency Responsibilities:

- Supervise the initial reaction to the disaster and ensure that organizational property and lives are secured.
- Ensure that the Business Contingency & Continuity Plan has been activated
- Determine to what extent the Recovery Plan will be implemented.
- Initiate recovery process.
- Oversee smooth implementation of the response and recovery section of the plan
- Determine the need for and activate the use of an alternate operation site and other continuity tasks
- Review the damage and notify the appropriate state authorities, communicate with key stakeholders as needed
- Provide important information for distribution
- Inform recovery team members of any changes to situation.
- Provide detailed accounting of the damage to senior management

Emergency Management Team Members

Emergency Responsibilities:

- Distribute the new phone number(s) to all teams and emphasize the use of the phone only for necessary information.
- Arrange the alternate facility to be used to continue operations.
- Start using the Disaster Recovery Logs for all operations.
- Supply senior management and the Help Desk with scheduled updates on status.
- Notify all users of the status of the computer facility.
- Restore files and applications and operate systems at the alternate site.
- Prepare operations schedule at the alternate site.
- Order and install computer hardware necessary for normal processing at permanent location.

7.2.1.3 Local Restoration Team [LRT]

The restoration team should be responsible for getting the alternate site into a working and environment.

Name of the Contact Option	Contact Details	
Mr. M. J. H. Perera	Work	216
	Mobile	777796019
	Home Address	40b, Samanala, Kandy Road, Nittambuwa
	Email Address	vajira@lcbfinance.lk
Mr. R M Gnanarathne – Head of Finance	Work	222
	Mobile	703738248
	Home Address	No.16/6, Grama Sanwardhana Rd, Polwatta, Pannipitiya.
	Email Address	ratnayake@lcbfinance.lk
Mr. Oswald Sahabandu – Head of Business Development	Work	214
	Mobile	717694552
	Home Address	582/2/3, Highway Garden, Mahakatuwana, Homagama
	Email Address	oswald@lcbfinance.lk;

Roles and functioning Responsibilities of LRT

Local Restoration Team Members

Emergency Responsibilities:

Computer operations

- Set up Hardware equipment, data links at the alternate site [or coordinate the above activities provided by the service providers]
- Install operating system software at the alternate site allowing the minimum required operations and internal communications to be restored.
- Obtain the latest backup and restore files at alternate site / connect to the secondary backup.
- Carry out tests to ensure the integrity of the data
- Audit financial files with functional users to ensure recovery process was complete.
- Test critical systems for production processing.
- Monitor controls and security during recovery mode.

Replacement of hardware

- Contact hardware Provider to determine if current hardware is repairable or have to be replaced and make necessary arrangements to replace/ repair hardware.

- Purchase cables, connectors, and other equipment which is required to set up the IT equipment.
- Determine the need for other support equipment: PC's, printers, paper-handling equipment, etc. Order all required equipment.

Supplies

- Prepare list of requirements.
- Contact Providers and arrange for shipment of new supplies

Procurement and Administration

- Provide procurement and administrative support for the recovery activity.
- Provide assistance with purchasing replacement computer, office, or other equipment as required.
- Arrange for shipments of material, supplies, and computer equipment.

Administrative services

- Provide all necessary administrative services, such as the payment for emergency equipment and issuing critical supplies, etc.
- Provide for additional office facilities, including furniture, phones, and office equipment.

7.2.1.4 Location Response Coordinator [LRC]

The Location Response Coordinator is responsible for coordinating the process of moving from the primary site to the alternate site and from the alternate site to the restored primary location.

Name of the Contact Option	Contact Details	
Mr. M. J. H. Perera – Chief Risk Officer	Work	205
	Mobile	773421215
	Home Address	No. 05, Base work shop area, Ampara
	Email Address	jayalal@lcbfinance.lk
Mr. G.A.M.U.W. Emitiyagoda – Manager IT	Work	217
	Mobile	779406140
	Home Address	284, Balagolle, Kengalle
	Email Address	uditha@lcbfinance.lk
Mr. D M W Bandara – Manager Admin	Work	204
	Mobile	772092218
	Home Address	354/B/4, Madapathgama, Gonagoda, Katugasthota
	Email Address	admin@lcbfinance.lk

Roles and Responsibilities of LRC

Location Response Coordinator

Emergency Responsibilities:

- Coordinate the process of relocating from the primary site to the alternate site and moving back to the restored original site
- Coordinating with the Key management team to provide assistance in providing transport to staff to reach the alternate site
- Coordinating with the software/ hardware vendors.

7.2.2 ALTERNATE RESOURCES

In case of risks arising from lack of availability of the designated resources, the following resources back up plan will be enabled for the backup resources to perform the roles of the primary resource.

LCBL will conduct job training of the identified resource during the regular operations.

#	NAME	DESIGNATION / OPERATION	SUCCESSOR/S
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

7.3 Emergency Response Plan

The Emergency Response Plan needs to be activated after reporting of a significant incident which could lead to loss of life and assets. Safety of employees and assets will be ensured in the same order. It also provides a structured means of communicating event status and issues to key personnel and external agencies.

7.3.1 PURPOSE OF EMERGENCY RESPONSE PLAN

To provide a plan for orderly evacuation of LCB Finance and to identify key contacts for emergency notification and to establish the emergency notification list to support the following objectives:

- Minimize loss of life and property.
- Ensure all media communications is routed through Business Center Manager.
- Evacuation of the premises to the safe assembly area as per the emergency evacuation procedures.
- Assembly of key personnel (as required, if possible). Facilitate gathering of information necessary for selecting the appropriate scenario of disaster.
- Immediate notification to key personnel for mobilization of Recovery Teams.

7.3.2 ASSESSING THE COMPLETENESS OF THE EMERGENCY RESPONSE PLAN OF THE BCCP

This Business Contingency & Continuity Plan (BCCP) should be tested and updated regularly to ensure that it is up to date and remain effective. The following checklist was prepared based on input and experiences from disasters happened to entity is a useful guide in assessing and upgrading the BCCP of LCB.

Problem	Responses or potential activities to be adhered to
BC Manager is not available	• Deputies especially for crisis management have to be named beforehand. Experience and local network are key stakes for succession.
Roles and responsibilities uncertain	• Decision makers for all key functions have to be named including deputies • Every key function must have its representative • Measures should be clearly addressed and repeated by the addressee to ensure common sense
Crisis situation is underestimated	• Expect the worst case and consider an escalating procedure • Consider and prepare against potential risk scenarios (civil unrest, manmade risks or natural catastrophe), even if the present situation is stable • Have pre-defined trigger points for actions for those scenarios, you expect to become reality

Decision makers have different knowledge	• Define a single point of contact for all information (in and outbound) • Define meeting procedures (regular meeting frequency, meeting place) for situation updates
Crisis team alerts are not efficient enough	• Predefine meeting facilities for crisis team • Have all crisis team contacts distributed among members • Have an ambitious approach between alert until readiness of the crisis team (convention procedures for business and non-business hours) conduct regular alarm drills check, if an automated alarm system is appropriate
Escalation to Group Crisis Team	• Define information procedure and when to inform or escalate to Parent Company
Looting and vandalism of unoccupied buildings	• Have established channels to security authorities • Harden doors and windows against breakup • Lock doors and all-important subsidiaries • Increase number of guards • Consider a hardened and locked shelter inside to protect confidential or expensive assets • Avoid storage of flammable objects (waste, fuel, gas etc.) in surrounding • Shut central supply installations (e.g. water, elevators, electricity) • Consider remotely watched and recorded CCTV and remotely watched alarm systems (if available) • Conduct regular checks

Fire	Check readiness of firefighting equipment
Claiming damage	Take pictures of damage
Some specific telephone services may be disrupted locally	• Have different phone cards from various providers available • Ensure that phones are ready for use (power, charger, payments…)
When should the employees be informed and to whom to escalation if situation worsens	• Define information procedure and when to escalate to Group • Whom to inform: BCM Officer or Group Crisis Committee
Staff has to be reached at any time, also out of business hours	• Have private numbers of staff available. Collect landline and mobile numbers. Collect email, if appropriate • Define call trees through departments • Use SMS, if calls are not answered

Internet and mobiles not working	• Use landlines • Define meeting points
Staff does not know how to react after an incident	• Send CEO message to staff through available channels including priorities and next steps • Prepare hotline/answering machine or dark side on Internet
Key personnel not defined or available	• Know your critical staff/decision makers and their availability
Clients do not know, how to get in contact with LCBI, if agents or offices cannot be reached	Use all available means of communication(media, internet, hardcopies, phone announcements, agents e.g.) to give clients Contacts
Key customers need special service	Ensure, that our key account managers proactively contact our key customers
Call Center is not available	Backup for call center
Inquires	Ensure 24h availability of claims and inquires handling by phone, if phones are working if not, define backup procedures, e.g. enhance direct contacts to walk-in, clients in office or on site, if appropriate
Many different parties may ask for information or support	• Set priorities (first own interest, than 3rdparties) • Ensure steering of external communication by communication professionals only
Internet, landlines and mobiles not working	• Use satellite phones • Ensure serviceability of satellite phones
Public traffic may be disrupted	• Built a car and motorcycle pool • Define a responsible person for managing the pool • Define, who is allowed to use the cars • Ensure, that cars are always fueled up • Check usability of motorcycles for short to medium distances

A curfew prohibits or limits traffic	• Some employees should stay at office • Remote access to systems can solve this, if prepared
Chaos caused by unprepared mass evacuation	• Have an evacuation plan prepare evacuation before officially announced • Define clear triggers for evacuation
Escape routes not known or prepared	• Pre-arrange escape routes to airports, seaports or borders for foreign staff (if any) • Check routes in advance of real evacuation by driving the

Main office cannot be reached or used	• Backup location must be fully equipped to fulfill its role right from the beginning • Backup must have enough space to coverall important functions defined in the BCCP • Backup should be equipped to house some staff permanently (supplies, sleeping accommodation, sanitary installation)
Backup location too far away of most employees residential area	• Ensure that backup location is available and can be reached by your staff in case of local disaster hits the area • As alternate solution ensure that trained staff is available at backup location
Backup location too close to main office and therefore not useable	• Backup should be established at an area out of expectable risks, e.g. natural catastrophe shell, out of financial district, flooding zone etc.
Main office and backup location cannot be used	• Check, if alternate sites can be used as a backup • Check, if a provisional backup can be setup (e.g. hotel or branch-office) • Check, if a neighborhood country can fulfill backup-role
Access to client data not permanent available	• Have a system to collect all relevant data for cross-check, until access to IT is reinstalled
IT backups in country not safe enough	Consider backups in OEs in a Virtual/ Cloud environment
Office space cannot be used, but IT is available	Ensure that all key staff has remote access
Cash not available	Ensure, that there is a certain amount of cash available (safe storage)
Fuel not available	• Emergency fuel should held in storage for emergency power as well as for cars. • Prefer Diesel for both.
Medical aid difficult to get	• Have first-aid packages at hand • Prepare, that most used drugs are on hand(discuss with company or contracted medic)
Clean drinking water or food supplies difficult to get	• Have more water in storage than used in a few days • Evaluate to store or organize supplies needed

7.3.3 HEALTH CHECK - REQUIRED FOR SUCCESSFUL EMERGENCY EVACUATION

Fire Alarm and Extinguishers – Checks should be performed twice a year to ensure that they are in good working condition.

7.3.4 EMERGENCY PROCEDURES & EVACUATION PROCESSES

- Identify the fire/ other cause for emergency evacuation
- Inform the nearest ERT leader/ member.
- Pick up fire extinguisher and attack fire or take action as per specific incident necessitating this emergency evacuation. The security guards have also been detailed for this job.
- ERT Leader will reach the spot of fire, or any place where an event has occurred necessitating evacuation of personnel.
- ERT leader declares the emergency;
- Summon fire brigade/ contact hospital/ inform blood entity – ERT Leader
- Guide evacuation, check cloak room & toilets – By ERT members
- Assist mentally and physically challenged personnel, walk one after another, don't' run.
- Don't panic; walk quickly.
- Switch off A/C, lift, gas etc. – By Facilities/ Maintenance personnel
- All the evacuated people should assemble in the safety assembly area and ERT members according to their floors should do head count and report should be given to the ERT leader.
- If it is a fire drill then the observers should note down timing and fill up the drill check list
- [Refer Annexure 9 – fire drill check list]
- All clear signal
- De- briefing by ERT.

7.3.4.1 Fire Evacuation Policy & Procedure

Standard:

Our employees are our biggest asset. Therefore, their health & safety is of primary concern to us. We will make all efforts to ensure that we provide a safe work environment to all our employees.

Scope:

All employees of LCB and visitors to the LCB building.

The Procedure:

a. All occupants except the designated Fire Team members, on hearing the Fire Alarm, will immediately evacuate the building, and proceed to the Assembly Area

b. All employees should immediately switch off the main computer power switch and leave the building through the nearest fire exits. Do not panic.

c. Ensure that the Elevators are not used.

d. All occupants must ensure that they can reach their Primary or Alternate means of escape in not more than 2 to 3 minutes.

e. All occupants must know the route to and the location of their respective Assembly Area

f. All evacuees will proceed, in a quick and orderly manner, to the nearest and safest Fire Exit.

g. Any employee outside their relevant department does not need to return to the department again.

h. The Staff on arriving at their Assembly Areas will assemble by their respective Departments to facilitate a "Head Count." by one of the fire team members.

i. The visitors on arriving at the Assembly Area to assemble separately in order to facilitate a "Head Count"

j. Fire brigade should be informed of same.

k. No person is to enter the premises other than authorized persons, until the alarm has been switched off and it has to be clearly indicated by the Manager Administration/Human Resource Manager that it is safe to do so.

Fire Preparedness

a. Pay serious attention to fire drill procedures, which should be conducted regularly in all facilities.

b. Take your pre assigned emergency-related duties seriously and go over your instructions frequently.

c. Those employees located near fire doors should ensure that there is always clear access to those doors. If passage is blocked, please notify ECT as and then so the area can be cleared.

7.3.4.2 Simple First Aid Procedures

In case of a medical emergency at LCBL, please follow these procedures:

a. First Aid Kit is located at the <location>

b. Keep calm

c. To ensure adequate breathing, open and maintain the victim's airway by gently tilting head back. If victim is not breathing, immediately begin mouth to mouth resuscitation.

d. Check and periodically recheck the victim's carotid pulse in the neck, using two fingers. (If pulse is not present, immediately begin CPR (Cardio-Pulmonary Resuscitation)

e. Stop all obvious bleeding by applying direct pressure over the wound with your hand (if available use a clean cloth or bandage)

f. Do not remove victim, unless a hazard is present. Keep the victim in a quiet, comfortable position.

g. Loosen all tight clothing (collars, ties, belts etc.)

h. Keep victim warm - do not induce sweating

i. Give no fluids - except very small sips of water, only if requested by victim.

j. Elevate victim's legs slightly, unless an injury is present on the chest or head.

k. Comfort and reassure the victim constantly.

l. Notify your supervisor as soon as possible

7.3.4.3 Practice drills

The practice emergency evacuation drills are done as per following requirements –

1. A minimum of one drill to be performed half yearly.
2. Of the two annual drills, one should be conducted unannounced to the employees.

In case of fire evacuation training drills the following additional roles to be performed –

1. Designated persons to check that all emergency lights are working.
2. How long the alarm sounded.
3. Whether alarm was heard in all areas.

7.3.4.4 Natural Disaster

Severe Windstorm, Tornado or Hurricane

- Clear books, papers, and desktop items that are near windows and secure them in drawers.
- Place heavy objects, and telephones under desks.
- Close all doors at entrance to the building. Leave interior doors open to prevent atmospheric pressure problems
- Assist in moving computer equipment under desks or to interior stairwells, if possible. If windows are broken, stairwells will offer some form of protection.
- Follow emergency evacuation procedure, if severe weather is already in progress.

Earthquake

- Do not attempt evacuation during an earthquake. The safest place and most structurally secure place are under any doorway. Crouch and hold both sides of the doorway.
- If you are unable to get to a doorway, take cover under a desk or other sturdy object or against a wall in the core of the building.
- Protect your head. Duck, cover and hold.
- Stay away from windows, book cases, filing cabinets and anything else that could tip or shatter.
- Use water from water coolers only.
- Do not move a seriously injured person, unless he/she is in immediate danger.
- Do not use matches, and open flame, or turn on any electrical appliances. This might trigger a gas explosion.
- If you keep shoes at your desk, wear them to protect your feet from debris and broken glass.
- If the phone system is functioning, use it for emergency calls only.
- Be prepared for aftershocks, weather you are still in the building or moving to a new location.
- Listen for instruction from emergency personnel over the public address system.

7.3.4.5 Explosion or Bomb Threat

Explosion

- Either follow instructions to evacuate the building, or take cover under sturdy furniture and away from moveable objects that could fall (bookshelves, filing cabinet, etc.)

- Make an effort to stay away from windows and glass.
- Move cross-wind if possible to avoid upwind and downwind toxic fumes
- Evacuate immediately. Do not take time to gather personal belongings
- Help administer first aid or help a disabled person get out with the assistances of a colleague
- Do not return to the building unless official clearance has been given

Bomb Threat

- Take it seriously and assume it is intended. Notify building management as well as your supervisor
- Inform the police of the threat and provide all information requested. They are likely to send a search team and may require directions. They will request details of the threat, the voice, the gender, approximate age of the caller. Be prepared to answer such questions.
- Do not touch anything that looks suspicious. Make sure authorities know about any suspicious objects so they can be investigated.
- Proceed with evacuation instructions as per the public address system, or evacuate the building as per instructions.

7.3.4.6 Thief, Armed Intruder or Assailant

Thief

If you witness a theft in the office:

- Take note of the person's distinguished characteristics (clothes, height, weight, etc.)
- Contact building security using the Emergency Numbers listed
- Do not try to stop the intruder yourself, as he or she may be armed.
- Inform the reception area to expect police or security guards and direct them appropriately.
- Quietly ensure that the surrounded area is cleared of personnel in case violence ensues.

Armed Intruder

If confronted by an armed intruder:

- Remain calm and do not behave belligerently, as this may challenge the intruder and result in violence.
- Try not to show excessive fear and follow the intruder's directions carefully.
- Attempt to calm anyone who becomes hysterical in order to keep the intruder's anxiety level down.

- Comply fully with the intruder's wishes to the extent that you can protect yourself and others. Hand over jewels, money, or goods, make any telephone calls commanded, and do whatever is required to diminish confrontation and violence.
- Comply if you are told to lie on the floor or move with another room
- Study the intruder as closely as possible to note distinguishing characteristics. If masked, hands, distinctive voice or accent, type of weapon, etc.
- If it is safe when the suspect leaves, and you are in the position to do so, inform the police of the incident
- Notify building security
- Administer first aid or help any injured person as necessary, including contacting ambulance.

Prevention

Always, emphasis is placed on preventive measures therefore;

- If you see anyone walking around the premises who you don't recognize, and who is not
- accompanied by a colleague, approach and ask if you can help them.
- Call security and find out if anyone was admitted without a badge.
- If no one was admitted without a badge, approach and ask if you can help.
- Even if the guest mentions a colleague by name, it is possible that the person read it on a nameplate. It is safe to call the colleague and/or assistant to make sure the person is a guest. It is also important to contact ECT.
- The best way to avoid embarrassment is to escort your guests around the office yourself, or have an assistant or colleagues accompany them.
- Lock valuables in your desk. Always keep safes, vaults, strongboxes, or similar devices locked, particularly when unattended.
- Never divulge the combination to safes or vaults to anyone for ease. Do not leave such information where it can be found or easily deciphered.
- Anyone wishing to remove property from the building should have a signed letter from a tenant authorizing such removal

7.3.5 EMERGENCY NUMBERS

NAME OF THE ENTITY	CONTACT NUMBERS
Police Head Quarters	011 241111-2327711
Police Station - Kohuwala	011 2852621
OIC-Police Station - Kohuwala	011 2853929 0718591669
Police Emergency Service	011 2433333 - 2421988
Police Emergency Numbers	118 -119
Bomb Disposal	011 2434251
Army Head Quarters	011 2437078 - 2432682
Navy Head Quarters	011 2421151 - 2421152/85
Air Force Head Quarters	011 2441044
Fire Brigade	011 2422222
Ceylon Electricity Board	011 2466660 - 4617575
General Hospital	011 2691111
Kalubovila Hospital	011 2832950
Ambulance Service	011 2422222
Sri Lanka Telecom	011 2329711 - 2333111
Nawaloka Hospital	011 2544444 - 7
Durdans Hospital	011 2575555 - 5410000

7.4 Recovery Plan

Recovery is the return to the pre-emergency condition. Performing the critical activities as soon as possible after a critical incident is the primary focus.

7.4.1 RECOVERY PHASES

PHASE	DESCRIPTION
Initial Response	As soon as an emergency situation occurs, the on-site personnel shall contact the appropriate Response Team who will take the necessary steps to minimize property damage and increase the safety of the staff of LCB. This is typically the period between notification of a disaster situation to the ERT Leader and the decision by Senior Management for declaration of a disaster. Mobilization of recovery teams happens as part of the first response. **Important Note:** In the event of a disaster having even the smallest possibility of threat to the life and health of employees, the priority of that point in time is to evacuate ALL employees from the building to safe assembly area.

Preparation for alternate site operations	In the event of a major disaster where the original site cannot be used to carry out day to day operations, the designated alternate site could be used. The Head of IT/ IT Officer and the CEO will coordinate with the relevant software/ hardware vendors to obtain the required support.
Operations at recovery location	This is the period from notification to ERT Leader, initiation of initial assessment of the situation and if necessary, declaration of disaster. Prompt action during this phase is essential for timely and efficient mobilization of Recovery Teams. Once the hardware and software are installed, latest backups are restored and the functionality of the systems is tested and operational, the production processing is moved from the original site to the alternate site. Certain operations will be carried out until the system is ready to be used.
Restoration/ migration	This is the period during which plans for restoring or relocating the affected facilities are implemented, and business functions are migrated from the recovery location back to the restored or relocated building. This phase normally begins while the operations at recovery location are underway.

7.4.2 RECOVERY PLAN FOR MINOR DAMAGE

During minor damage Processing can be resumed in a short time with no special recovery procedure and downtime is less than half-a-day. Damage could include system failure, electrical power shortage, and hardware equipment failure.

<u>Electrical Power Shortage / Power Failure</u>

In the event of a power shortage / failure, acceptance of Deposits, completed application forms and other relevant documents with reference to Lease and Hire purchase facilities will be carried out as usual. Manual receipts shall be issued to customers and Cheques for lease and hire purchase facilities shall be issued to the agents.

Manual registers with reference to the above facilities will be maintained. Once recovered from the power failure, and when the system is available, the integrity of the database and application will be determined by the IT officer. All the manual works carried out will be updated to the system.

If the power outage remains for more than 4 hours, the management will consider the necessity of relocating at the alternate site.

IT systems Failure / hardware failure

In the event of IT systems Failure, the IT officer/ Executive IT will coordinate with the software/ hardware vendor to restore the system subsequently after verifying the integrity of the application and database. (To identify data losses due to the sudden system/ hardware failures)

Note: Refer Disaster Recovery Plan for Recovery Times

Evacuation of the Facility

The primary site will be evacuated if the building is unsafe or operations cannot be carried out. Employees will be constantly trained in emergency procedures and will know evacuation routes from various parts of the building.

7.4.3 RECOVERY PLAN FOR MAJOR DISASTERS

During major disasters processing cannot be resumed in the original site and recovery teams will be called to direct restoration of normal operations at alternate site. Acceptable downtime is two-six days. Damage could include floods, fire.

Flood

Floods may cause temporary service outage/ system downtime or permanent hardware failure. Currently, the servers are placed on racks however in the event of a flood, the following steps are followed to minimize/ eliminate damage:

If the Water Damage Exposure Has Affected the Computer Hardware:

(1) Switch off hardware equipment and disconnect from the power lines

(2) Notify the IT Officer who will be responsible in arranging another storage location for servers

(3) If required [based on the damage], the IT officer will coordinate with the hardware vendor to obtain support for replacement of hardware equipment

(4) In the event that a server is replaced, the IT officer will coordinate with the software/

hardware vendors and Executive IT to verify that all files are properly restored.

Establishment of Full Recovery at Backup Site

Copies of software/ Operating System software [in the form of CDs & DVDs] are bundled together and stored [at the place where backups are stored] along with the daily backups of the system.

Communications network and other equipment are in place to be fully operational.

Arrangements with the Operational System software / hardware, Telephone Company and other communications Providers for services and delivery and installation of temporary equipment are available [Refer agreements].

7.4.4 RELOCATING AT ALTERNATE SITES & RECOVERY OF SYSTEMS

Process	Action	Responsible Person
Evacuating the Original Site	Coordinate and supervise orderly evacuation of the original site Guide staff to reach the emergency assembly point until the alternate site is ready for use. Distribute the new phone number(s) to all teams and emphasize the use of the phone only for necessary information.	Operations & Recovery Officer
Purchasing/ installing furniture and preparation of the alternate site to be used to commence operations	Based on the damage assessment, determine which furniture needs to be purchased. Contact furniture suppliers to order/ transport and for installation of office furniture. Office furniture at the original site which could be used at the alternate site shall be brought to the alternate site. Coordinate the activities related to the transportation of office furniture to the alternate site Assign duties to office assistants Arrange transport to deliver the office furniture Once office furniture is delivered, supervise the installation of furniture Contact electrician to attend to activities with reference to power supply/ installation of A/C Check and arrange other facilities for staff. E.g. water Contact telecommunication service providers to obtain PABX/ Telephone lines and telephones	Manager – IT / IT Officer Administration Assistant Administration Assistant Administration Assistant Administration Assistant Administration Assistant Administration Assistant IT Office

Identifying, purchasing and installing hardware to expedite system recovery	CEO and Executive IT shall carry out a damage assessment to identify which hardware equipment's need to be replaced / purchased.	CEO & Executive IT
	Information with reference to hardware under warranty and vendors shall be obtained from the IT Inventory list attached as an annexure to this BCCP	Manager – IT
	For hardware equipment under maintenance agreements/ warranty: Executive IT shall contact the hardware vendor for replacement of hardware equipment.	Manager – IT
	For hardware equipment that are not covered by a maintenance agreement: obtain approval from the Managing Director for the purchase of new equipment.	Manager –IT
	A list of hardware equipment vendors is attached as an annexure [Annexure 5]; Coordinate with the above vendors to obtain new hardware equipment.	Manager – IT IT Officer
	Arrange transport to bring hardware equipment that could be used at the alternate site	Manager – IT
	Coordinate the above tasks and assign duties to officer assistants/ other staff	Manager –IT
	Cabling and other requirements should be determined by the Executive IT and should be purchased or shipped to the alternate site from the original site [if moving to an alternate site]	Manager – IT
	The IT officer shall install hardware or vendor support	IT Officer

	could be obtained for installing hardware. Operating system software's [if required] is included in the CD Bundle maintained offsite. This bundle should be brought to the alternate site	IT Officer
Setting up PCs, and other hardware at the alternate site	Once the PCs and other hardware equipment are transported to the alternate site, the IT officer, with the help of vendor or other employees shall set up the hardware. Install operating system software and other software required for operations.	IT officer IT officer
Coordinating with the software vendor to install/ test software systems at the recovery site/ primary site (in case of a system failure)	Maintenance agreements are in place [maintained by the CEO] with the software vendors for the installation of software in the event of a disaster. Executive IT will coordinate with the system providers to obtain services related to restoration of the system. Contact details of the vendor are included in the "external contact list" attached. If the systems should be installed at the alternate site, the software vendor shall be notified about the location	Executive IT Alternate Person: IT Office Executive – I Manager – IT
Restoring systems, installing applications on the backup systems	Set up and test new servers at alternate site Install the system in new server	System Engineers System used

Monitoring application performance and integrity of the database	Once the system is installed and the database is linked; check the integrity of the system. The following reports will be generated and checked for completeness : • Debtors • Creditors • Customer Account Balances • NPA Reports • Arrears Lists Entity Reconciliation Reports	Operational users from each division
Re-establishing user/ system network, providing network and access to systems	Call SLT to obtain support for internet links Re-establish network and provide access to the systems	IT Officer Network engineers
Installing communications hardware at recovery site (or coordinating with the vendor to install the above)	Coordinate with vendor to establish data links and telephone lines	IT Office
Locate, coordinate, and installation of user terminals, printers, photocopy machines and other equipment	Determine which equipment needs to be purchased and which equipment needs to be transported to the alternate site from the original site A list of IT assets along with their details such as warranty details and vendor information's are attached as an annexure [Annexure 6] to this BCCP. Call respective vendors to purchase new equipment if required. Arrange transport and assign the task of transporting equipment from original site to the alternate site to an officer Transport required equipment from the original site	CEO Manager – Procurement/ Admin Manager – Procurement/ Admin Manager – Procurement/ Admin Senior Executive

Retrieving data from offsite storage	A backup of the database is stored offsite, at the CEO's Residence, Located at <Address> The backup should be picked up from the above location and should be taken to the alternate site/ original site as required	CEO Alternate Person : Executive IT
Coordinating/ arranging transport for users to reach the alternate site	Coordinate the orderly evacuation of the damaged original site Call cab service to provide transport for users to reach the alternate site Contact details of the cab service providers are included in the external contacts list	Manager – Administration Manager – Sales Manager – Sales
Supplying office stationery	A list of Office stationery requirements is attached [Annexure 11] in this BCCP. Call office stationery suppliers to obtain required office supplies.	Manager – Administration
Arranging payments/ finances for employee relocation expenses at the recovery facility	Arrange payments for relocation expenses.	Manager - Finance
Coordinating systems use and employee work schedules	After reaching the alternate site, gather all employees and distribute employee work schedules and provide instructions to employees Please refer recovery strategies	Manager – Fixed Deposits Manager – Finance

Obtaining, packaging and shipping media and records (manual registers) to the alternate site	Manual registers are stored in the CEO's room and cabinets.	Manager – Finance
	Obtain the above documents and transport the documents to the alternate site	Manager – Finance
	Contact vendors to obtain stocks of FD certificates, KYC forms other documents required.	Manager – Finance
	A stock of FD Certificates is stored in a fire-proof safe at the original site.	Manager – Finance
	If the fire-proof safe can be accessed, transport the FD certificate stocks to the alternate site	Manager – Finance
	If the fire-proof safe cannot be accessed or the FD certificates are destroyed, contact FD certificate press to obtain a stock of FD certificates.	Manager – Finance
	Lease, Hire Purchase and FD files shall be brought to the alternate site.	Manager – Finance
	Arrange transport to send the file from the original site to the alternate site.	Manager – Finance
	Assign office assistants to transport file and to Store files in a separate location at the alternate site	Manager - Finance

8 Risk Awareness & Testing

The Management will identify the teams in order to train the team to adhere to appropriate emergency response activities.

The testing of the BCCP will be carried out in conjunction with the training exercises such as checklist reviews, walk-through, table-top and a full interruption exercise.

A Comprehensive training on BCCP will be provided to the relevant team members and awareness created on their roles in the implementation/operation of the BCCP i.e. all individuals will be trained to adhere to their respective specified roles efficiently and effectively in order to assure the accuracy of the team responsibilities and resumption o.

Audit & Compliance will monitor the BCCP exercise during the testing period. In addition, the audit team will review the test plans and the outcome of the testing (test results).

8.1 BCCP Testing Policy

The entity will conduct a business-process-wide testing (Critical Systems & Interdependencies/Systems) integrated with BIA and Risk Assessment.

8.2 BCCP Testing Methodologies & Gathering Test Results

The entity will ensure that the testing of Critical systems and test results will be gathered and documented prior to the review of same by the management. The testing process will be carried out under the supervision of the BCM, which will address functionality and connectivity of the business processes and its capacity. In addition, the following concerns will be strictly observed:

1. Systems applicability, accessibility & accuracy
2. Validation of RPO & RTO
3. Roles & Responsibilities of the Officials
4. Coordination with Interdependencies
5. Identify gaps in BCCP Documentation and Planning
6. Effectiveness of the plan under different scenarios
7. Validation of the resources required (Human, Technology, etc.) to meet BC Objectives
8. Evaluation of weaknesses & strengths

The BCM & the Team will initially conduct a "checklist review" in order to check whether the BC/DR Plan addresses the entirety of the procedures & critical systems.

Secondly, the "Table-top exercise" will be conducted to assign responsibilities to each member and their reaction in a crisis scenario. During this exercise, each step of the BC/DR plan will be walked- through and be marked as performed. A report will be documented including the responsibilities assigned to each member.

A "Walk through simulation test" will be conducted after the "Table Top exercise". In this testing, assigned members perform their emergency response. In this phase, the actual recovery procedure (Systems Recovery) will not be initiated.

The final testing phase will be "Full-Interruption exercise". IN this phase, BC/DR Plan for all critical systems and the interdependencies/systems will be initiated. The BCM shall obtain the approval of the BOD through the Executive IT prior to performing this exercise. In addition, all officials and stakeholders should be informed in advance of having obtaining such approval. All assigned members will participate in this phase. The detailed test results will be gathered and documented. The generated test results document will be reviewed by the BCM and Audit.

8.3 BCCP Test Results Documentation

Once the testing (Full-Interruption Exercise) is completed, the Operations Manager will take the responsibility to document the test results. The following information shall be included in the document.

- Test Date
- An Executive Summary with the comparison of between the test objectives and test results such as estimated RTO/MTD and actual RTO/MTD
- Evaluation of RPO
- Identified Problems and Issues (i.e. Resources requirement, interdependencies)
- Deviations in the procedures & plans
- Strengths & weaknesses in the BCCP
- Internal Audit Review

9 Acceptance & Maintenance

9.1 Review and Approval of Test Results

The BCCP test results documentation will be forwarded to the Board through the Executive IT along with Management's recommendation (Based on test results). The recommendations may result in modifications to BCCP and other areas such as IT Infrastructure, Resources (Human, Training) and the areas which are not included in the BCCP.

The test results and the recommendation will be reviewed by the Board. The Board will provide their consent to the BCM & team to proceed with the recommendations or to proceed with the recommendation or to explore alternatives.

9.2 Business Impact Analysis (BIA) Maintenance

The BIA will be reviewed by the Entity's Board & Management teams with the BCCP annually. The updated BIA will reflect significant changes in IT Systems, Technical Advancements, Entity's operations and Audit recommendations during the testing process. A copy of the updated BIA will be maintained at primary site, as well as at the DR Operational Site.

9.3 Review & Update of BCCP Document

The LCB will follow a change control process for managing the BCCP and periodic reviews will be conducted in order to update the BCCP. The Management will assess whether the plan needs any change and of any change is made to the plan, they will conduct a BCCP Training and Testing to ensure that the change adequately satisfies all requirements.

In addition, it will be ensured that all officials and parties involved in the BCCP are well informed of the changes in the BCCP.

The Board approved BCCP document will be made official.

Board Paper No : 2024 / 811 / 09 / S Date : 27 / 09 / 2024

Board Meeting No : 77

IT DISASTER RECOVERY PLAN

Policy Owner : Chief Risk Officer

BIRMC Presented Date : 14 / 05 / 2024

Board Approved Date : 27 / 09 / 2024

Version : 01

COPYRIGHT

CONFIDENTIALITY

Information contained herein is the property of LCB Finance. This document and the LCB Finance procedure and other associated documents it describes as confidential in nature and all parties should keep all information contained herein confidential and on no account should the information, in whole or in part, be disclosed or disseminated to any third party without the express written permission of the Management of LCB Finance. The document may be used or copied only in the accordance with the terms of such Agreement. Neither this document nor the LCB Finance procedures and other associated documents be used, sold, transferred, copied, translated, transmitted or reproduced in any form or by any means, electronic or mechanical for any purpose, in whole or in part other than in accordance with the terms of such agreement, or otherwise without prior consent of the LCB Finance.

The information contained in this document is subject to change in accordance to the Document Change Control.

DOCUMENT DETAILS

Area	Description
Title	DISASTER RECOVERY PLAN (DRP)
Date	27 / 09 / 2024
Version	FINAL
Owner	INFORMATION TECHNOLOGY DIVISION

DOCUMENT CHANGE CONTROL

DATE	REASON / CHANGE	CHANGE AUTHOR	RECCOMENDED BY

BOARD APPROVAL

DATE OF APPROVAL: 27 / 09 / 2024

DISASTER RECOVERY PLAN

10 DRP General Information & Guiding Principles

10.1 Introduction

The Disaster Recovery Plan supports business operations and provisioning of IT services to ensure availability and recovery of critical business processes.

The Disaster Recovery plan defines the IT disaster recovery processes, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure in the event of an actual emergency situation.

10.2 Disaster Recovery Policy Statement

- A formal Business Impact Analysis shall be carried out to determine the requirements for the disaster recovery plan.
- The company shall develop the IT disaster recovery plan covering all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- Disaster recovery tests should be carried out with the participation of the Key Disaster recovery team members to ensure that the plan can be implemented in emergency situations/ the event of a disaster.
- Responsibilities of staff members related to the recovery process should be clearly defined.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

10.3 Objectives

- To develop, test and document a well-structured plan which will ensure quick and effective resumption of the business.
- Ensure safety and security of people
- To ensure that all employees fully understand their duties in implementing a disaster recovery plan
- To minimize the loss and damage caused by disasters
- To ensure that proposed contingency arrangements are cost-effective

11 Acceptance & Maintenance of DRP

11.1 UPDATING THE PLAN

Changes to the plan should be controlled and a version history should be maintained. Whenever changes are made to the plan, the plan should be fully tested.

11.2 PLAN DOCUMENTATION STORAGE

Copies of this Plan, soft copies and hard copies will be stored in secure locations to be defined by the company. Board of Directors and each member of senior management will be issued a copy of this plan to be filed at his/her premises.

Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a softcopy and a hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

12 Key Details & Contact Information

12.1 MEMBERS OF THE DISASTER RECOVERY TEAM

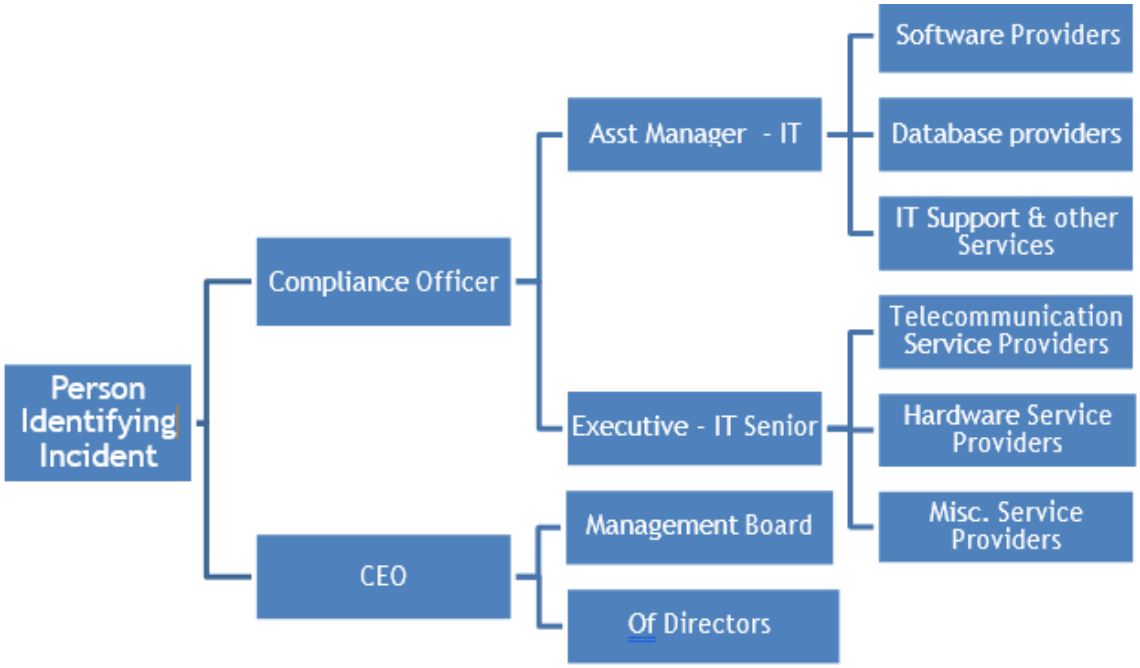
Name of the Contact Option	Contact Details	
Mr. K G Leelananda CEO	Work	200
	Mobile	777724761
	Home Address	564, Isuru Uyana, Baaswatta, Narawala, Poddala
	Email Address	leelananda@lcbfinance.lk
Mr. K K Wannige – AGM Finance & Strategic Planning	Work	209
	Mobile	760988089
	Home Address	No. 12/546, Himburawa Road, Galle
	Email Address	kelum@lcbfinance.lk
Mr. M. J. H. Perera – Chief Risk Officer	Work	205
	Mobile	773421215
	Home Address	No. 05, Base work shop area, Ampara
	Email Address	jayalal@lcbfinance.lk
T M N J Fernando – GDM Credit	Work	245
	Mobile	771859996
	Home Address	No. 2/2, Palliya Road, Diyalagoda, Maggona.

	Email Address	nishantha@lcbfinance.lk

12.2 External Contact List

Services	Vendor	Address	Contact	Mobile	Telephone	Email
SLT Voice & Data Links	SLT Mobitel PLC	Lotus Rd, Colombo 10	Lahiru Kularathna	710119642	112864314	lahirus@slt.com.lk
Secondary Data Link & Voice Package	Dialog Axiata PLC	475 Union Pl, Colombo 2	Malinda Wijesinghe	777331662	777678700	Malinda.Wijesinghe@dialog.lk
End Point Security	AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 2	Damitha Anuradha	775071078	117439208	damitha@acsysnetworks.com
HP Servers / SAN	VS Information Systems (Pvt) Ltd	7 Sulaiman Terrace, Colombo 005	Dithika Jayakody	773448335	112038568	dithika@vsis.lk
NAS	DMS Electronics (Pvt) Ltd	Pagoda Rd, Sri Jayawardenepura Kotte	Dhanushka Madushanka	773959577	114732100	dhanushka.madushanka@dmselectronics.com
Backup Appliance	Ultrium Technologies (Pvt) Ltd	RVH9+5F3, Dehiwala-Mount Lavinia	Lahiru Kariyawasam	768203620	115882933	lahiru@ultryum.com
Server Room Maintenance	Assidua technologies (Pvt) ltd	149 Galle Rd, Dehiwala-Mount Lavinia	Nadeepa Silva	767634666	112710088	nadeep@assiduasolutions.com
Branch Centralize UPS	Asiacom Engineering Services (Pvt) Ltd	No.123, Bauddhaloka Mawatha, Colombo 04	Manjula Madurapperuma	765788944	117444125	manjula@asiacom.lk

12.3 NOTIFICATION CALLING TREE



In the event of a Disaster: The Disaster Recovery Team shall meet at the designated assembly point. The CEO shall coordinate all activities. The Executive IT alongside the IT Personnel shall coordinate with the vendors to obtain assistance in recovering critical systems, infrastructure and data.

12.3.1 IT Recovery Team Leader - (HOIT) & It Consultant (Vendor)

Responsible for the technical recovery and operations of the computer facilities at the DR site. The primary task is to ensure the resumption of computing services following a disaster declaration by activating interim processing for critical operations at the DR site.

12.3.2 Other Functional Team Leaders

Responsible for resuming operations of their units upon restoration of computing facilities at the DRS.

13 Information Security

13.1 Introduction

Allocation of adequate resources, effective arrangements for promoting good information security practice and establishment of a secure environment is set out in this section in order to control the business risk associated with information system

This section covers five distinct aspects of information security:

i) IT Facilities - Networks and Computer Installation
ii) Critical Business Developments
iii) End User Environment

iv) System Development
v) Security Management

Many key business processes of LCB depend on IT applications, making the Critical Business Applications central to the design of this DRP. Computer Installation and Networks provide the underlying infrastructure on which the Business Applications run. The End User Environment covers the arrangements associated with protecting corporate and desktop applications, which are used by individuals to process information and support business processes. Systems Development deals with how new applications are created or outsourced and Security Management addresses high-level direction and control.

13.2 Management Commitment

The Board of Directors and Chief Executive Officer are committed to:

Complying with the requirements of the Public Debt Department and Payments and Settlements Department of the Central Entity of Sri Lanka, treating information security as a critical business issue.

The principles applied by the Chief Executive Officer in terms of DRP include:

- Assuming ultimate responsibility for the internal control of the organization;
- Ensuring that controls over information and systems are proportionate to risk.
- Assigning responsibility for identifying, classifying and safeguarding information and systems to individuals;
- Approving access to information and systems in accordance with explicit criteria.

13.3 High Level Control – Communication Teams

A Local Restoration Team has been appointed to co-ordinate information security activity across LCB. This Working Group is responsible for:

- Approving information security policies and standards / procedures
- Monitoring information security performance (e.g. analyzing the current security status, handling information security incidents and costs)
- Approving and prioritizing information security improvement activity
- Ensuring information security is addressed in LCB's IT planning process

13.4 Security Awareness

Security awareness is the extent to which members of staff understand the importance of information security, the level of security required by LCB and their individual security responsibilities.

a. Staff has been given guidelines on:

- the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
- the importance of complying with information security policies and applying associated standards / procedures

- Their personal responsibilities for information security (e.g. reporting actual and suspected information security incidents).

b. Security awareness is being provided with information security education/training by using various techniques and by supplying specialized security awareness material.

13.5 Security Education & Training

Staff members are educated/ trained in how to run systems correctly and how to adopt information security controls, with a view to equipping them to fulfill their information security responsibilities.

a) Information Security Awareness Training is included in the staff induction process depending on the work areas due to be assigned to the new recruit.
b) Education/Training has been provided to ensure that computer installations and networks are run correctly and the required security controls are applied effectively.

13.6 Insure Assets against Risks & Hazards

All assets held in the name of LCB will be adequately insured. LCB Finance has taken out insurance policies to cover hazards to facilities commonly used by the group companies.

13.7 Information Classification

Information is classified as follows:

- Public disclosures such as press releases, publishing of annual reports, employment advertisement, product brochures, and public website are to be authorized by – The Chief Executive Officer.
- Internal documents – organization charts, various policies of LCB, Manuals of operations, training materials- will be used by the user(s) on their business need under the supervision of departmental heads.
- Confidential information – Personal details of customers and their investment records, statements and confirmations.
- Restricted information – Customer data base, Financial & contractual records, Board papers, pricing information, strategic plans, marketing plans, Personnel data, Salaries & Emoluments, Risk Management Reports, etc.

13.8 Ownership of IT Assets

Each IT asset, (hardware, software, application or data) has a named Custodian who is responsible for the information security of that asset and the respective Head of Departments is responsible for the assets allocated for the use of his/her department.

13.9 Protection against IT Disruptions

13.9.1 Computer Viruses

The risk of virus infection has been reduced by warning users not to:

- install software from untrusted sources

- open untrusted attachments
- click on hyperlinks within e-mails or documents
- attempt to manually resolve malware problems.

13.9.1.1 Anti - Virus Software

LCB has presently installed a powerful anti-virus solution. Anti-virus software has been installed on systems that are susceptible to viruses (e.g. those that have access to the Internet), including relevant servers (e.g. servers that are at risk from viruses, such as file and print servers, application servers, web servers and database servers), desktop computers, laptop computers.

Anti-virus software has been configured to be active at all times.

Configure On-delivery E-mail Scanner to detect viruses and Trojans, clean attachments, move attachments to a folder or delete if cleaning fails and/or delete e-mail and notify user.

Configure scheduled Auto Update tasks to keep product, scanning engine and patches up-to date. Configure On-Access Scanner to provide continuous, real-time scanning of the following as they are accessed.

- Executable files (including macro files in desktop software)
- Protected files (e.g. compressed or password-protected files)
- Removable computer storage media (e.g. USB storage devices)
- Network traffic entering the corporate network (including e-mail and downloads from the Internet)
- Computer memory

Configure on-Demand Scan to scan files and processes including subfolders and boot sectors for unwanted programs, viruses and Trojans and clean/delete if threat is found.

Configure Alerts specifying the following actions to be taken when detection occurs.

- Provide a notification when suspected malware is identified (e.g. by producing an event log entry and providing an alert)
- Quarantine files suspected to contain malware (e.g. for further investigation)
- Remove the malware and any associated files or reset system settings
- Ensure that important settings cannot be disabled or functionality minimized.

13.9.1.2 Specialist Technical Support

Executive IT ensures that:

- Anti-virus software has been installed in all servers, desktop and laptop computers and configured appropriately
- updates are applied within defined timescales
- Emergency procedures are in place to deal with a virus-related information security incident.

In case of Detection of Viruses/Virus Attacks, users should inform LCB-IT who in turn should notify the technical support provider and mobilize their services with respect to Cleanup/restoration of computers.

13.9.2 Intrusion Prevention

LCB operates with VLAN segments for its back office and internet/email networks which run on different IP ranges. The VLAN segments are connected to the central firewall system with a Unified Threat Management (UTM). The facilities available are:

- Anti-virus Protection (AV)
- Intrusion Prevention (IPS)
- Anti-spam
- Firewall Protection

13.10 Critical Business Applications

Critical business applications - By recognizing the business impact of a loss of confidentiality, integrity or availability of information, LCB has established the level of importance of each application. This provides the basis for identifying information risks and determining the level of protection required to keep information risks within acceptable limits.

13.11 Confidentiality Requirements

Unauthorized disclosure of information associated with the application will result in an adverse business impact on LCB in terms of loss of competitiveness, loss of management control and breach of operating standards.

It can also have a customer-related impact in terms of loss of clients, loss of confidence by key institutions and damage to its reputation. As such, it is pertinent to document and agree the confidentiality requirements of the application. There is a need for information to be kept secret or private within a predetermined group.

13.12 Integrity Requirements

The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the application is significant. There is a need for the information to be valid, accurate and complete. Therefore, it is prudent to document and agree the integrity requirements (the need) of the application.

13.13 Availability Requirements

The business impact of business information stored in or processed by the application being unavailable for any length of time has been assessed and it has been agreed that the critical timescale of the application (i.e. the timescale beyond which an outage is unacceptable to LCB is - two (2) hours.

13.14 Recovery Time Objectives & Recovery Point Objectives of Critical Systems

LCB is a financial institution that it is reliant on the e-Financials Systems for transaction processing and for accounting purposes. LCB has defined the Recovery Time Objectives (RTOs) and the Recovery Point Objectives (RPOs) of the critical systems described above.

CRITICAL SYSTEM	FUNCTION	RTO	RPO
e Financials System	Core Banking (GL, Central, Savings, FD, Loan, Gold Loan, Foreign Exchange)	2 Hours 30 Minutes	15 Minutes

13.15 Back-Up & Restoration Arrangements of Critical Systems

13.15.1 E-FINANCIAL SYSTEM

The technology architecture of the Core Banking System are maintained by the software vendor – Scienter Technologies, the back-up and recovery procedures of the system have been documented below.

13.15.1.1 General Backup Procedure :

HOT Backup on Backup Server (Location: Onsite)

Backing up of files to the HOT backup server is transparent to users, using batch files which are scheduled to run on a pre-defined time interval.

13.15.1.2 Backup Restoration Testing

HOT Backup recovery is tested by IT-Manager once a week.

b. On-line Backup to DR Server

Installation and configuration of the on-line backup to the DR server was carried out by IT-Manager (Systems) and IT Consultant.

Data is transferred from the live server to the HOT backup server by running a script file at pre- determined intervals within a LAN and archives are stored in a specific folder. Archive files are transferred thereafter through an extended Point to Point Data connection from the HOT backup server to the server located at the DRS by running a script at pre-defined time intervals.

Recovering systems on DR server following the crash of the live server and HOT back-up server due to an OS and/or Hardware failure LCB-IT shall transfer files backed up on the desktop computer located at the DRS to the DR server at least once during a working day. The IT Team shall also restore systems on the DR server by following "Backup Procedure for (Off-Site) - at least once a week.

13.15.2 BACK-UP ARRANGEMENTS FOR WORKING FILES, DESKTOP APPLICATIONS & OTHER PHYSICAL DOCUMENTS

Working files and desktop applications of users have been documented and backed-up and copied to the server at the DRS.

13.15.3 GENERAL BACKUP STRATEGY

Key business processes and the agreed backup strategy for each are listed below. This strategy entails the maintenance of a full back-ups onsite and offsite.

Key Business Process	Backup Strategy
IT Operations	Offsite data storage facility
Tech Support – Hardware	Support provided by the Vendor
Tech Support – Software	Support provided by the Vendor
Email	Support provided by the Vendor
Operations	Offsite data storage facility
Disaster Recovery	Offsite data storage facility
Finance	Offsite data storage facility
Web Site	Support provided by the Vendor

13.15.4 Computer Installations

Computer installations support all main business applications and safeguarding them is a key priority. Since the same information security principles apply to any computer installation (irrespective of where, or on what scale or types of computer it takes) a common standard of good practice for information security has been applied.

13.15.5 Installation Management

13.15.5.1 Roles & Responsibilities

IT Executive is responsible for evaluating and recommending the purchase of required IT assets in consultation with the IT Consultant and ensuring that delivery is in line with the agreed specification. He is also responsible for supervision of all computer installations carried out by vendors.

13.15.5.2 Service Agreements

- Computer Hardware

LCB has procured the hardware from various Service Providers. Assistant Manager - IT is responsible for monitoring if personnel from service provider call over to carry out the routine service of computer hardware. In the event that the routine visits are not carried out, the LRT should be notified.

If any problems are encountered by users with the computer hardware assigned for their use, they should inform LCB - IT, who in turn should report the incident to the hardware provider. LCB - IT should record all remedial maintenance visits and action taken in the prescribed form.

- **Computer Software**

LCB has entered into a software maintenance agreement with Scienter which covers the e Financials System.

(Please refer Maintenance Agreement with the stated entities for more details)

13.15.5.3 Asset Management

- **Computer Hardware**

All computer hardware has a named custodian who is responsible for the security of that asset and the respective Head of Department is held responsible the assets allocated for the use of their department.

Users are not allowed to install software on LCB's property without explicit permission from LCB -IT and BCCP.

- **Data Communications devices and methods**

All data communication devices have a named custodian who is responsible for the security of that asset and the respective Head of Department is held responsible for the assets allocated for use of their department.

13.16 Live Environment

13.16.1 INSTALLATION & DESIGN

a. Installation design:

Takes account of user requirements and is consistent with other installations used by the organization and is able to cope with foreseeable developments in the organization's use of IT (e.g. growth projections)

b. Key components of the installation are protected by:

- Segregating critical business applications from other business applications and information.
- Storing source code with an acceptable Escrow agent and restricting access to authorized individuals
- Segregating different types of software and information (e.g. by storing them in separate directories)

13.16.2 SECURITY EVENT LOGGING

a. Security event log management includes setting policy, defining roles and responsibilities, ensuring the availability of relevant resources and guidance on the frequency and content of reports.

b. The following security event logs are available in the System

- Error Log
- Unauthorized Login Attempts Log

- Authorized Login Attempts Log
- Password Expiry Check Report
- Log of Changes done to User Accounts

13.16.3 WORKSTATION PROTECTION

a. Workstations (i.e. Desktop computers and Laptop computers) connected to systems are:

- Purchased from reliable suppliers (i.e. those with a proven track record of supplying robust and resilient equipment)
- Tested prior to use
- Supported by maintenance agreements
- Provided with standard configuration (e.g. running a standard operating system, standard applications and/or common communication software)

b. Workstations are protected by:

- Access control mechanisms
- Access to the workstation is restricted to the named custodian by use of passwords which are disclosed to the respective Heads of Departments
- Up-to-date malware protection software
- Automatic time-out after a set period of inactivity
- Restrictions on use of removable storage media -can be used on selective basis with prior approval of Compliance Officer/ CEO. Such media must also be fully virus checked before being used on LCB's equipment.

c. Workstations that can connect to the Internet are protected by:

- Using web browsers with a standard, secure configuration
- Applying updates to web browser software
- Using firewalls – Cyber Roam

13.17 Hazard Protection

a. The main server room is protected by

- Keeping it free from intrinsic fire hazards (such as paper or chemicals)
- A fire detection system
- Device to maintain room temperature

b. Fire alarms are monitored continuously, tested regularly and serviced in accordance with manufacturer specifications

c. The impact of hazards are minimized by:

- Locating hand-held fire extinguishers so that minor incidents can be tackled without delay
- Training staff in the use of fire extinguishers and other emergency/safety equipment and in emergency evacuation procedures
- Protecting computer equipment against damage from environmental hazards (e.g. smoke, dust, vibration, electrical interference, food and drink)

- Monitoring and protecting the temperature and humidity of computer rooms in accordance with equipment manufacturer recommendations

13.18 Power Supplies

a) The power supply to critical computer equipment is protected by using uninterruptible power supply (UPS) devices
b) Providing back-up generators (supplied with adequate quantities of fuel) in case of extended power failure
c) Emergency equipment (E.g. UPS equipment and back-up generators) are serviced in accordance with manufacturer recommendation and tested regularly

13.19 Physical Access

a. Physical access to the computer installation has been restricted to authorized individuals by

- Installing a finger-print access control system at the main server room and locks in their areas.
- Employing security guards

b. Identification labels have been attached to equipment owned by LCB. (E.g. Desktop computers, laptop computers etc.)

c. Visitors to the installation are :

- Permitted access only for/to defined and authorized purposes/areas
- Monitored by recording arrival time and departure time
- Supervised at all times

d. Individuals are required to obtain written approval before leaving the premises with computer equipment (e.g. servers, workstations, network devices and printers etc.)

14 Disaster Management

The entity views Business Continuity & Disaster Recovery Planning as a culture to be embraced by all staff and the process has been integrated with the day- to-day operations. The business recovery procedures have taken into consideration, the nature, magnitude and complexity of operations to, establish a sufficient, robust and consistent level of resilience.

It defines all IT related actions to be taken in order to ensure the continuity of critical key business operations. A disaster can be any event that disrupts the normal operations and services of the company.

14.1 LIST OF EVENTS THAT CAN BE DECLARED AS DISASTERS

- Fire
- Flood
- Electrical Power failure/ shortages
- Loss of communication network services
- IT system failure
- Natural Disasters – Tsunamis / Cyclones

Likelihood of occurrence	Low	Medium	High
High	• Short term or localized disruption to electrical power supplies. • Air conditioning failure		
Medium	• Human error • Programming error	• Water damage • Loss of key individuals • Extended disruption to electrical power supplies. • Interruption to the communications networks	• Fire • Bomb Explosions • Terrorist Attacks
Low	• Utility failure (sewage and water supply) • Smoke damage	• Civil disturbance • Vandalism • Local flooding • Lightning strike	• Complete network interruptions • Complete critical IT systems interruptions
		Impact	

14.2 IT EMERGENCY EVENTS

- Virus Attacks
- Theft of Data
- Hacking
- Loss of Data
- Power Failure
- Sabotage / Fraud
- Hardware failure

15 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:
Calamities or Disasters on a Large Scale

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor Interruption

POTENTIAL DISASTER		PROBABILITY RATING	BUSINESS IMPACT	REMEDY
Natural Disaster	Flood	5	1	Insurance Coverage
Natural Disaster	Fire / Explosions	3	1	Insurance Coverage
Technology Disruption	Electrical power Failure / shortage	2	1	Power Generator
Technology Disruption	Loss of communications network services	4	4	Service Provider assistance
Technology Disruption	IT system failure	4	1	Obtain vendor support
Natural Disaster	Tsunami	5	1	-
Technology Disruption	Malware Attacks	3	2	Obtain vendor support
Technology Disruption	Termination of Service by the vendor	4	3	Escrow agreements
Disruption due to Human Activity	Terrorist Attack	5	1	-
Natural Disaster	Cyclones	5	1	Insurance Coverage
Disruption due to Human Activity	Theft or Vandalism	4	2	Insurance Coverage
Disruption due to Human Activity	Restricted Access to Premises	3	1	Relocate to DR Site / Alternate Location
Disruption due to Human Activity	Loss or Illness of Key Staff	2	2	Training of Alternate personnel to take over responsibilities
Reputational Crisis	Loss of Goodwill	5	1	-
Strategic Risk	Tightening of Regulations / High Risk Ventures	4	1	Diversification of Portfolio / Products

16 Emergency Response

Notification of a disaster or a disruption of operations requires prompt action by responsible personnel to minimize the financial, legal, and other risks arising from such disruptions. This section gives the required guidelines in a disaster.

16.1 RECEIVE NOTIFICATION

The BCM will be notified immediately of any emergency or potential emergency by the building management or building security staff or any other authorized person.

- Get the identity of the caller and the contact number
- Question the caller to get a good description of the situation
- Identify if any emergency or prevention steps have already been taken
- Authenticate the caller and deduce the seriousness of the situation
- Decide on the next course of action - conduct preliminary assessment, advice
- BCM to declare disaster

16.2 CONDUCT PRELIMINARY ASSESSMENT

The EMT should conduct a preliminary assessment to ascertain the following:

Estimated time to recover facilities

Estimated time to be operational

Need to activate the DRS

16.3 REPORT INITIAL FINDINGS TO BCM

The EMT will submit a written report to the BCM within one hour of notification, if the impact of the crisis cannot be ascertained immediately.

16.4 PARTICIPATE IN DECISION TO ACTIVATE RECOVERY PLAN

If the BCM perceives that a disaster would be declared, then he/she should place the recovery team leaders on alert. This will enable the team to be mobilized quickly should the activation notice be executed. The BCM and LRT should assemble within the hour to make a decision regarding the activation of the recovery plan. Should the findings be unclear, the BCM may be required to look for alternatives or gather more information. When a decision is made, this team will deliberate on the appropriate recovery strategy to be adopted.

16.5 DECLARATION OF DISASTER

16.5.1 DRS Activating

When an incident occurs the BCM should notified immediately and instruct he in turn should instruct to notify and thus activate the DRS Disaster Recovery Team (DRT). The DRT will then decide the extent to which the DRP must be invoked.

Responsibilities include:

- Responding immediately to a potential disaster and call emergency services
- Assessing the extent of the disaster and its impact on the business, data center, etc.
- Deciding which elements of the DR Plan should be activated
- Establishing and manage disaster recovery team to maintain vital services and return to normal operation
- Ensuring employees are notified and allocate responsibilities and activities as required.

The DRT shall,

- Establish facilities for an emergency level of service within 2.0 business hour
- Restore key services within 4.0 business hours of the incident
- Recover to business as usual within 8.0 to 24.0 hours after the incident

16.5.2 Activate Teams

BCM will contact the team leaders and instruct them to mobilize their respective Teams. Clear directions must be given to avoid confusion and misunderstandings.

16.5.3 Notify Central Entity of Sri Lanka & Other Stake-Holders

BCM should instruct the respective recovery team leaders to notify the Central Entity of Sri Lanka, clients, counterparties, vendors and suppliers that LCB has declared a disaster and shifted operations to the DRS.

16.5.4 Activate Security at Affected Area

Should the entire or part of the premises be exposed to the public or non-authorized people, it is advisable to cordon off the area place and security guards to prevent stealing, pilfering or further damage to the premises. Accordingly, BRC should instruct Manager – Administration to secure the premises with 24-hour security.

16.5.5 Resumption of Critical Business Functions

This section addresses the steps and procedures that need to be taken to restore or resume critical business functions and recover vital transaction information that may be lost or missing.

17 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

17.1 DR Site Location

The DR Site is located at No.155, High Level Road, Maharagama.

17.2 Frequency of Testing

LCB will work from the DRS in order to test the complete Disaster Recovery Plan, in **May** and **November** each year.

In May and November each year LCB will test the eFinancials System alongside Network Connectivity by executing transactions on a selective basis.

17.3 Test Report Forms

Each functional team leader will submit a report on a prescribed format to the EMT on completion of the test runs. The EMT will prepare a summary report to the BCM & BOD highlighting the short comings identified by the functional team leaders and any remedial action taken.

17.4 Reverting To Primary Site After Test Runs At DRS

Members of the Operations and Finance Teams will revert to the Primary Site and record all transactions for the day in the Live Server by referring to source data, consequent to which LCB - IT should verify that all transactions and processes have been updated in the Live Server.

17.5 System Recovery Times & Systems Recovery Points

to tests carried out, actual System Recovery Times and System Recovery Points have Consequent been quantified separately for the critical systems based on the back-up and restoration procedures adopted.

Critical System	Function	Scale of Disruption	Recovery Strategy	System Recovery Time	System Recover Point
E Financials System	Investor Registration and service solution for fund operations	Failure of Live Server at Primary Site	Recovery System on the Cloud Back-up and upload to the existing network	3 Hours	15 Minutes
		Failure of Live Server and network at Primary Site Or Complete disaster / disruption at Primary Site	Revert to DRS. Recovery Systems on DR Server using data backed up in DR server and achieves copied from the back-up at the Primary Site to the PC at DRS	3 Hours	15 Minutes

17.6 Functional Restoration & Data Re-Synchronization

17.6.1 RECOVER SYSTEMS ON SERVER LOCATED AT DRS

BCM should instruct LCB - IT to recover the systems on the server located at the DRS using the archives stored in the DR server and desktop computer at the DRS.

17.6.2 DATA RE-SYNCHRONIZATION

In case of a disruption at the Primary Site, systems can be restored up to the entry recorded 15 minutes prior to the event in the Live Server. If the PC on which facsimile messages are stored could be salvaged, transactions may be entered to the system from there onwards. BRC should instruct EMT to send a communiqué to the stakeholders requesting them to re-direct the relevant parties to the DRS by facsimile.

SERVER	Database server
PRODUCTION SERVER	Location: LCB Head Office Server Model: HPE ProLiant DL360 Gen10 8SFF Operating System: Windows Server 2019 Stander Edition CPUs: Intel Xeon-Silver 421Q (2.2GHz/10-core/85W) Memory: 64GB Dual Rank x4 DDR4-2933 Total Disk: 300GB SAS 12G Enterprise 10K SFF (2.5in) System Serial DNS Entry: 10.10.1.10 IP Address: 192.168.10.1 and 10.10.1.50 Storage HPE MSA 2050 SAN Dual Controller SFF Storage HPE MSA 1.8TB 12G SAS 10K SFF (2.5in) 512e Enterprise Hard Drive HPE MSA 16Gb Short Wave Fiber Channel SFP+ 4-pack Transceiver
DR SITE SERVER	

17.7 Disaster Recovery Plan for the Available Systems & Infrastructure

KEY CONTACTS	
Hardware Vendor	V S Information Systems (Pvt) Limited
System Owners	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04. Tel: 011 2598555
Database Owner	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04.
Application Owners	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04.

BACKUP STRATEGY FOR CORE-BANKING SYSTEM	
Daily	System end of day backup takes automatically Databases – Destinity Lease, Destinity_Scienter, Lease These are moved to E:\EOD_Backups folder in database server. Microfinance database backups taken are automatically moved to E:\MFBackup folder in database server Those backups are full backups in Databases and can be restored any time. Finally, those backups are move to separate NAS drive and it located in new building.
Monthly	Before the End of The Month, the system takes backups from every database automatically and move copies to the NAS drive

Recovery Procedures for Individual Network Elements

Network Element	Type of Loss /Damage	Recovery Procedures
Database Server	Total loss of single DB server	Purchase replacement server from HP. Contact V S Information Systems (Pvt) Ltd and request engineer for system rebuild under the silver support contract (011 2038568) Re-store the server mirror from DR site
	Hard disc failure	Identify failed hard drive – indicator on RAID controller Contact V S Information Systems (Pvt) Ltd to arrange shipment of replacement drive (011 2038568) HP staff to hot swap hard drive on arriva

	Other hardware failure	Contact V S Information Systems (Pvt) Ltd to arrange for hardware engineer to attend – same day (011 2038568) HP engineer to replace faulty part. Restart system
	Software failure	Contact V S Information Systems (Pvt) Ltd and request engineer for system rebuild under the silver support contract (0112038568)
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server First Contact Esna Allied Enterprises to check the generator issue, if not contact the Lanka Electricity Board to check the issue.
	Total loss	Purchase replacement server from HP

IT SERVICE PROVIDER CONTACTS	
V S Information Systems (Pvt) Ltd	+94 112038568
Mr. Dithika Jayakody	+94 77 344 8335
Scienter Technology (Pvt)Ltd	+94 112598555
Mr. Dineth (Scienter)	+94 712220038
Mr. Irwin L. Costa	+94 718731262

SERVER Application Server

PRODUCTION SERVER	Location: LCB Head Office Server Model: HPE ProLiant DL360 Gen10 8SFF Operating System: Windows Server 2019 Stander Edition CPUs: Intel Xeon-Silver 421Q (2.2GHz/10-core/85W) Memory: 64GB Dual Rank x4 DDR4-2933 Total Disk: 300GB SAS 12G Enterprise 10K SFF (2.5in) **System Serial #** DNS Entry: 10.10.1.10 IP Address: 192.168.10.1 and 10.10.1.50 **Storage** HPE MSA 2050 SAN Dual Controller SFF Storage HPE MSA 1.8TB 12G SAS 10K SFF (2.5in) 512e Enterprise Hard **Drive** HPE MSA 16Gb Short Wave Fiber Channel SFP+ 4-pack Transceiver
HOT SITE SERVER	

KEY CONTACTS	
Hardware Vendor	V S Information Systems (Pvt) Limited
System Owners	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04. Tel: +94112598555
Database Owner	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04.
Application Owners	Scienter Technology (Pvt) Ltd, No.302, Galle Road, Colombo 04.

Network Element	Type of Loss /Damage	Recovery Procedures
Application Server	Total loss of Application Server	Purchase replacement server from HP.

		Contact V S Information Systems (Pvt) Ltd and request engineer for system rebuild under the silver support contract (+94 112038568) Re-store the server mirror from DR site
	Hard disc failure	Identify failed hard drive – indicator on RAID controller Contact V S Information Systems (Pvt) Ltd to arrange shipment of replacement drive (+94112038568) HP staff to hot swap hard drive on arriva
	Other hardware failure	Contact V S Information Systems (Pvt) Ltd to arrange for hardware engineer to attend – same day (+94112038568) HP engineer to replace faulty part. Restart system
	Software failure	Contact V S Information Systems (Pvt) Ltd and request engineer for system rebuild under the silver support contract (+94112038568)
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server First Contact Esna Allied Enterprises to check the generator issue, if not

		contact the Lanka Electricity Board to check the issue.
	Total loss	Purchase replacement server from HP

1. Disaster Recovery Plan for Firewall

SYSTEM	Network Security system
EQUIPMENT	**Location: LCB Head Office** **Device Type: Firewall** **Model No.: FortiGate 100E** **System Serial #: FG100ETK18011308** **DNS Entry: 10.10.1.10 / 10.10.1.11** **IP Address: 192.168.10.1**

KEY CONTACTS	
Hardware Vendor	ACSYS NETWORKS PRIVATE LIMITED, LEVEL 12, PARKLAND BUILDING, # 33, PARK ST, COLOMBO 02, TEL: +94117439208
System Owners	
Software Vendors	

BACKUP STRATEGY	
Daily	Get total database backup in one a week and upload to the forti cloud (SAND BOX)

Network Element	Type of Loss /Damage	Recovery Procedures
Hardware Firewall	Total loss Firewall	Purchase replacement Firewall from Fortinet. Contact Mr Damitha Anuradha support contract (+94 775071078 / +94 117 439208) Restore the most recent database backup form cloud and Restart system
	Other hardware failure	Contact Mr Damitha Anuradha to arrange for hardware engineer to attend – same day (+94775071078 / +94 117 439 208) Fortinet to replace faulty part. Restart system
	Software failure	ACSYS NETWORKS PRIVATE LIMITEDAND REQUEST ENGINEER FOR SYSTEM REBUILD (+94 775071078 / +94 117 439 208)
	Power failure	Ensure UPS is operating correctly If power is not restored within 5 minutes shutdown server and await power restore When power is restored, restart server First Contact Esna Allied Enterprises to check the generator issue, if not contact the
	Total loss	Purchase replacement Firewall from Fortinet.

KEY CONTACTS	
AcSys Networks Private Limited	+94 117 439 208
Damitha Anuradha	+94 775071078

ANNEXURE 1- OFFICE LOCATIONS AND LOCATION HEAD

	Location	Location Head	Contact	Email Address	Location Address
1	Galle Branch	L I Pushpakumara	(+94) 91 2 247222	mgrgalle@lcbfinance.lk	No 119, Wakwalla Road, Galle
2	Karandeniya Branch	K B G I Nishan	(+94) 91 2 290255	mgrkarandeniya@lcbfinance.lk	Elpitiya Road, Maha Edanda, Karandeniya
3	Matara Branch	T M Priyankara	(+94) 41 2 250017	mgrmatara@lcbfinance.lk	No 68, Anagarika Dharmapala Mawatha, Matara
4	Pelawaththa Branch	L D R Perera	(+94) 34 2 284810	mgrpelawatta@lcbfinance.lk	No, 07 Mathugama Road Pelawaththa
5	Kohuwala Branch	P H N J Dias	(+94) 11 28 25 404	mgrkohuwala@lcbfinance.lk	No 76, S De S Jayasinghe Mawatha, Kohuwala Nugegoda
6	Rathgama Branch	S S Heenatigala	(+94) 91 2 268160	mgrrathgama@lcbfinance.lk	No. 622, Devenigoda, Rathgama
7	Karapitiya Branch	M A K S Gunarathna	(+94) 91 2 245810	mgrkarapitiya@lcbfinance.lk	No 249/d, Golden Range, Karapitiya.
8	Negombo Branch	K G D C Gamage	(+94) 31 2 226565	mgrnegombo@lcbfinance.lk	No 615, Colombo Road, Kurana, Katunayaka.
9	Kuliyapitiya Branch	T C Maduragoda	(+94) 37 2 286280	mgrkuliyapitiya@lcbfinance.lk	No 33, Hettipola Road, Kuliyapitiya.
10	Tangalle Branch	M R Weerarathna	(+94) 47 2 244000	mgrtangalle@lcbfinance.lk	No 157, Hambanthota Road, Tangalle.
11	Deiyandara Branch	S P T H Subasinghe	(+94) 41 2 268958	mgrdeiyandara@lcbfinance.lk	Opposite Deiyandara Hospital, Deiyandara

12	Akuressa Branch	D M Chaminda Kumara	(+94) 41 2 280090	mgrakuressa@lcbfinance.lk	No 66/A, Matara Road, Akuressa.
13	Embilipitiya Branch	A K A D V Sithara	(+94) 47 2 261505	mgrembilipitiya@lcbfinance.lk	No 47, Pallewela, Embilipitiya.
14	Maharagama Branch	K H M I Madushanka	(+94) 11 2 840244	mgrmaharagama@lcbfinance.lk	No 155, High level Road, Maharagama.
15	Kegalle Branch	L A S S S Liyanarachchi	(+94) 35 2 233383	mgrkegalle@lcbfinance.lk	No. 44, Main Street, Kegalle.
16	Tissamaharama Branch	H K G Priyankara	(+94) 47 2 259044	mgrtissa@lcbfinance.lk	No. 472 Opposite the clock tower Debarawewa, Tissamaharama.
17	Walasmulla Branch	S A S Rukshan	(+94) 472247067	mgrwalasmulla@lcbfinance.lk	No 70, Beliatta Road, Walasmulla.
18	Agunukolapelessa Branch	G V N Sandaruwani	(+94) 472228313	mgragunukolapelessa@lcbfinance.lk	No 439/11, Ranna Road, Angunakolapelessa
19	Gampaha Branch	A K V Perera	(+94) 332238062	mgrgampaha@lcbfinance.lk	No 57A, Bauddhaloka Mawatha, Gampaha.
20	Minuwangoda Branch	M P Pushpakumara	(94)112285804	mgrminuwangoda@lcbfinance.lk	No. 194, Veyangoda Road, Minuwangoda.

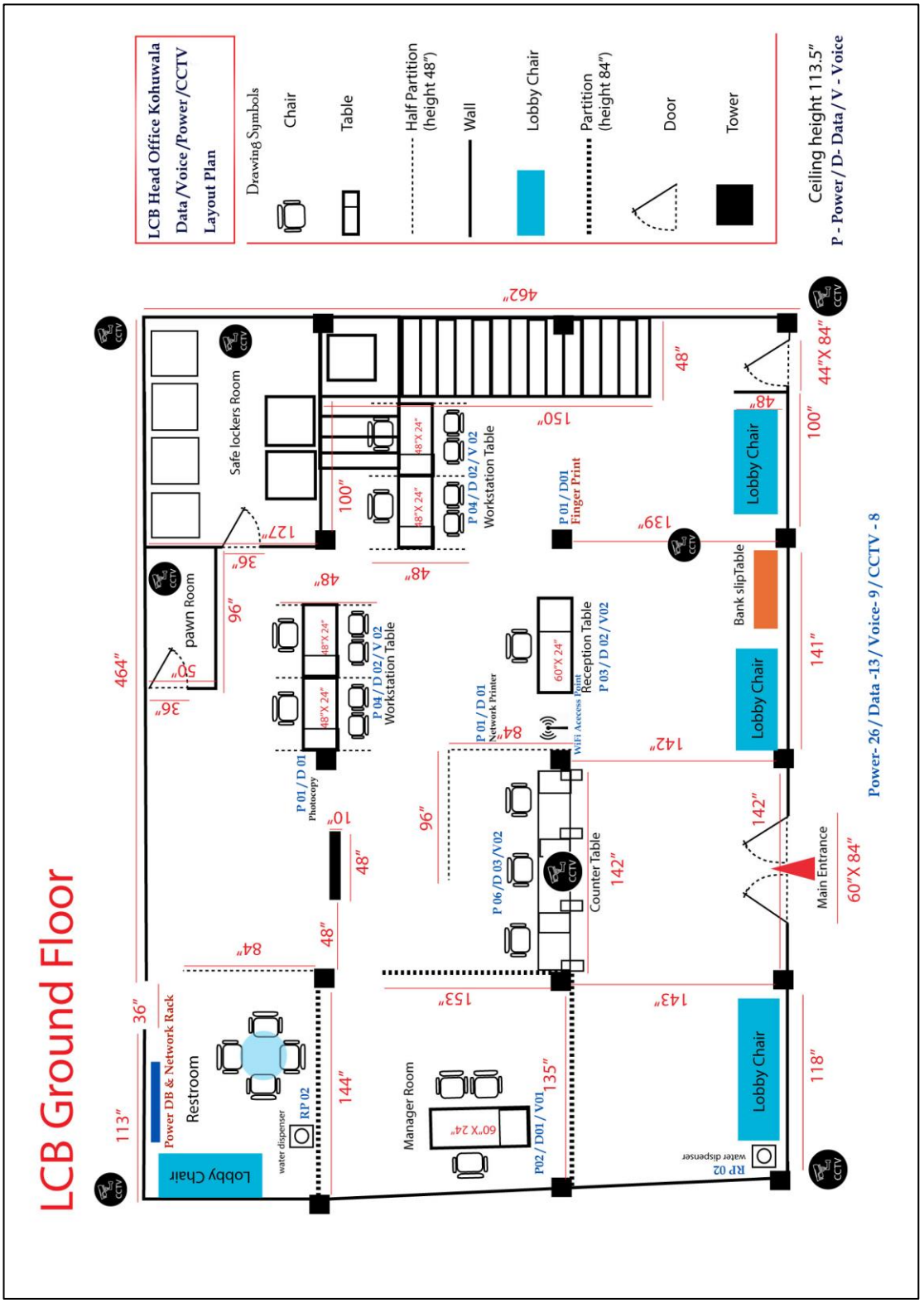
ANNEXURE 2 – NEAREST BRANCH AS AN ALTERNATIVE

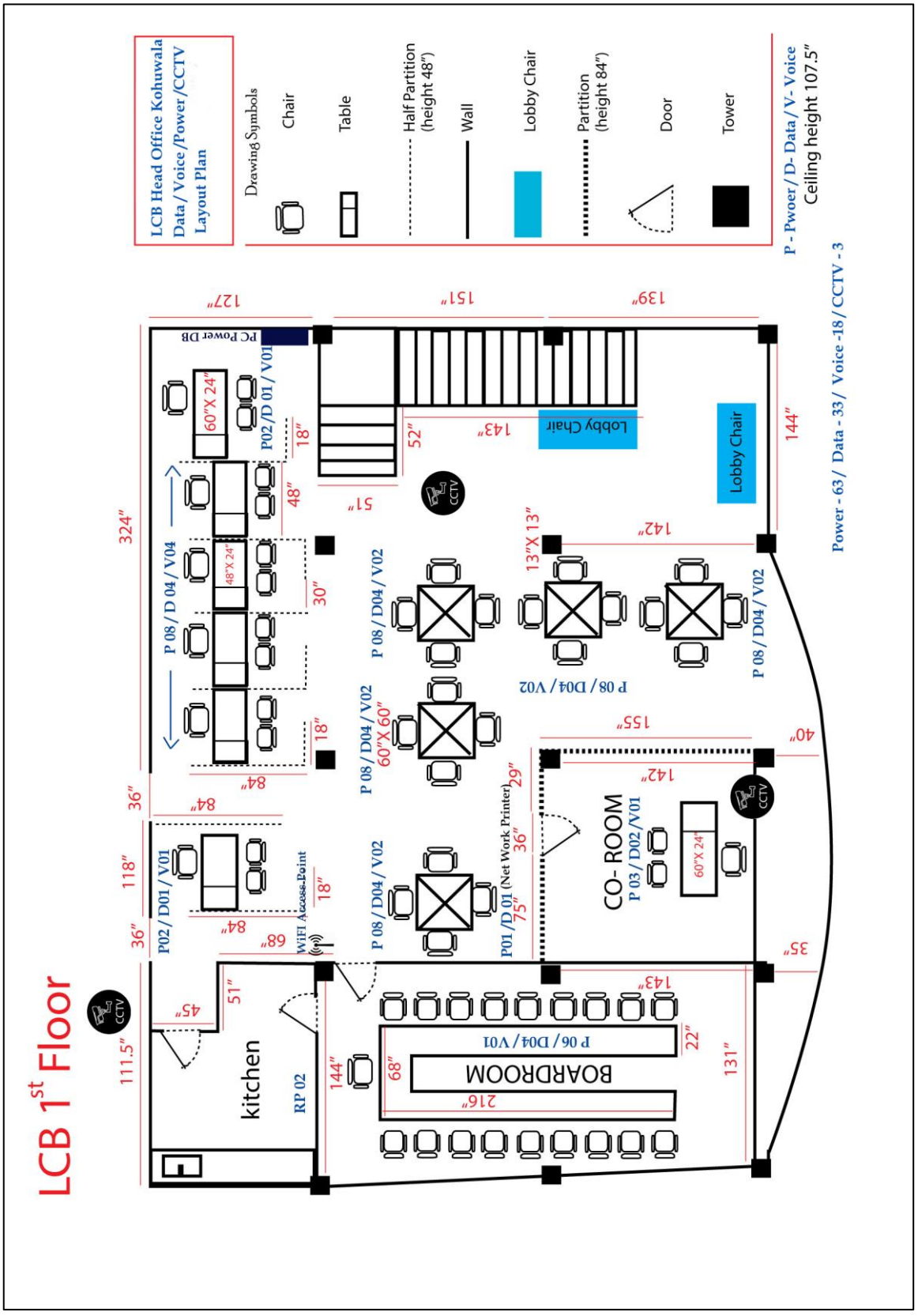
SL. NO	BRANCHES	NEAREST BRANCH
1	Galle Branch	Karapitiya Branch
2	Karandeniya Branch	Rathgama Branch
3	Matara Branch	Akuressa Branch
4	Pelawaththa Branch	Karandeniya Branch
5	Kohuwala Branch	Maharagama Branch
6	Rathgama Branch	Galle Branch
7	Karapitiya Branch	Galle Branch
8	Negombo Branch	Kuliyapitiya Branch
9	Kuliyapitiya Branch	Negambo Branch
10	Tangalle Branch	Matara Branch
11	Deiyandara Branch	Tangalle Branch
12	Akuressa Branch	Matara Branch
13	Embilipitiya Branch	Agunakolapelessa Branch
14	Maharagama Branch	Kohuwala Branch
15	Kegalle Branch	Gampaha Branch
16	Tissamaharama Branch	Tangalle Branch
17	Walasmulla Branch	Agunakolapelessa Branch
18	Agunukolapelessa Branch	Walasmulla Branch
19	Gampaha Branch	Minuwangoda Branch
20	Minuwangoda Branch	Gampaha Branch

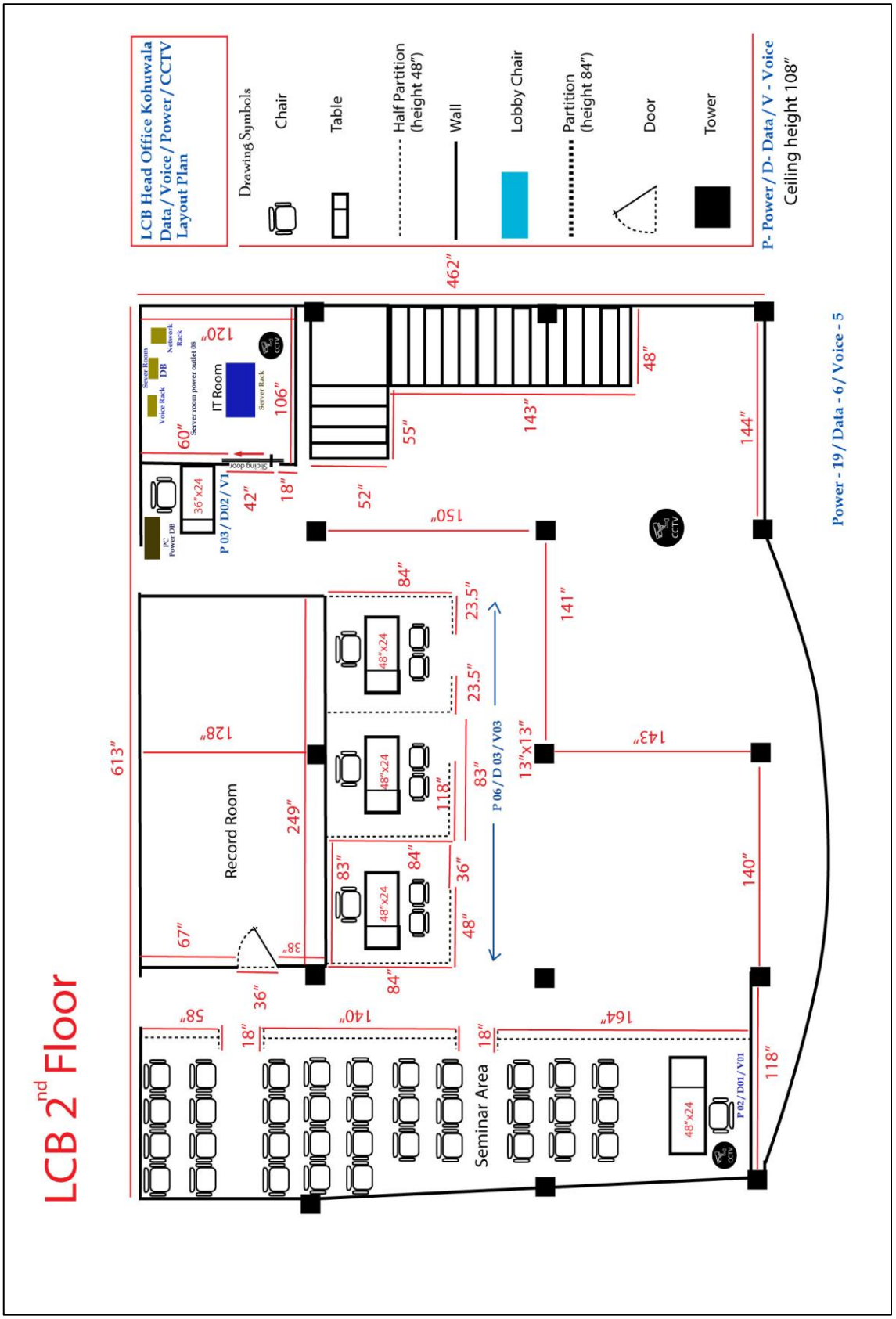
ANNEXURE 3 – ASSEMBLY POINT

SL. NO	BRANCHES	ASSEMBLY POINT
1	Galle Branch	Karapitiya Branch
2	Karandeniya Branch	Rathgama Branch
3	Matara Branch	Akuressa Branch
4	Pelawaththa Branch	Karandeniya Branch
5	Kohuwala Branch	Maharagama Branch
6	Rathgama Branch	Galle Branch
7	Karapitiya Branch	Galle Branch
8	Negombo Branch	Kuliyapitiya Branch
9	Kuliyapitiya Branch	Negambo Branch
10	Tangalle Branch	Matara Branch
11	Deiyandara Branch	Tangalle Branch
12	Akuressa Branch	Matara Branch
13	Embilipitiya Branch	Agunakolapelessa Branch
14	Maharagama Branch	Kohuwala Branch
15	Kegalle Branch	Gampaha Branch
16	Tissamaharama Branch	Tangalle Branch
17	Walasmulla Branch	Agunakolapelessa Branch
18	Agunukolapelessa Branch	Walasmulla Branch
19	Gampaha Branch	Minuwangoda Branch
20	Minuwangoda Branch	Gampaha Branch

ANNEXURE 4 - FLOOR PLAN OF HEAD OFFICE




LCB Head Office Kohuwala
Data / Voice /Power /CCTV
Layout Plan
Drawing Symbols
Chair
Table
Half Partition (height 48")
Wall
Lobby Chair
Partition (height 84")
Door
Tower
P - Pwoer / D- Data / V- Voice
Ceiling height 107.5"
Power - 63 / Data - 33 / Voice -18 / CCTV - 3
LCB 1st Floor
kitchen
RP 02
BOARDROOM
CO- ROOM
Lobby Chair
PC Power DB
WiFi Access Point
P01 /D 01 (Net Work Printer)
P02/ D01/ V01
P02/D 01 / V01
P 08 / D 04 / V04
P 08 / D04 / V02
P 03 / D02 /V01
P 06 / D04 / V01
60"X 24"
48"X 24"
60"X 60"
13"X 13"
127"
151"
139"
324"
144"
142"
155"
143"
216"
111.5"
131"
118"
84"
68"
51"
45"
40"
35"
30"
29"
22"
18"
52"
36"
75"


LCB Head Office Kohuwala
Data / Voice / Power / CCTV
Layout Plan
Drawing Symbols
Chair
Table
Half Partition (height 48")
Wall
Lobby Chair
Partition (height 84")
Door
Tower
P- Power / D- Data / V - Voice
Ceiling height 108"
LCB 2nd Floor
Power - 19 / Data - 6 / Voice - 5
IT Room
Server Room
Server Rack
Network Rack
DB
Voice Rack
Server room power outlet 08
Sliding door
PC
Power DB
P 03 / D02 / V1
Record Room
Seminar Area
P 06 / D 03 / V03
P 02 / D01 / V01
CCTV
613"
462"
249"
128"
67"
38"
36"
58"
18"
140"
164"
118"
106"
120"
60"
42"
52"
150"
55"
143"
48"
144"
84"
23.5"
141"
83"
13"x13"
140"

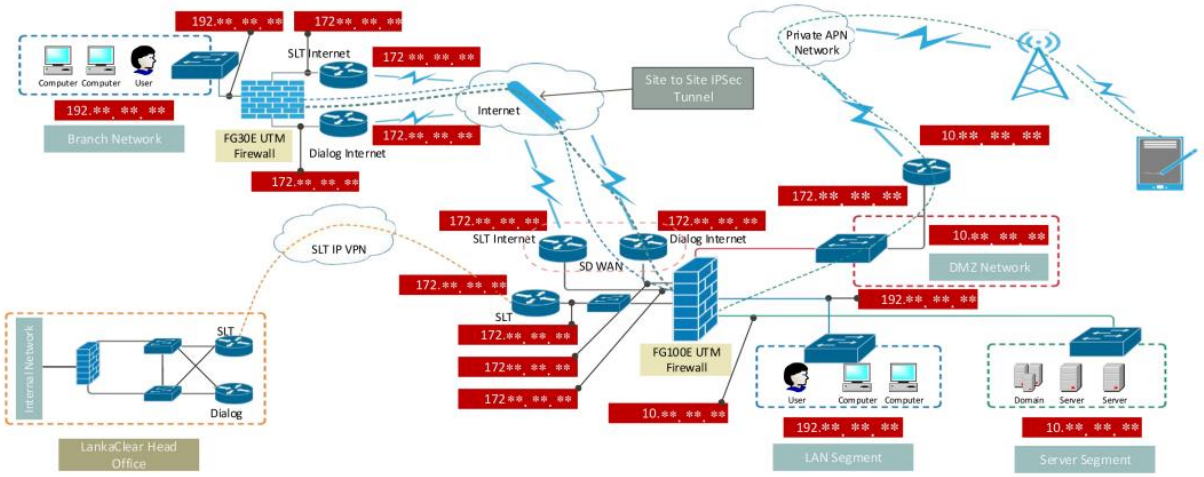
ANNEXURE 5 - SERVICE PROVIDERS

vendor name	Address	Contact Person	Mobile Contacts	Tel Contacts	Email Address	services
SLTMobitel PLC	Lotus Rd, Colombo 10	Lahiru Kularathna (AM)	710119642	112864314	lahirus@slt.com.lk	All SLT Links
Dialog Axiata PLC	475 Union Pl, Colombo 2	Malinda Wijesinghe	777331662	0777 678700	Malinda.Wijesinghe@dialog.lk	All SLT Links - Diolog 4G /APN/Mobile Connections
AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 2	Charith (Support Engineer)	767907266	0117 439 208	charith@acsysnetworks.com	firewall
AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 3	Shehan (Support Engineer)	761486293	0117 439 208	shehan@acsysnetworks.com	firewall
AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 3	Vidasun (Support Engineer)	761486450	0117 439 208	vidasun@acsysnetworks.com	Comvault
AcSys Networks Private Limited	Level 12, Parkland Building # 33, Park St, 3	Dasun (Support Engineer)	759912442	0117 439 208	Dasun@acsysnetworks.com	Comvault / End point
V S Information Systems (Pvt) Ltd	7 Sulaiman Terrace, Colombo 005	Dithika Jayakody	077 344 8335	112038568	dithika@vsis.lk	HP Servers / SAN

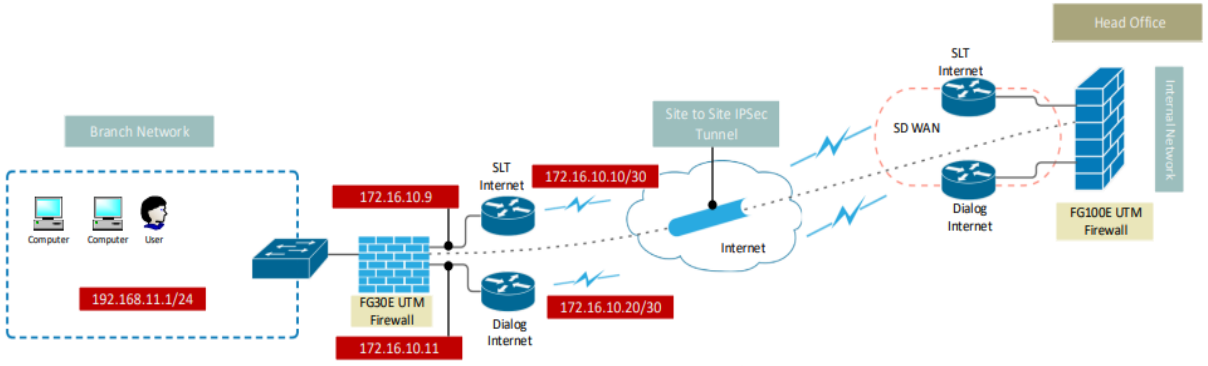
Delco Technology (Pvt) Ltd	Pagoda Rd, Sri Jayawardenepura Kotte	Dhanushka Madushanka	740340717	114732100	dhanushka@delko.lk	NAS
Ultrium Technologies (pvt) Ltd	RVH9+5F3, Dehiwala-Mount Lavinia	Lahiru kariyawasam	768203620	0115 882 933	lahiru@ultryum.com	HP Support
Interlink Engineering (pvt) ltd		Mahesh	772683402		mahesh@interlinkengineering.lk	server room UPS maintenance

ANNEXURE 6 – NETWORK DIAGRAM

LCB Finance Network Diagram



LCB Finance Branch Network Diagram



ANNEXURE 7 - IT INVENTORY LIST

Inventory Report				
Branch : Maharagama				
Category	Brand	Model	Serial No	Market Value
CPU	HP	HP ProDesk 600G1 SFF	6CR4383NSQ	110,000.00
CPU	HP	Hp ProDesk 400G1 SFF	6CR4203XM7	110,000.00
CPU	HP	HP ProDesk 600G1 SFF	6CR4383NSG	110,000.00
CPU	HP	HP ProDesk 600G1 SFF	6CR4383NT7	110,000.00
UPS	PROLINK	PRO 701SFC	564801214805005	11,500.00
UPS	PROLINK	PRO 701SFC	564801214805006	11,500.00
UPS	PROLINK	PRO 701SFC	564801214805007	11,500.00
UPS	PROLINK	PRO 701SFC	564801214805008	11,500.00
Monitor	HP	HP PRODisplay P191	6CM5251KBO	12,500.00
Monitor	HP	HP CompaqLe 1902X	3CQ30106N8	12,500.00
Monitor	HP	HPLV1911	6CM2340JDN	12,500.00
Monitor	HP	HPLV1911	6CM2340KJP	12,500.00
UPS	PROLINK	PRO1201SFC-4U	553701214800343	50,000.00
Keyboard & Mouse Combo Pack	RAPOO	X120Pro	A3802X120100480	4,000.00
Keyboard & Mouse Combo Pack	RAPOO	X120Pro	A3802X120100479	4,000.00
Keyboard & Mouse Combo Pack	RAPOO	X120Pro	A3802X120100155	4,000.00
Keyboard & Mouse Combo Pack	RAPOO	X120Pro	A3802X120100476	4,000.00
Passbook Printer	EPSON	EPSON -PLQ 20	RJLY171112	220,000.00
Firewall	Fortigate	FG-40F	FGT40FTK2109BRUM	480,000.00
Printer	CANON	IMAGE RUNNER 2006N	2FF16577	450,000.00
Mouse (CCTV)	LOGITECH	B175	2143LZX0ZHM8	5,500.00
Webcam	LOGITECH	C270 HD720P	2143AP08CDA9 / 2143AP08WH38	14,000.00
Printer	Portabale Printer		675	25,000.00
Speakers	LOGITECH	KAZAI ICON-100 K-298	106817 2	5,000.00
Hikvision DVR	Hikvision	DS-7108HQHI	K10820210105CCWRF37298030WCVU	65,000.00
Laptop	HP	HP Probook 450g2	CNDS364P03	120,000.00
Camera	8 port dvr	8 cam		
seagate hard	6tb	1		
NAS	QNAP		Q239F055185	Maharagama Backup NAS
Switch	BDCOM	BDCOM S2510 -C	G20009066401	
UPS	Prolink	PRO1201SFC	5.53701E+14	
Computer For Consumer	Dell	Optiplex 5050	GYPY9P2	Consumer Loan
Monitor For Consumer	Dell	Plat pannel	CN-ONCO2M-FCCOO-95D-C5RB-A07	Consumer Loan

Category	Brand	Model	Serial No	Cost /Market Value	Branch	Department
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ00J5DK	80,000.00	Head Office	Admin
CPU	Dell	Optiplex 3060	8LZCBW2	80,000.00	Head Office	Admin
CPU	Dell	Optiplex 3070	BMNH6Z2	80,000.00	Head Office	Credit
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ00Y4GN	80,000.00	Head Office	Credit
CPU	Dell	Optiplex 3060	8LJCBW2	80,000.00	Head Office	Credit
CPU	Lenovo	Thinkcenter	1S10A8CTO1WWPC056MD	80,000.00	Head Office	Credit
CPU	HP	HP ProDesk400 G2 SFF	6CR51155CV	80,000.00	Head Office	Finance
CPU	HP	HP ProDesk 600 G1 SFF	6CR4383NRY	80,000.00	Head Office	Finance
CPU	Dell	Optiplex 3060	J0X1LQ2	80,000.00	Head Office	Finance
CPU	Dell	Optiplex 5050	67QPLN2	80,000.00	Head Office	Finance
CPU	HP	Prodesk 600 G1 SFF	6CR4171HXH	80,000.00	Head Office	Credit
CPU	Dell	Optiplex 3060	8K8FBW2	80,000.00	Head Office	Finance
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ01CQ4W	80,000.00	Head Office	IT
CPU	Dell	Optiplex 3060	DH6N6Q2	80,000.00	Head Office	IT
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ017P2Y	80,000.00	Head Office	IT
CPU	Lenovo	Thinkcenter	PC0604ZQ	80,000.00	Head Office	IT
CPU	Dell	Optiplex 3060	DHBQ6Q2	80,000.00	Head Office	HR

CPU	HP	HP ProDesk600 G1 SFF	6CR4383NSN	80,000.00	Head Office	HR
CPU	HP	HP ProDesk600 G1 SFF	6CR4383NR7	80,000.00	Head Office	HR
CPU	HP	HP ProDesk600 G1 SFF	6CR4171HWZ	80,000.00	Head Office	HR
Laptop	Lenovo	T 450S	40A4juu		HO	Gold
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ 007KSY	80,000.00	Head Office	Legal
CPU	Dell	Optiplex 5050	6YRY9P2	80,000.00	Head Office	Legal
CPU	Dell	Optiplex 5050	6YSX9P2	80,000.00	Head Office	Legal
CPU	Dell	Optiplex 5050	6YPY9P2	80,000.00	Head Office	Legal
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ 00A7NR	80,000.00	Head Office	Recovery
CPU	Lenovo	Thinkcenter	MJ05FS1G	80,000.00	Head Office	IT
CPU	HP	HP Compaq pro 6300SFF	SGH430TZ3B	80,000.00	Head Office	IT
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ 00QWCO	80,000.00	Head Office	Recovery
CPU	Lenovo	Thinkcenter	1S10A8S00200MJ OOJ5QS	80,000.00	Head Office	Recovery
CPU	SAMSUNG	BA68-05402A	ZWCY96BB10017 6X	80,000.00	Head Office	Recovery
DVR			DS-7116HGHI -F1 CO8701138	70,000.00	Head Office	HO
EMS Unit	Vutlan	Vutlan VT825	10722	1,500,000.00	Head Office	Server Room
Firewall	Fortigate	Fortigate - 100E	FG100ETK180113 08	3,500,000.00	Head Office	Server Room
Laptop	Lenovo	Thinkpad T470	PF-0wL13N	120,000.00	Head Office	Boardroom
Laptop	Asus	Asus P2540F	L5nxcv10T25521F	120,000.00	Head Office	Finance

Laptop	HP	3165NGW	CND6460LR2	120,000.00	Head Office	Finance
Laptop	HP	RTL8821CE	CND131761J	120,000.00	Head Office	Finance
Laptop	Asus	X510U	J7HOCXO9958229A	220,000.00	Head Office	IT
Laptop	Lenovo	Thinkpad T470	PC-0A4HTN	120,000.00	Head Office	Recovery
Monitor	Acer	V206HQL	MMLXKSG0015060714E4220	35,000.00	Head Office	IT
Mouse	A4tech	OP-620D	762010	1,750.00	Head Office	Admin
Monitor	Dell	E1916H	CN-0NC02M-FCC00-910CN9D-A07	35,000.00	Head Office	Admin
Monitor	Acer	V206HQL	MMLXKSG00172004DF54227	35,000.00	Head Office	Credit
Monitor	Lenovo	Thinkcenter	V5848654	35,000.00	Head Office	Credit
Monitor	Dell	E1916H	CN-0JF27G-FCC00-7CP-DRHB-A04	35,000.00	Head Office	Credit
Monitor	Dell	E1916H	CN-0NC0SM-FCC00-910-CPCD-A07	35,000.00	Head Office	Credit
Monitor	HP	HP P222VA	CNK6320LVS	35,000.00	Head Office	Finance
Monitor	LG	20M38D	605NTCZ17699	35,000.00	Head Office	Finance
Monitor	Dell	E1916H	CN-0NC02M-FCC00-910-CNVD-A07	35,000.00	Head Office	Finance
Monitor	Dell	E1916H	CN-OJF27G-FCC00-7C4-AD6B-AO4	35,000.00	Head Office	Finance
Monitor	HP	HP Compaq LE 1902 x	3CQ2430CBH	35,000.00	Head Office	Recovery
Monitor	ViewSonic	VA1701WB	QUD081301516	35,000.00	Head Office	IT

Monitor	Dell	E1916H	CN-0NC02M-FCC00-85V-C1PB-A06	35,000.00	Head Office	IT
Monitor	Dell	E1916H	CN-0NC02M-FCC00-95D-C5NB-A07	35,000.00	Head Office	IT
Monitor	Dell	E2213HB	CN-0C8XTW-74261-357-4GRL	35,000.00	Head Office	IT
Monitor	HP	HP LV1911	6CM2340JD6	35,000.00	Head Office	IT
Monitor	Dell	E1916H	CN-0NC02M-FCC00-85S-CPUB-A06	35,000.00	Head Office	HR
Monitor	SAMSUNG	S19A100N	ZTRRH4LD62218B	35,000.00	Head Office	HR
Monitor	HP	HP Compaq LE 1902 x	CNT22835YH	35,000.00	Head Office	HR
Monitor	I-O DATA	LCD-AD193EB	GAJ5003159SX	35,000.00	Head Office	HR
Monitor	HP	LE1911	6CM23905X4	35,000.00	Head Office	Credit
Monitor	ViewSonic	VA1701WB	QUD081301499	35,000.00	Head Office	Legal
Monitor	Dell	E1916H	CM-OJF27G-FCC00-7CP-DPWE-A04	35,000.00	Head Office	Legal
Monitor	Dell	E1916H	CN-OJF27G-FCC00-7C4-HA7B-A04	35,000.00	Head Office	Legal
Monitor	Dell	E1916H	CN-0NCO2M-FCC00-95D-C5RB-A07	35,000.00	Head Office	Legal
Monitor	Dell	E2213HB	CN-0C8XTW-74261-39R-0JML	35,000.00	Head Office	IT
Monitor	ViewSonic	VA1701WB	QUD081301514	35,000.00	Head Office	Recovery
Monitor	HP	ProDisplay P191	6CM3180KHP	35,000.00	Head Office	Recovery
Monitor	HP	ProDisplay P192	6CM3210XMR	35,000.00	Head Office	Recovery

NAS 1	QNAP	qnap tvs-972xu-rp	Q19110070	1,800,000.00	Head Office	Server Room
NAS 2	QNAP	qnap ts-432pxu-rp	Q23AI03763T	2,500,000.00	Head Office	Server Room
Network Switch	CISCO	SG-300-28	74-7002-04-cd	350,000.00	Head Office	Server Room
Network Switch	HP	HPE 1420 24G	CN70GVHOCT	350,000.00	Head Office	Server Room
PABX System 1	Panasonic	KX-NS300ML	8BCTW003887	700,000.00	Head Office	Server Room
PABX System 2	Panasonic	KX-NS320XE	OEBCXOO2038	700,000.00	Head Office	Server Room
Printer	Canon	Image Runner 2224N	2SF02542	450,000.00	Head Office	Admin
Printer	HP	LaserJet PRO400	VNC3K06050	50,000.00	Head Office	Finance
Printer	HP	Laserjet pro MFP M227	VNL3G01065	25,000.00	Head Office	HO
Printer	Epson	PLQ-20	G5AY131428	200,000.00	Head Office	IT
Printer	Canon	F166400	NTLA509780	5,000.00	Head Office	Legal
Printer	HP	LaserJet P1005	BNC8Y06718	5,000.00	Head Office	Marketing
Printer	HP	HP LaserJet 1020	CNC2N57036	7,500.00	Head Office	Recovery
Printer	HP	LaserJet P1005	VNC7L01829	5,000.00	Head Office	Secretary
Projector	Epson	H843C	X4HW9X00192	350,000.00	Head Office	HO
Projector	Epson	H556C	VB8K5501598	200,000.00	Head Office	HO
SAN	HP	HPE 2050 SAN Dual controller	2S6938B956	5,000,000.00	Head Office	Server Room
Mouse	A4tech	OP-620D	702009	1,750.00	Head Office	Credit
Scanner	Epson	DS-770 ii	*X8QE001566	250,000.00	Head Office	Credit

Servers	HP	DL 360 Gn10	SGH942X222	4,000,000.00	Head Office	Server Room
Servers	HP	DL 360 Gn10	SGH942X21R	4,000,000.00	Head Office	Server Room
Servers	HP	DL 380	2M274503NG	1,550,000.00	Head Office	Server Room
Servers	DELL	powerEdge R230 V6	BZTV8T2	1,850,000.00	Head Office	Server Room
Servers	IBM	X3200 M3	99F5775	200,000.00	Head Office	Server Room
Servers	IBM	X3200 M3	06TTT10	200,000.00	Head Office	Server Room
Servers	HP	ML 30	G038N8H	800,000.00	Head Office	Server Room
Servers	IBM	X3200 M3	06GTN21	200,000.00	Head Office	Server Room
UPS	Prolink	Pro701SFC	564801203800541	14,000.00	Head Office	Admin
UPS	Techfine	650VA	90525009BAS	14,000.00	Head Office	Admin
UPS	Techfine	650VA	806220234AS	14,000.00	Head Office	Credit
UPS	Prolink	Pro701SFC	564801203800765	14,000.00	Head Office	Credit
UPS	Techfine	650VA	8064220298AS	14,000.00	Head Office	Credit
UPS	Prolink	Pro701SFC	564801203800767	14,000.00	Head Office	Credit
UPS	Techfine	650VA	810130345AS	14,000.00	Head Office	Finance
UPS	Prolink	Pro701SFC	564801214804187	14,000.00	Head Office	Finance
UPS	DCP	DCP 650 P-T	180402011620	14,000.00	Head Office	Finance
UPS	DCP	DCP 650 P-T	180402011618	14,000.00	Head Office	Finance
Printer	HP	Laser Jet Pro MFP M227 FDN	VNL3GO1O77	150,000.00	Head Office	IT

UPS	Prolink	Pro701SFC	564801214802974	14,000.00	Head Office	IT
UPS	Techfine	650VA	905250099AS	14,000.00	Head Office	Finance
UPS	Prolink	PRO1201SFCU	538701180902040	28,000.00	Head Office	HO
UPS	Prolink	Pro701SFC	564801203800768	14,000.00	Head Office	IT
UPS	Techfine	650VA	904220300AS	14,000.00	Head Office	IT
UPS	Techfine	650VA	904220142AS	14,000.00	Head Office	IT
UPS	Prolink	Pro701SFC	564801203801028	14,000.00	Head Office	HO-Recovery
UPS	Techfine	650VA	803020659AS	14,000.00	Head Office	HR
UPS	Techfine	650VA	810160190AS	14,000.00	Head Office	HR
UPS	DCP	DCP 650 P-T	180402010448	14,000.00	Head Office	HR
UPS	Prolink	Pro701SFC	564801214802975	14,000.00	Head Office	Credit
UPS	Techfine	650VA	9G4220393AC	14,000.00	Head Office	Legal
UPS	Prolink	Pro701SFC	564801214804186	14,000.00	Head Office	Legal
UPS	DCP	650 P-T	180402011617	14,000.00	Head Office	Legal
UPS	DCP	DCP 650 P-T	180402010708	14,000.00	Head Office	Legal
UPS	Techfine	650VA	904220297AS	14,000.00	Head Office	IT
UPS	Techfine	650AV	806160846AS	14,000.00	Head Office	Recovery
UPS	Techfine	650VA	810160275AS	14,000.00	Head Office	Recovery
UPS	TechFine	6KVA	11002516496968450015	500,000.00	Head Office	Server Room

UPS	TechFine	6KVA	110025164969122000000	500,000.00	Head Office	Server Room
cpu	HP	HP-600G1	6CR4383NR7	80,000.00	Head Office	Admin
Monitor	Samsung	SA-100	ZTRRH4D602218B	35,000.00	Head Office	Admin
UPS	Techfine	650VA	S/N-0000043	14,000.00	Head Office	Admin
Mouse	A4tech	OP-620D	762015	1,750.00	Head Office	IT
Mouse	A4tech	OP-620D	762011	1,750.00	Head Office	IT
Mouse	A4tech	OP-620D	762012	1,750.00	Head Office	IT
Mouse	A4tech	OP-620D	762007	1,750.00	Head Office	IT
Mouse	A4tech	OP-620D	762013	1,750.00	Head Office	IT
Mouse	A4tech	OP-620D	762014	1,750.00	Head Office	Risk
CPU	Dell	Optiplex 3060	N1MR6A00	80,000.00	Head Office	Risk
Monitor	HP	P201	6CM4081NZK	35,000.00	Head Office	Risk
UPS	Prolink	Pro701SFC	564801214802973	14,000.00	Head Office	Compliance
CPU	Dell	Optiplex 3060	N1MR6A001	80,000.00	Head Office	Compliance
Monitor	HP	P201	3CQ33605D1	35,000.00	Head Office	Compliance
Laptop	Lenovo	Thinkpad	PF21Z2QW 19/12	120,000.00	Head Office	Leasing
Monitor	HP	P201	CNOIKH87	35,000.00	Head Office	Leasing
CPU	Dell	Optiplex 3070	…	80,000.00	Head Office	Leasing
UPS	Prolink	Pro701SFC	564801203800765	14,000.00	Head Office	Leasing

Monitor	HP	P201	6CM7010H6W	35,000.00	Head Office	Leasing
Mouse	A4tech	OP-620D	762016	1,750.00	Head Office	Leasing
CPU	Dell	Optiplex 5060	…	80,000.00	Head Office	Leasing
UPS	Prolink	Pro701SFC	590301232001753	14,000.00	Head Office	Leasing
Laptop	Lenovo	T450S	11S45N1126Z1ZS885CF13S	120,000.00	Head Office	Marketing
Keyboard	A4tech	KM-720	762017	2,950.00	Head Office	IT
Keyboard	A4tech	KM-720	762018	2,950.00	Head Office	IT
Hard-disk	SEAGATE	Vedio 3.5 HDD	W5238V1Q		Head Office	IT
Hard-disk	SEAGATE	Vedio 3.5 HDD	W5221ZV0		Head Office	IT
Hard-disk	SEAGATE	Vedio 3.5 HDD	W523LDBX		Head Office	IT
Hard-disk	SEAGATE	Vedio 3.5 HDD	Z526R616		Head Office	IT
Hard-disk	SEAGATE	Vedio 3.5 HDD	W5247KH7		Head Office	IT
Laptop	DELL	Latitude 3500	3KRZGT2	120,000.00	Head Office	IT
Laptop	DELL	Latitude 5500	s/n 72X13Z2	120,000.00	Head Office	IT
Laptop	Lenovo	T470	s/n 015105001256619	120,000.00	Head Office	Audit
Laptop	Lenovo	T490	PF1DV959	120,000.00	Head Office	Audit
Laptop	Lenovo	T490	PF27VBXW	120,000.00	Head Office	Audit
Laptop	DELL	Latitude 5500	s/n 24N53Z2	120,000.00	Head Office	Finance
Laptop	Lenovo	T-470	C697D5B1	120,000.00	Head Office	HR

CPU	Assemble	Assemble	Assemble	600,000.00	Head Office	Marketing
Laptop	Lenovo	IdeaPad L-340	PF1SEN8Z	120,000.00	Head Office	Finance
CPU	Dell	Optiplex 5060	S/N 63J8BW2	80,000.00	Head Office	Credit
Monitor	HP	V203P	6VM7010HXL	35,000.00	Head Office	Credit
UPS	Prolink	Pro701SFC	..	14,000.00	Head Office	Credit
UPS	Prolink	Pro701SFC	564801203801028	14,000.00	Head Office	Recovery
Laptop	Lenovo	T 450S	40A4juu	120,000.00	Head Office	Compliance
UPS	Prolink	Pro701SF	S/N 564801214802976	14,000.00	Head Office	IT
CPU	DELL	OPTIPLEX 3060 MICRO	R-RMM-E2K-D10U003	80,000.00	Head Office	IT
CPU	DELL	OPTIPLEX 3060 MICRO	S/N 60FFBW2	80,000.00	Head Office	IT
Monitor	HP	HP P222VA	CNK6400CHL	35,000.00	Head Office	IT
Monitor	HP	HP P222VA	CNK60708XV	35,000.00	Head Office	IT
Monitor	HP	HP P203P	6cm7130rf9	35,000.00	Head Office	IT
UPS	Prolink	Pro701SFC	S/N 564801203800765	14,000.00	Head Office	IT
Laptop	HP	ProBook 450 G8	#5CD2107VZ6	400,000.00	Head Office	IT
Laptop	Lenovo	Thinkpad T450s	PC-02L6VD	120,000.00	Head Office	Credit
Laptop	Asus	P2540F	L4NXCVO9N99716A	120,000.00	Head Office	Coporete management
Laptop	Asus	Asus P2540F	L5NXCV10T35	120,000.00	Head Office	Coporete management

Laptop	Dell	Inspiron 15 3000	8VQ4C73	120,000.00	Head Office	Secretary
CPU	HP	Prodesk 600 G1 SFF	6CR4171HXH		HO	Gold
Monitor	HP	V203P	6CM8030GCS	35,000.00	Head Office	IT
Monitor	HP	P203	CNC7510N6G	35,000.00	Head Office	Credit
Monitor	HP	HP P222VA	CNK65207PN	35,000.00	Head Office	IT
UPS	Prolink	Pro701SFC	590301232001245	14,000.00	Head Office	IT
UPS	Prolink	Pro701SF	S/N 590301232004903	14,000.00	Head Office	IT
CPU	DELL	OPTIPLEX 3060 MICRO	s/n 060821	80,000.00	Head Office	Credit
CPU	DELL	OPTIPLEX 3060 MICRO	s/n 060822	80,000.00	Head Office	IT
CPU	DELL	OPTIPLEX 3060 MICRO	JOZJLQ2	80,000.00	Head Office	Kohuwala Branch
CPU	Lenovo	Lenovo M93P	MJ012XCV	80,000.00	Head Office	Kohuwala Branch
CPU	DELL	Dell Optiplex 5050	6YQE9P2	80,000.00	Head Office	Kohuwala Branch
CPU	DELL	Dell Optiplex 5050	XYZ0BP2	80,000.00	Head Office	Kohuwala Branch
CPU	DELL	Dell Optiplex 5050	6YHW9P2	80,000.00	Head Office	Kohuwala Branch
CPU	DELL	Dell Optiplex 5050	683PLN2	80,000.00	Head Office	Kohuwala Branch
Monitor	Dell	E 1916H	CN-ONCO2H-FCC00-85V	35,000.00	Head Office	Kohuwala Branch
Monitor	Lenovo	03T8464	V5207622	35,000.00	Head Office	Kohuwala Branch
Monitor	Dell	E 1916H	CN-OJF27G-FCC007CP-PRA04	35,000.00	Head Office	Kohuwala Branch
Monitor	Dell	E 1916H	CN-OJF27G-CC00FC4-GH4DA04	35,000.00	Head Office	Kohuwala Branch

Monitor	Dell	E 1916H	CN-OCF27G-FCC00-7CP	35,000.00	Head Office	Kohuwala Branch
Monitor	Dell	E 1916H	CN-OJF27G-FCC00-FC4	35,000.00	Head Office	Kohuwala Branch
UPS	Techfine	650 VA	90525097AS	14,000.00	Head Office	Kohuwala Branch
UPS	Techfine	650 VA	SN0000058	14,000.00	Head Office	Kohuwala Branch
UPS	DCP	650 VA	180402010664	14,000.00	Head Office	Kohuwala Branch
UPS	DCP	650 VA	180402010662	14,000.00	Head Office	Kohuwala Branch
UPS	DCP	650 VA	180402010663	14,000.00	Head Office	Kohuwala Branch
UPS	DCP	650 VA	1403031598	14,000.00	Head Office	Kohuwala Branch
UPS	Prolink	650va	564801203800776	14,000.00	Head Office	HR
Laptop	Lenovo	T480	PF1HSA1A	120,000.00	Head Office	Risk
UPS	Techfine	650VA	905250099AS	14,000.00	Head Office	Recovery
laptop	Dell	Dell Latitiude 5500	s/n jkdr2r2	120,000.00	Head Office	Marketing
MONITOR	HP	V203P	6CM6491DTV		HO	Gold
UPS	PROLINK	PRO701SFC	5.64801E+14		HO	Gold
Pendrive	Lexar	M-400(32GB)	LJDM400032G-BNBNG	1,600.00	Head Office	Finance
Nikon Cam	Nikon	D7500	8240286	290,000.00	Head Office	Marketing
Camera Flash	Godox	V860	23100122511	50,000.00	Head Office	Marketing
Lense	Nikon	AF-S-DX (18-140mm)	70549340		Head Office	Marketing
SD Card	SANDISK	SANDISK Ultra SD 32 GB 120MB/s	BM2402353748Z	3,500.00	Head Office	Marketing

NIKON BAG	NIKON	Nikon DSLR side Camera bag		7,500.00	Head Office	Marketing
Dry Box		DRY BOX 3828 W/METER		13,000.00	Head Office	Marketing
Flasher Battary	Godox		20230907FA1816		Head Office	Marketing
Camera Battary	Nikon		21NR19-66		Head Office	Marketing
Monitor	SAMSUNG	733NW	CM17H7FQA13018F	35,000.00	Head Office	Recovery
	Monitor	DELL	E1914HF	CN-OXOT4K-72872-52Q-DP8M	12,500.00	Galle CCTV Moniter
Laptop	Dell	Latitude5400	5L1C0Z2	IT Backup	Head Office	IT
Charger	Dell	Latitude5401	071886(My ITEM Code)	IT Backup	Head Office	IT
Laptop	Dell	Latitude5401	B282Z33	Audit (Internal)	Head Office	Audit
Charger	Dell	Latitude5401	71884 (My ITEM Code)	Audit (Internal)	Head Office	Audit
Laptop	Dell	Latitude5401	897DZ33	Audit (Internal)	Head Office	Audit
Charger	Dell	Latitude5401	DPNOG4X7T	Audit (Internal)	Head Office	Audit
UPS	PROLINK	PRO701SFC	s/n-564801203800767	Recovery - DGM	Head Office	Recovery

ANNEXURE 8 - LIST OF AGREEMENTS/ CRUCIAL DOCUMENTS

DOCUMENT	VENDOR	MEDIA TYPE	LOCATION HELD
Server Agreements		Both Soft copies and Hard copies	Hard copies are held in File Cabinets Soft copies held in DR Site Server
UPS/ PC Maintenance Agreements			
Printer/ Scanner/ CCTV Camera Maintenance Agreements			
Any other agreements			
Depsoit Register		Hard copies	Hard copies are held in File Cabinets
Security Documentation			
Certificate Stock			
KYC Forms			
Application Forms & Mandates			
Letter Heads			
Reminder Letter Formats			
General Payment & Receipt Vouchers			
Demand Promissory Notes / Agreements /			
Asset Declaration			
Pawning Register			
Pawning Tickets			
Employee Contact Details			
Other Legal Documents			

ANNEXURE 9 - FILING LOCATIONS OF PHYSICAL RECORDS

SL. NO.	BRANCH / CENETR	TYPE		RECORD ROOM
		BRANCH	CENTER	
1		✓		YES
2		✓		YES

ANNEXURE 10 - LIST OF ITEMS REQUIRED TO RESUME OPERATIONS AT THE ALTERNATE SITE

ITEM	NO. OF UNITS REQUIRED
PCs	12
Servers	01
Printers	02
Scanners	01
Tables	12
Chairs	12
Water Dispensers	02
ACs	01
UPSs	12
Stationery items	Needs to be made Available
Network and Internet	
Copies of agreements	
NW and SW design and architecture docs	

ANNEXURE 11 - FIRE DRILL CHECK LIST

Fire Drill Checklist

Name of the leader:

Fire drill area:

Assembly area:

Method of activation of fire alarm:

Time fire alarm activated:

Time all employees evacuated the place completely;

SL NO	OBSERVATION	YES	NO	NOT OBSERVED	REMARKS
1.	ERT members wearing distinctive marking Arm Band or Hat				
2.	Assistance to physically challenged				
3.	Interior doors closed but not locked after search				
4.	ERT members checked toilets				
5.	If the drill involved simulation of fire, was a portable fire extinguisher brought to the location of the fire				
6.	Initial response of the occupants on sounding of the alarm				
7.	Overall response of the ERT members				
8.	Occupants aware of the emergency exit				
9.	Fire alarms are clearly marked in all areas				
10.	Did air conditioning system shutdown				
11.	Were exits freed of obstruction				
12.	Were any doors blocked				
13.	Condition and accessibility of portable fire extinguisher				
14.	Portable gas electric appliances turned off				
15.	Did evacuation proceed in smooth and orderly manner				
16.	Fire drill list to be retained in the safe files				

ANNEXURE 12 - EVENT LOG

Use the Event Log to record information, decision and actions in the period immediately following the critical event or incident.

DATE	TIME	INFORMATION / DECISIONS / ACTIONS	INITIALS

ANNEXURE 13 – RISK LEVEL ASSESSMENT

Hazard	Probability of occurrence			Estimated Impact on the staff and/or Company's physical assets			Estimated Impact on the business operation		
	Very low/Low	Moderate	High/Very High	Very low/Low	Moderate	High/Very High	Very low/Low	Moderate	High/Very High
Fire Emergencies									
Minor Fire (excluding IT Server room)									
Major Fire									
Explosion (excluding bomb explosions)									
Medical Emergencies									
Food poisoning									
Pandemic or other human diseases									
Injuries to many staff due to an office mishap									
Weather Emergencies									
Tsunami									
Cyclone, torrential rain									
Earth quake, strong									

earth tremors									
Threat of Violence									
Terrorist attack									
Bomb threat									
Hostage situation									
Vandalism									
civil disturbance e, blockade of access to the premises due to demonstrations									
Sabotage									

Hazard	Probability of occurrence			Estimated Impact on the staff and/or Company's physical assets			Estimated Impact on the operation		
	Very low/ Low	Moderate	High / Very High	Very low/ Low	Moderate	High / Very High	Very low / Low	Moderate	High / Very High
Building Systems									
Telephone failure									
Power outage – short period									

Power outage – longer period									
Information Technology									
Fire damage to IT Server room									
Auto-shut down of A/C as a result excess heating damaging IT equipment									
IT system bugs/errors, virus attack, hacking									
Theft of critical IT equipment/sever									
Data communication (email) failures									
Other									
Helicopter collision with building									
Transportation system disruptions due to malicious activity, work stoppages, or accidents									

Hazardous chemical spill and/or air contamination									
Floor flooding as a result of pipe burst and leaks									
Interruption of call center operation/service – short term									

RECOMMENDATION

…….

Chief Risk Officer

……

CEO/Chief Executive Officer