Version History

Ver. No.	*Authors*	*Date*	*Reviewers*	*Review Date*	*Release Date*
1.0	CISO	27-Aug-2018	ISMF	31-Aug-2018	03-Sep-2018
2.0	CISO	03-Dec-2019	ISMF	13-Dec-2019	16-Dec-2019
3.0	CISO	02-Nov-2020	ISMF	06-Nov-2020	10-Nov-2020

Change History

Ver. No.	*Section*	*Date*	*Change Information*	*RFC No.*
1.0	All	03-Sep-2018	New Release	-
2.0	All	16-Dec-2019	Annual Review	-
3.0	CISO	10-Nov-2020	Annual Review	-

Table of Contents

Business Continuity Management Process

1.0 Objectives

The objective of this document is to define the process for the Business Continuity Management for CIPL.

2.0 Scope

This process applies to all the processes, and / or sub processes under the purview of the Scope of ISMS.

3.0 Policy

3.1 Policy Statement

- Business Continuity Management Policy

3.2 Framework to Support or Implement this Policy

- Business Continuity Management policy is implemented as per the procedure mentioned below

4.0 References to (checklists, forms, guidelines, lists, standards, templates, other processes)

Process Element	*Description*	*ID*
Checklists	*NA*	
Forms	*Business Impact Analysis*	ISMS-L4-FR-CISO-22
	Business Continuity Test Report	ISMS-L4-FR-CISO-23
Guidelines	*NA*	
Lists	*NA*	
Standards	*NA*	
Templates	*NA*	
Other Processes	*NA*	

5.0 Entry Criteria

Inputs	*Source Processes*
Incident	Incident Management
Business Continuity Tests	-

6.0 Responsibilities

Role	*Responsibilities*
DR Declaration team	• Power to communicate for disaster.

Role	*Responsibilities*
Incident Response Team	• Power to called disruption. • Co-ordination with branches and technology team during disaster.
Application & Support Team	• Parameter configuration in SAP, SAP-BI etc.
Information Technology Team	• To ensure DR Server is in complete sync with primary server • To coordinate with recovery team to make primary site up.
Implementation Team	• To ensure planned activities as per BCP are completed in shortest possible time
Administration Team	• To make available facilities like transportation, electricity, Diesel & other admin processes. • Maintain list of emergency contact.
Senior Management	• Review the status of Business continuity Test Reports during Management Review • Approve sufficient funds for Business Continuity Management Activities • Provide guidance Teams and provide decisions during Business Continuity Management Incident

7.0 Process Description

Overview Diagram

Refer below to specific process for flowchart.

7.1 Business Continuity – Fire Safety

7.1.1 DR Declaration Team / BCP Owner

BCP Owner	Contact Details
Managing Director	
Chief Operating Officer	
Head – Operations	
Head – Delivery	
Head – IT	
Head – Human Resources	
Head – Administration	
Chief Information Security Officer (CISO)	

7.1.2 Objective of Fire Evacuation Procedure:

- Fire safety is everyone's responsibility. This procedure is to ensure that all employees, third party vendors, contractors, and visitors are protected from the risks of fire.
- With this aim appropriate fire prevention/precaution measures, appropriate evacuation procedures shall be developed, drafted, implemented and periodically tested.
- Evacuation decisions shall be clearly communicated to employees to assure that they follow proper procedures. Head Administration shall execute evacuation plan for fire or make announcement for any other emergency. Head Administration / Manager Administration / any

other person in Admin authorized by Head Administration shall inform each department of CIPL personally or over the phone.

7.1.3 General Instructions:

- All staff must be familiar with the fire and evacuation procedures.
- The highest-ranking person who is physically present in each department is responsible for ensuring that all members of his/her department evacuate the area.
- As you exit, quickly check nearby restrooms, copier rooms, closets, etc. Accompany and help disabled personnel, visitors and any coworker who appears to need calm direction or assistance. If possible, lead them to the assembly area so that they may be accounted for.
- Before opening any doors, which are closed, please ensure that it is not unbearably hot to avoid any burn injuries.
- All staff must ensure that they are familiar with the alternative means of escape in case of fire and when regular routes are not available.
- Do exit quickly and calmly using the nearest fire exit and proceed to the designated point.
- Do NOT waste time in searching for your belongings, as life is precious.
- Do close the door behind you after ensuring that nobody is left behind; closed doors can slow the spread of fire, smoke and water.
- Do NOT use Lifts in case of any emergency situation e.g. Fire/Natural Disaster.
- Any staff on hearing continuously sounding fire alarm MUST leave area/building following the 'EMERGENCY EXIT' signage. Staff must be aware about the route signboards. On no account must they return to their own department.
- Check toilets and other areas for stragglers.
- The 'break glass' fire alarm call points can be found at following locations:
    - Near CIPL entrance door.
    - Opposite to lift.
    - Opposite to Data-Centre.
- Portable fire extinguishers are sited at following locations:
    - One near CIPL entrance door
    - One in lobby of way to Data-Centre
    - One in Data-Centre
    - One near desk of Head – Financial Process

7.1.4 Special Instructions for DC area:

Emergency Phone Numbers	Number
Police station - Control Room	**100**
Police station – Andheri MIDC **Police station – Pune**	**022-** **020-**
Fire Department - Emergency Dial	**101/022-**
Ambulance – For Accident - Emergency Dial	**102** **108**
Ambulance – Hiranandani Hospital	**022- 25763322\3323**

Hiranandani Hospital	**022- 25763333\300**

7.1.5 Fire safety precautions:

- Corridors, stairways, landings and escape routes must be kept clear at all times.
- All fire-fighting equipment must be kept free from obstruction and be readily available for use in an emergency. Portable fire-fighting equipment must not be removed or repositioned without authority from Administration Manager.

7.1.6 Any person suspecting or discovering a fire shall:

- Raise the alarm by breaking the glass of the nearest fire alarm call point.
- Inform Head Administration on phone or personally.
- If possible, tackle the fire with the correct type of extinguisher - but only if there is no risk to oneself and practical, "hands on" training has previously been undertaken.
- If circumstances dictate, or if ordered to do so, leave the building by the nearest available exit route.

7.1.7 Any Person on hearing the fire alarm:

- Decision to shut off electrical appliances will be taken by Head Admin based on the severity of the fire after due diligence procedure after communicated to concern officials.
- Leave lights on.
- If you lock your door, take your keys with you.
- Alert others around you.
- Assist people around you in evacuation process.
- When evacuating WALK, never run, and keep to the left of the hallways.
- Leave the building, even if the alarm stops while you are on your way out.
- Do not stop to collect your personal belongings
- Evacuate the premises in a calm and orderly manner using the nearest fire exit. NOT USING LIFTS and proceed to the designated 'ASSEMBLY POINT'.
- You may be specifically designated to switch off machinery in the event of a fire evacuation; you should do this prior to leaving, only if it is safe to do so.
- Do not return to the building until you have been told to do so.

7.1.8 Any person hearing a continuously sounding fire alarm shall:

- Leave the building by the nearest available fire exit route - NOT USING LIFTS
- Go directly to the designated assembly point i.e. near to the main entrance gate of the building.
- Never re-enter the building until the alarm is sounding.
- Instructions given in an emergency evacuation by the nominated staff must be followed and breaches of these procedures will be considered serious and may be dealt with disciplinary procedures.

7.1.9 Evacuation Drills:

- Fire evacuation drills shall be carried out by Admin Department in coordination with ISMS-IRT team/technology team for entire premises at least annually.

- The drills shall monitor the effectiveness of the local evacuation procedures and, where necessary, identify required changes.
- Reports on the effectiveness of drills shall be produced and presented by Admin to CISO, who in turn will present to the Apex committee.

7.1.10 Alarm Test:

- IT Manager / CISO in coordination with Admin department will test all fire alarms in CIPL during preventive maintenance once in six months.
- Preventive maintenance report of such test should be maintained.

7.1.11 Fire Extinguishers:

- Before you use a fire extinguisher you must know:
  - What fuel is burning?
  - What type of fire extinguisher is suitable for that type of fire?

Sr. No.	Type of fire	Category	Use on following fire types
1	Water	Class A (combustible Solids)	Wood, Cloth, Plastics, Paper
2	Foam	Class B (flammable Liquids)	Petrol, Oil, Paint
3	CO_2	Class C (flammable Gases)	Methane, Propane, Butane, Electrical equipment
4	Dry Chemical	Class D (combustible Metals)	Magnesium, Aluminum

7.1.12 Key Performance Indicators (KPIs)

- Proper communication of the procedure.
- Identification of floor coordinators and backups who clearly understand and will faithfully execute the established procedure for facility evacuation.
- Communication of the evacuation order to all persons within the facility.
- Providing an accurate accounting of the number of individuals in the building.
- Conducting an annual exercise of the plan to assure that information is up to date and assigned tasks are understood.

7.1.13 Incident Recovery Team

The following officers of CIPL, who are designated as having duties/responsibilities in reforms:

Name of Person	Designation	Duties/responsibilities in Reforms
	Head – Administration	Assist in evacuation decision
	Manager – Administration	Execute evacuation plan
	Manager – IT	Coordinator for work Area
	Head – HR	Coordinator for Resources
	Head – Delivery	Coordinator for Delivery Team
	Head – Operations	Coordinator for Operations Teams

Name of Person	Designation	Duties/responsibilities in Reforms
	System Administrator	Coordinator for DC Area
	CISO	To finalize & approve plan.

7.2 Business Continuity – Framework

7.2.1 Responsibility

The responsibility for developing and maintaining the business continuity plan lies with the Business Information Security Officer CISO along with the assistance of Management Information Security Forum (ISMF) comprising of key personnel from operational and support areas.

7.2.2 Framework

The BCP framework has been outlined based on the following;

- Identification and categorization of processes based on their impact to the organization if not available i.e. BIA (Business Impact Analysis).
- Use of proven principles in disaster recovery and business continuity:
    - Backup & recovery or operations at an alternate site.
- Extensive and elaborate plan on data backup and storage.
    - Offsite storage.
    - Onsite storage

7.2.3 Threat Consideration

Recovery strategy and plans are based on analysis of various threat events that can occur. Following is a list, illustrative and not comprehensive, of threat events that can occur are identified;
The threats are segregated into:

- Natural
- Accidental / Intentional – Technical Disasters
- Accidental / Intentional – Man Made disasters

Disasters	
Natural	FIRE
	THUNDERSTORMS & LIGHTNING (ELECTRIC STORMS)
	EARTHQUAKES
	LANDSLIDES & MUDFLOWS
	TSUNAMIS & OTHER TIDAL ACTION
	FLOODS & FLASH FLOODS
Accidental / Intentional (Human)	TERRORISM
	CYBER ATTACKS
	RIOTS/CIVIL UNREST

Disasters	
	PUBLIC PROTEST
	TAMPERING
	THEFT
Accidental / Intentional (Technical)	LOSS OF UTILITIES (WATER / POWER SUPPLY)
	VIRUS ATTACKS
	SYSTEM FAILURE
	HUMAN PANDEMIC VIRUS
	FUEL STORAGE

7.2.4 Categorization of Business Process

Following is the classification under which the various business processes will be classified under. This classification will aid in planning appropriate corrective and/or recovery action in case of a disruption.

Category	Description	Time to Recovery
Very Critical	All **very** c**ritical** processes where any disruption could lead to **High Impact** on business	2 Hours
Critical	All c**ritical** processes where any disruption could lead to **High or Medium Impact** on business	1 Day
Necessary	All n**ecessary** processes where any disruption could lead to average or **Medium or Low Impact** on business	1 Week
Desirable	All **Desirable** processes where any disruption could lead to **Low or No Impact** on business	1 Month

7.2.5 Business Impact Analysis and Recovery Strategy

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.

As part of the Business Continuity Plan business owners should undertake a Business Impact Analysis which will use the information in your Risk Management Plan to assess the identified risks and impacts in relation to critical activities of your business and determine basic recovery requirements.

The BIA report should identify and document the critical business functions and processes and the minimum assets required to restart the process after the disaster has occurred. RTO (Recovery Time Objective) and RPO (Recovery Point Objective) should be identified for each mission critical process based on which the recovery strategy should be decided.

RPO (Recovery Point Objective) refers to the amount of data at risk. It's determined by the amount of time between data protection events and reflects the amount of data that potentially could be lost during a disaster recovery. It is the amount of data loss tolerable by an organization. The time shall be recorded for further improvement for each incident.

RTO (Recovery Time Objective) is related to downtime. The metric refers to the amount of time it takes to recover from a data loss event and how long it takes to return to service. RTO refers then to the amount of time the system's data is unavailable or inaccessible preventing normal service. The time shall be recorded for further improvement for each incident.

The BIA report should prioritize the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first.

7.2.6 Business Impact Analysis Report

Refer to BIA Report

7.2.7 Recovery Strategy

Category	Recovery Provisions	
Critical and Very Critical	Hardware Recovery	• Preconfigured stand by equipment.
	Software Recovery	• Configuration backup/restoration. • Data backup/restoration. • Installation CD for Softwares
Necessary	Hardware Recovery	• Cold standby equipment. • List of Configuration Software and Configuration backup • Vendor list for purchase of equipment.
	Software Recovery	• List of Software to be procured. • Vendor list for purchase of software.

7.2.8 Continuity Maintenance

Ensuring that the Business Continuity Plan reflects on-going changes to resources is crucial. This task includes updating the Plan and revising this document to reflect the updates, testing the updated Plan and training personnel on the changes involved. The ISMF Members are responsible for this comprehensive maintenance task.

The ISMF will review the document once in a year or whenever there is a major change in the business to ensure that all critical changes required are incorporated into the continuity plan. Moreover, the document shall be reviewed at least once a year and approved by the Management Information Security Forum.

7.2.9 Organization of disaster response and recovery

For the Business Continuity of CIPL, two teams which handle the situation are Management Information Security Forum (ISMF) and Support Teams (IT, Admin, HR). In the event of a disaster, the ISMF provides general support; Support Team is concerned with resources and tasks integral to running the specific operational area.

The following is a list of each position on the ISMF, and a brief overview of each member's responsibilities:

Teams	Functions	Team Members
Information Security Management Forum (ISMF)	• Create BCP and approves the BCP • Declaration of emergency • Crisis Handling • Situation Monitoring and Assessment.	• CISO • Manager – IT • Managing Director • Chief Operating Officer • Head - Administration
Incident Recovery Team	• Damage assessment and notification. • Transportation of Recovery equipment / Media. • Liaison with Vendors to restore the systems • Recovery of Voice and Data Communications. • Liaison with Emergency services and Authorities. • Admin recovery	• CISO • Manager – IT • IT Team • Head – Human Resource • Head – Delivery • Head – Operations • Chief Operating Officer • Head - Administration

7.2.10 Event Identification and Response

Disaster detection

The detection of an event which could result in a disaster affecting IT systems at CIPL is the responsibility of any member of IT/ISMF Team or whoever first discovers or receives information about an emergency situation developing in the operational areas, premises, or the telecommunications lines, etc.

Disaster notification

The person who receives the notification or discovers the disaster will follow existing procedures and notify the individuals who is of the ISMF. The duty person on call will monitor the evolving situation and, if appropriate, will then notify the ISMF representative based upon a predefined set of notification parameters.

When a situation occurs that could result in the interruption of major systems or networks, the following people must be notified:

- Managing Director
- Chief Operating Officer
- Chief Information Security Officer – CISO
- Head – Delivery
- Head – Operations

- Head – Human Resource
- Head – Administration
- Head IT

7.2.11 Initiation of the disaster recovery plan

The responsibility for initiation of the disaster recovery plan lies with the CISO. The same can also be initiated by any member of the ISMF.

Activation of the designated alternate site

The responsibility for activating any of the designated alternate sites or back-up resources is delegated in the following sequence:

- ISMF
- CISO
- Any ISMF member in absence of CISO
- Any other officiating director in absence of both above mentioned entities

7.2.12 Disaster recovery strategy

The Disaster Recovery Strategy explained below pertains specifically to a disaster disabling the main business center located in CIPL.

Location – 1

Clover Centrum, Galaxy Society
Plot No 5, Boat Club Road,
Pune 411 001, India
Tele: +91 20 2616 0022 /23 /24
Fax: +91 20 5601 4881

Location – 2

2nd Floor, Dhana Singh Processors Building,
Vazir Glass Lane, J B Nagar, Andheri (East),
Mumbai- 400 059, Maharashtra, India
Tele: +91 22 29261650
Fax: +91 22

This section addresses three phases of Disaster Recovery:

- Emergency Phase
- Backup Phase
- Recovery Phase

Emergency Phase

The Emergency Phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures direct efforts to protect life and property, which is the primary goal of initial response. Security over the area is established as local support services such as the police and fire departments are enlisted through existing mechanisms. The ISMF personnel is alerted by mobile / SMS and begins to monitor the situation.

If the estimated outage is less than 2 Hours, recovery will be initiated under normal IT systems operational recovery procedures. If the outage is estimated to be longer than two hours for critical events and 1 day(s)/1 week in necessary events, the Business Information Security Officer-Head will declare the situation as disaster and the continuity of business plan is activated. The recovery process then moves into the back-up phase.

The ISMF remains active until recovery is complete to ensure that the teams will be ready in the event the situation changes.

Backup Phase

In the initial stage of the back-up phase, the goal is to resume critical activities within the least possible time. Activities will resume either at the original site or at the designated alternate site, depending on the results of the assessment of damage to equipment and the physical structure of the building.

In the back-up phase, the alternate site will support Critical functions / processes for up to one week and as many Necessary business functions / processes as resources and time permit. During the backup phase period, the processing of these systems resumes, possibly in a degraded mode, up to the capacity of the alternate site. Within this one week period, the operations will be returned to full operational status.

Proposed Alternate Site:

Location – 1

Mumbai Site shall become alternative site for Pune

Location – 2

Pune Site shall become alternative site for Mumbai

Recovery Phase

The time required for recovery of the functional area and the eventual restoration of normal activities depends on the damage caused by the disaster. The timeframe for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated alternate site. The primary goal is to restore normal operations as soon as possible.

7.2.13 Roles and Responsibilities

Role	Responsibilities
CISO	As an ISMF Coordinator, he provides liaison between CIPL ISMF Team, and the support teams in affected areas. The CISO is also responsible for on-going maintenance, training and auditing of the continuity plans. In absence of the CISO, the member from ISMF will take over the co-ordination activities in the event of a disaster.
ISMF Team	The following shall be the functions of the ISMF: Oversee development maintenance and testing of the Recovery plan And in the event of a disaster shall include: • Receive an initial assessment of the nature and extent of the problem. • Decide whether to activate the Plan. • Alert all Recovery team leaders. • Alert and mobilize all other team members. • Make a preliminary (verbal) report to senior management. • Make a second, more detailed, report to senior management on the content of the meeting and the actions being taken. • Report progress to senior management. • Document progress against agreed schedules. The team is composed of key management personnel from each of the areas involved in the recovery process. The team interfaces with and is responsible for all business continuity plans and planning personnel at CIPL.
Incident Recovery Team	Incident Recovery Team comprises of the CISO, IT team, Admin team and at least one member from every business processes identified. In event of a disaster the Incident Recovery team is responsible to work closely with the ISMF. The support team will maintain contact list of all the vendors for their respective business operations and will liaison with them to recover and restore the business operations.

7.2.14 Recovery Plan

Threat	Recovery Plan
Fire, Electric Storms, Earthquakes, Floods, Terrorism, Riots, Protest, Theft, Loss of utilities.	In case of inability to carry out operations at the current location due to the threats, the ISMF/CISO will activate the alternate location for carrying out the operations. In which case, the alternate location's Admin-in-charge shall be informed, whereby he shall mobilize the required resources necessary to operate from the alternate location. Prerequisites and assumptions; All servers are present in the data-center and can be accessed from the alternate location. The minimum required Infrastructure (Laptops, Desktops, Internet connectivity, and Data cards) is present in the alternate location.

Threat	Recovery Plan
	Data loss up to 1 day is tolerable for Networks, Server, and IT teams. The data required, to carry on operations after disaster, can be reconstructed from the backups stored onto the file server.
Hardware Failure Recovery	In case of failure of critical hardware equipment, the support team will try to resolve the problem at the earliest. If the problem is severe, arrangements will be made to start using backup / alternate equipment. If the equipment is not available, attempts will be made to procure new equipment at the earliest through either purchase or lease.
Software Failure Recovery (System Failure)	In case of failure of critical software or operating system, the IT teams will try to resolve the problem at the earliest. If the problem is severe, arrangements will be made to start using backup / alternate machines with the relevant software. In addition, the IT team will try to reinstall the software on the same machine or install on a new machine if necessary. In case of loss of data, the support team will restore the most recent backup.
Virus Attack Recovery	The affected machines will be immediately isolated from the network. Attempts will be made to clean-up the infected machines using the anti-virus software. If the machines are still not cleaned up, the machines will be formatted after obtaining due permissions from the relevant personnel. If possible, backup of clean data will be taken before the formatting and restored after formatting. After restoration, the machine will again be checked for virus infections.
Cyber Attacks	The affected machines will be immediately isolated from the rest of the network. If necessary, the firewall / machine(s) connected to the internet will be disconnected. Simultaneously, attempts will be made to trace the source from where the attack took place. Relevant authorities will be notified. There will be a general stock taking done to assess the damage done due the attack. If there is any loss of data, the most recent backups will be restored. As a General Precaution, the administrator, super user, and other passwords of the affected machines will be modified.
Vendor Support Failure Recovery	It is necessary at CIPL to maintain the preferred vendor list for any service that is outsourced. Depending on the criticality of the service either the next vendor on the list would be approached or a fresh vendor evaluation.
Pandemic Human Virus	In case of Pandemic Human Virus, Employees may not be able to reach office location due to lockdown declared by State or Central Govt. In this case, employees will have to perform their activities by “Work from Home” Concept. Employees requires Machine (Laptop / Desktop) and VPN connectivity to shared drive data as well as server data, Mobile connectivity, access to mails and tools for video conferencing connectivity. Even employees are required to take backup of their important official data/ files on their local drives. All of the organizational employees are required to follow Guidelines for Pandemic.

7.2.15 Incidence Recovery Team email – IRT@clover.com

Internal

Title	Name	Office	Residence	Mobile
CISO		022-		
Head – IT		022-		
System Admin head		022-		
IRT team		022-		
Network Team		022-		
Head – Delivery		022-		
Head – Operations		022-		
Head – Administration		022-		
Head – Human Resource		022-		

- The personnel are equipped with mobiles and they can be contacted directly.
- The duty persons will monitor the situation and determine if it has the potential to affect ability to extend services.

External Authorities

- Available with Administration / IT Team

7.2.16 IRT coordinator

This sub-section contains instructions to the IRT Coordinators for overseeing disaster response and recovery efforts.

Action Procedures:

- Coordinator to ensure that the entire IRT have been notified.
- Coordinator to meet with Incident Recovery team to review their findings and present results to IRT.
- Coordinator to present recommendations to IRT for next steps in recovery effort.
- Coordinator to begin notification of recovery. Check to ensure all recovery participants have been notified.
- Coordinator to monitor the activities of the recovery teams. Assist them as required in their recovery efforts.
- Coordinator to report to IRT on a regular basis on the status of recovery activities.
- Coordinator on an hourly basis or other appropriate interval updates the recovery status information to the CISO.

7.2.17 Support Team

This sub-section contains instructions to the Support Team Coordinators for disaster response and recovery efforts.

Action Procedures:

- Receives report of disaster.
- Oversees assessment of damage to infrastructure and telecommunications facilities. Directs contingency and recovery efforts.
- Provide updates to IRT on a regular basis.

- Arranges for voice and dial-up data communications services to support critical functions. Procures stock to repair or replace damaged equipment. Restores full services in a timely manner.
- Assists other departments with relocation and restoration of data facilities.

7.2.18 Rehearse, Maintain and Review.

It is critical to rehearse this business continuity plan to ensure that it remains relevant and useful. This may be done as part of a training exercise and is a key factor in the successful implementation of the plan during an emergency.
IRT shall ensure that BCP activities are regularly reviewed and updated, to maintain accuracy and reflect any changes inside or outside the business. BCP activities shall be reviewed once a year.

The following points may help:

- A training schedule must be prepared for all people who may be involved in an emergency at the site.
- Pay attention to staff changes.
- It is best to use staff titles rather than names.
- If there is a change in the organizational structure or suppliers/contractors this must be amended in your plan.
- After an event it is important to review the performance of the plan, highlighting what was handled well and what could be improved upon next time.

7.2.19 BCP Testing

The following points will be covered in the BCP tests which should be conducted as per the frequency defined by ISMF; records of the tests should be maintained by CISO:

Parameters	**Frequency**
Fire and Evacuation Drill	Once in a year
Review Call Tree/Emergency Contact Numbers	Once in a year
Uninterrupted Power System Testing	Once in 3 months
L3 (Layer 3) switch testing	Once in 6 months
BCP Activities Review	Once in a year
Redundancy Test for WAN	Once in 6 months

7.2.20 Business Continuation Plan Activities

The following points are considered as Business Continuity Plan activities at Pune & Mumbai:

SN	Details	Location	Number of Team members	Size of Data	Description/ Server user for	Backup details	BCP
1	Backup Server	Pune & Mumbai	50	150GB	This Server Contains backup of all users' servers.	Hard Drive, Backup Tapes	We execute weekly backup on USB Hard drive and monthly backup of Tape Drives. In-case any hardware failure we can restore it from the USB or tape drives. We execute daily backup on HD1 and rotate HD2 drive on a fortnightly basis and send it to an offsite location. We also take monthly backup at the end of the month on Tape Drive. As per our IT Policy, also we take fortnight backup every 15 days
2	CCTV Servers	Pune & Mumbai	-	20GB	This server used for CCTV monitoring	N/A	We can install CCTV. No restoration required as this s/w is in-built with its DVR card and data can be restored from the local HDD connect to old DVR
3	Domain Controller	Pune & Mumbai	50	100GB	This server is domain controller	Backup server	We do manual snapshot backup and also have additional ADC. If hardware is available we can do reinstallation in max 3 Hours, else it will take 1 day to procure hardware or take it on leases from vendor "Domain Services".

SN	Details	Location	Number of Team members	Size of Data	Description/ Server user for	Backup details	BCP
4	Anti-Virus	Pune & Mumbai	50	100 Gb	This server is McAfee Antivirus Server	Backup Tapes	We take snapshot backup for Antivirus Servers. Also we can install Antivirus on another machine with same port & IP. If hardware is available we can do this in max 3 Hours else it will take 1 day to procure or take on leases Hardware from vendor “Domain Services”
5	Firewall	Pune & Mumbai	50	80GB	This is Hardware Firewall	Mail	We have scheduled daily automatic backup for the configuration which is coming daily on infra group mail. Pune Location -We have a dual redundancy Firewall in Active & Passive mode with Sophos (Active) & Cyberoam (Passive) for Mumbai location – We can make this device available in 4hrs through vendor “SM Technologies”.
6	Leased Line	Pune & Mumbai	50	--	ISP’s	Alternate ISP’s or USB Dongle (Photon)	We do not have to do anything manually as we have done load balancing through firewall & we have 2 ISP’s for redundancy 1 are wired and 1 is on RF also we can configure external dongle like photon on it.
7	Laptops	Pune & Mumbai	5	--	--	Spare Laptops from Mumbai location	Spare laptop from Mumbai location
8	Desktops	Pune & Mumbai	45	--	--	Spare Desktops from Mumbai location	Spare Desktops from Mumbai location
9	Data card	Pune & Mumbai	3	--	--	Spare Data Cards from Mumbai location/ Or new Procurement max 1day.	Spare Data Cards from Mumbai location/ Or new Procurement max 1day.

Note: In case backup server, backup tape crash we can restore data from backup tape which we send every Month to MD resident for safe storage.

7.2.1 Different Scenarios

The following different scenarios are considered at Pune & Mumbai:

Sr. No.	Situation	Present BCP	Expected Down time	Expected loss of data	Remarks
1	When one Lease Line is down	Alternate ISP's or Dongles	No Downtime as Load balancing	No data loss No Productivity affected	---
2	When all Lease Lines are down	Data Card for Seniors and Connect Team use Data Card for Connectivity	Immediate	No Data Loss and no Loss of Productivity affected	On Firewall We can Configure external USB dongle like Photon for Internet connectivity
3	Electricity failure	UPS & Generator	No downtime	No data loss	In case MSEB electricity goes down we 1st switched on UPS & within 2mints we automatically shift on generator. All machines connected to UPS & UPS has power supply of MSEB & Generator. Generator has 340 ltr capacity of diesel we have always min 160ltr in store on that we can work 24hrs if it extends we have to purchase diesel only.
4	Server Crash	Restoration from Backup Server or Backup Tape or	3 hrs to Max 1day	One Day Data Loss	Since backups are done on Daily, Weekly and monthly basis there would be no data loss.
5	Earthquake	Restoration from Backup Server or Backup Tape / Hard Drive	for setting up Infra we will need max 2 days	2 weeks data loss	In case of an earthquake we will use Deccan Warehouse Deccan Warehousing Sr.No.70, Vadgaon Tal-Maval Dist-Pune as standby premises, also we can use cloud computing option available for setting up Infra
6	Fire	Restoration from Backup Server or Backup Tape / Hard Drive	for setting up Infra we will need max 2 days	2 weeks data loss	In case of an Fire we will use Deccan Warehouse as standby premises, also we can use cloud computing option available for setting up Infra

Sr. No.	Situation	Present BCP	Expected Down time	Expected loss of data	Remarks
7	Riots	Restoration from Backup Server or Backup Tape / Hard Drive	Depending on situation	2 weeks data loss	All our VIP Users are using Laptop. Desktop will be bought on rent basis for connect Users & will move Hardware to Deccan warehouse. For internet they will use data card
8	Flood	Restoration from Backup Server or Backup Tape / Hard Drive	Depending on situation	2 weeks data loss	All our VIP Users are using Laptop. Desktop will be bought on rent basis for connect Users & will move Hardware to Deccan warehouse for internet they will use data card
9	Pandemic Human Virus	Work from home and access to servers and shared drive through VPN	Depending on situation	Depending on situation	In case of Pandemic Human Virus, Employees may not be able to reach office location due to lockdown declared by State or Central Govt. In this case, employees will have to perform their activities by "Work from Home" Concept

8.0Quality Mechanisms

- Review of Fire Safety Equipments
- *Review of Emergency Contact Details*
- *Review of Fire Drill Records*
- *Review of Business Continuity Testing Report*
- *Review of Incident Recovery Team Members List*
- *Review of Business Impact Analysis Report*
- *Review of Disaster Recovery Strategy*
- *Review of Roles and Responsibilities of Disaster Recovery Team*

9.0Security Objectives

Sr. No	*Objectives*	*Responsibility*	*Frequency of Measurement*	*Reporting of Measurement*	*Target to Achieve*
1	Business Continuity Incidents	ISMF	Six Monthly	Incident Request	Not to exceed 2
2	Business Continuity Testing	ISMF	Six Monthly	Business Continuity Testing Report	100%

10.0 Identified Risk

- All risks identified for the process will be recorded into the Risk Assessment Sheet
- Risks will be reviewed and monitored as per the agreed schedule

11.0 Exit Criteria

Outputs
Fire Safety Equipments Maintenance Reports
Emergency Contact List
Fire Drill Records
Business Continuity Testing Report
Business Continuity Disaster Recovery Team Members List
Business Impact Analysis Report
Disaster Recovery Strategy
Roles & Responsibilities of Disaster Recovery Team