Annexure-S5

BUSINESS CONTINUITY PLAN (BCP)

OF

INDIAN GAS EXCHANGE

4th & 5th Floor, Plot No 7, TDI Center, Jasola
New Delhi - 110025, India
Tel.: (+91 11) 43004000.
www.IGXindia.com

TABLE OF CONTENTS

INTRODUCTION

1. PURPOSE

The purpose of this Business Continuity Plan is to prepare **Indian Gas Exchange Ltd. (IGX)** in the event of extended service outages caused by factors beyond control (e.g., natural disasters, man-made events), and to restore services to the fullest extent possible in a minimum time frame. All operational teams are expected to implement preventive measures whenever possible to minimize failure and to recover as rapidly as possible when a failure occurs.

2. SCOPE

The intended scope and use of this Business Continuity Plan are to minimize the impact of any unexpected occurrence – not only to the Technology, but also to the entire organization. This plan does not address any one type of contingency, as all disruptions tend to be unique. The scope goes far beyond the technical complexities of recovering disrupted computing platforms or networks. It addresses all possible complexities that may arise in a worst-case scenario.

The geographical scope of this Business Continuity Plan extends to the business operations at the following premises:

Head Office	**Branch Office**	**Data Center (Primary)**	**Data Center (DR)**
Indian GAS Exchange Ltd. 4th & 5th Floor, Plot No 7 TDI Center, Jasola New Delhi - 110025, India.	Indian GAS Exchange Ltd. 904, 9th Floor Meadows, Sahar Plaza, JB Nagar, Andheri Kurla Road, Andheri East Mumbai	Data Center-Delhi Tata Communication Nextgen Tower, 4th Floor, Ho Chin Marg, Opposite Savitri Cinema Flyover, Greater Kailash-1, New Delhi-110048	Tata Communication IDC A Wing, 3rd Floor, Kashinath Dhuru Marg, Dadar West, Opposite Kiti Collage, Prabhadevi, Mumbai: 400028

3. OBJECTIVES

The objectives of this plan are:

- To develop an effective Business Continuity Plan to resume operations of critical departments within a given time frame in case of any disruption or disaster.
- To define Roles & Responsibilities of all the teams involved in Business Continuity and Disaster Recovery.
- To define schedules for training and awareness on Business Continuity.
- To define the schedule and mechanisms to test this plan.
- To ensure that all critical activities to support business operations are available.
- To minimize the likelihood and impact (risk) of disruption.

4. BUSINESS CONTINUITY PLANNING SCENARIOS

Any event, whether anticipated (e.g. floods) or unanticipated (a blackout or earthquake), leading to a large-scale impact on IGX functioning and reputation affecting the organization's credibility to deliver quality services in a secure environment shall be termed as a disaster.

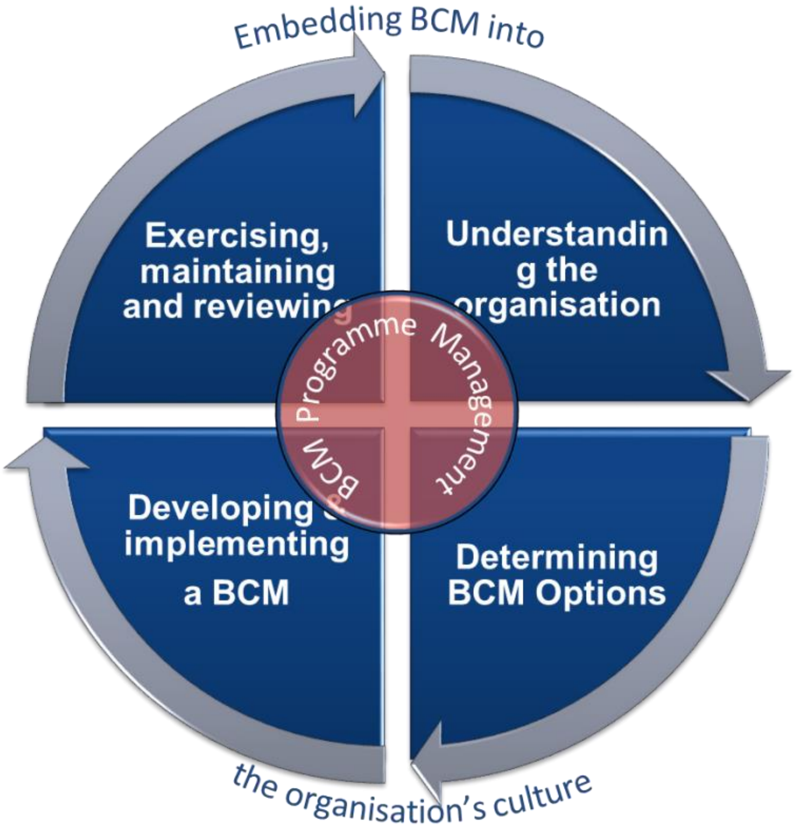
This Plan mainly focuses on the disruption caused by the following scenarios:

- → **Catastrophic events** resulting into a major disruption of services and complete processing capability cannot be achieved for a substantial period. In these cases, recovery will require use of alternate processing site (DR Site) as well as offsite offices for employees over an extended period. Some examples of such events are earthquake, acts of terrorism, etc.
- → **Disastrous events** where overall business infrastructure may experience a severe disaster resulting in the total shut down and complete processing capability of all business processes may be down. Further, key personnel may not be able to access the premises and lead to non-availability of key resources in the building. Some examples of such events are fire, riots/ civil unrest, power shutdown, etc.
- → **Moderate outages** where some or all business processes at the location may experience moderate damage / outage. Processes may not continue or may run at a degraded level. In such cases, an alternate site may not be required for continuing business, but alternate equipment / redundant network links / restoration of back-up may be required depending on the criticality of the business process and infrastructure. Some examples of such outages are LAN switch or router failure, damage of equipment due to power surge, temporary power failure, core access layer switch failure, server crash, data corruption, etc.
- → **Minor outages** where business processes may experience minor damage / outage and will run at a sub-standard level. Some examples of such outages are link connectivity being temporarily down, switch or router port failures, System or network CPU failures, System Fan failures, System or Network Power supply failures, Ethernet card failures, etc.

In case of problems at Clearing Banks Primary Site, we will connect to their respective DR site. In case

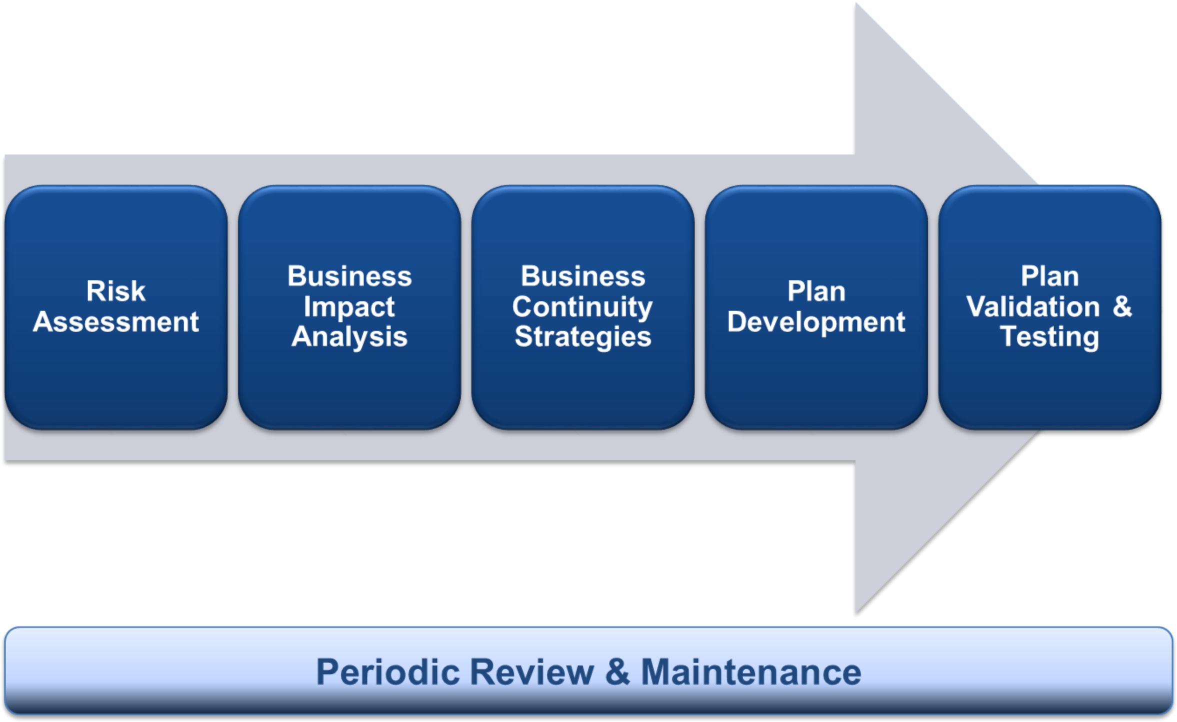
IGX BCM APPROACH & BCM PROCESS

1. BCM APPROACH -


Embedding BCM into
Understandin g the organisation
Determining BCM Options
Developing & implementing a BCM
Exercising, maintaining and reviewing
BCM Programme Management
the organisation's culture

BCM approach is developed from the guidance on the way in which recovery can be affected. Regular assessment needs to be done based on the process change and implementing the change.

2. BCM PROCESS -


Risk Assessment
Business Impact Analysis
Business Continuity Strategies
Plan Development
Plan Validation & Testing
Periodic Review & Maintenance

BCM process needs to be assessed by doing risk assessment of the respective department. Process impact analysis needs to be done and accordingly BC strategies need to be defined.

A plan needs to be developed by doing testing at regular interval. Results of the testing needs to be analyzed which will help in validating the BCM process.

Business Continuity Management is a holistic management process that identifies potential impacts that threaten Exchange and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

BCM Policy and Program Management

The BCM Policy of IGX provides the framework around which the BCM capability is designed and built. BCM policy describes the scope of the program and assigns responsibilities. An effective BCM program requires the participation of various managerial, operational, administrative, and technical disciplines that need to be coordinated throughout its life cycle using procedures such as those outlined in BCP and DR Plan.

Though Business Continuity Management is primarily a planning activity, it is inevitable that the BC team will be expected be ready to respond and ready to provide a lead during incident response.

Understanding the organization

Understanding the Organization is the first step to develop an appropriate Business Continuity Management program. It also requires understanding the urgency with which activities and processes need to be resumed if they are disrupted. To understand the organization better information to be gathered by asking such questions as mentioned below: -

- What are the objectives of the organization and objectives are achieved?
- What are the products/services of the organization?
- What applications, systems, data, people, assets are required (both internally and externally) in the delivery of products/services?
- What are the time imperatives on their delivery?

Determining BC Strategies

This section is about determining and selecting Business Continuity Management Strategies to be used to maintain the organization's business activities and processes though an interruption. Business Continuity Management Strategies concern:

- The selection of alternative operating methods to be used after an interruption to maintain or resume the organization's business activities and their dependencies (internal and external) to a priority.
- The protection of vulnerabilities and single points of failure in business-critical processes identified in the Risk Analysis.

Corporate strategies

Key decisions at a corporate level are:

- Recovery Time Objective for each activity (based on the MTPOD)
  Separation distance of alternative facilities and data storage considering Recovery Point Objective

Activity Level Strategy

At the Activity Level the complexity of interdependencies on services, business processes, data and technologies need to be analyzed and appropriate tactics chosen to address the needs of:

- People, workforce, skills, and knowledge
- Premises
- Supporting technologies
- Information
- Equipment and supplies
- Stakeholders, partners, and contractors.

The organization should also:

- Understand the role of local emergency responders
- Reduce the likelihood of specific perceived threats
- Take appropriate impact mitigation measures

Resource level consolidation

This step consolidates the resource requirements of the various business activities across the organization and ensures that those meet both in scale and within the required timeframe.

Developing and Implementing a BCM

The aim of the various plan(s) covered in this stage is to identify in advance, as far as possible, the actions that are necessary and the resources which are needed to enable the organization to manage an interruption whatever its cause considering the BCM strategies derived in earlier stage.

Exercising, Maintenance and Review

A Business Continuity Management (BCM) capability cannot be considered reliable until it has been exercised, then maintained and reviewed.

Exercising

The development a BCM capability is achieved through a structured exercising program; to be successful an exercising program must begin simply and escalate gradually.

Maintenance

The BCM Maintenance Program ensures that the organization remains ready to handle incidents despite the constant changes that all organizations experience.

Review

An audit function is one of self-assessment or impartial review against defined standards and policies and to provide remedial recommendations. However, BCM may require a different audit approach because standards are constantly evolving. The BCP/DR Test Plans details the review mechanism.

Embedding BCM in the organization’s Culture

It is necessary to embed Business Continuity as culture to the Organization. It is vital to develop a BC culture to maintain readiness and effective response at all the levels. It is necessary to understand current level of awareness in the organization and then plan for designing components of awareness program. Detailed workshops for core team members and all employees to create awareness and educate all the members about their roles and responsibilities also should be planned. The awareness campaign should be reviewed as an ongoing task to identify any effort required to maintain it at an acceptable level.

IGX BC POLICY

1. MISSION

IGX aims to safeguard the organization's interest including key stakeholders, brand, reputation, and value through business continuity management – a process which identifies potential risks, their impacts, builds resilience and ensures capability for an effective response including effective crisis management. IGX seeks to ensure that all concerned departments meet their key responsibilities and help ensure that any regulatory obligations are satisfied.

2. POLICY STATEMENT

IGX has a BCP Policy Statement on Business Continuity Planning, which contains the following instructions:

- There shall be an approach in place which clearly defines the accountability, structure, roles, and corresponding responsibilities.
- For critical processes, recovery plans shall be in place as well as detailed guidance on recovery of critical resources and vital records.
- A training program shall be undertaken to ensure that all staff members are aware of their responsibilities in the event of a disaster.
- Business Continuity Plan shall be periodically tested to ensure that it can be implemented during emergency situations.
- Business Continuity Plan shall be reviewed on yearly basis, to consider changing circumstances, and to ensure its adequacy.

IGX - OVERVIEW

Indian Gas Exchange Ltd. (IGX) is India's first automated national level trading platform to promote and sustain an efficient and robust Gas market and to foster gas trading in the country. The platform features multiple buyers and sellers to trade in spot and forward contracts at designated physical hubs. IGX is a neutral and transparent marketplace where both buyers and sellers will trade Gas as the underlying commodity. The contracts traded at IGX are for compulsory specific physical delivery and settlement of the trade are subject to the condition that such contracts are non-transferable in nature and without any netting-off thereby. IGX enables efficient and competitive discovery of gas prices and one of its most important objectives is also to maintain market integrity.

DEPARTMENT OVERVIEW

Indian Energy Exchange Limited is the parent organization of IGX. Currently IGX is functioning in collaboration with IEX in terms of support & services from different departments of IEX. IGX are facilitated by various departments as below:

<u>IGX Departments</u>	<u>Shared Departments (Support & Services) with IEX</u>
1. Regulatory • *Surveillance* • Membership 2. Market Operations Departments • • Clearing and Settlement function • Delivery 3. Strategy 4. Business Development and Membership	1. Information Technology • Information Technology (System, Network, Security, Private Cloud) • IT - Local Enterprise (Managing Enterprise IT infrastructure) 2. Finance and Secretarial 3. Human Resource 4. Administration 5. Regulatory & Compliance 6. Policy and Communications

ROLES AND RESPONSIBILITIES

Business Continuity Roles and Responsibilities		
TEAM	MEMBERS	RESPONSIBILITIES
BCP Management Team (BMT)	→ Managing Director. → Head - Market Operation. → Head - IT → Head - Admin → Head - Finance → Head - HR	On-going Support → To review the results of Business Impact Analysis and approve the same. → To review DR drill report. → Approving enhancement of DR set up, if any findings in DR drill report. → To allocate resources for effective management of the business continuity initiative. → To authorize and communicate BCP roles and responsibilities to all concerned. → To advise various teams on business continuity plan conflicts, incongruities, etc. → To oversee progress on the implementation of business continuity plan/ disaster recovery plan. → Approval of overall BCP and changes therein. During Disaster → To analyze the details provided by the IMT and to decide further action plan → To declare Emergency / Disaster and invoke BC Plan in the War Room → To notify concerned Team Members about an Emergency and direct them to operate as per action plan → To advise various teams on the execution of BC and DR Plan → To oversee the execution of the BC Plan and advise team members, in case of conflicts

Business Continuity Roles and Responsibilities		
TEAM	MEMBERS	RESPONSIBILITIES
		→ To ensure timely communication about the emergency situation to the Regulator, members and Media. → To review the reports prepared by the various teams during recovery phase Refer to Annexure - E Guidelines for Management
Damage Assessment Team (DAT)	→ HOD - Systems & Networking → HOD - Administration Department →	**During Disaster** → To ensure effective execution of the actions / directions given by the BCP Management Team → To assess the physical damage incurred due to the disaster and report the same to the BCP Management Team → Summarize the damage assessment report for submission to the Management → To decide on procuring required IT infrastructure based on Damage Assessment and support DRT (Disaster Recovery Team)
Disaster Recovery Team (DRT)	Representatives of Systems & Networking, Admin, and HR	**On-going Support** → To ensure full functioning of alternate site in case of disaster at Primary Data Centre → To ensure proper replication of data at disaster site → To participate in mock drills as per plan **During Disaster** → To take charge of the respective teams for execution of DR Plan as per Management authorization → To co-ordinate with other teams as and when required

Business Continuity Roles and Responsibilities

Team	Members	Responsibilities
		→ To cross verify required applications on the critical user's machines → Acquisition of necessary assets/products during disaster with adequate approval, if required → To arrange other necessary equipment like Printers, FAX or any other communication devices etc. → To set up and route the network as per DR plan → To ensure full functioning of Primary Data Centre at the earliest after the occurrence of disaster → Acquisition of necessary assets/products to restore primary site → Setup the site at earliest and restore the operations at earliest. → To prepare/ update reports for Management Information
Floor Marshalls	Representatives from Admin Team as communicated from time to time	**On-going Support** → To provide necessary training to employees on how to safeguard themselves, in case of fire explosion **During Disaster** → To guide and instruct all the employees for evacuation, in case of fire explosion or any other eventuality in the premise → To douse the fire if there is no risk to one's self → To make necessary arrangements of medical facilities, in case of any emergency
Human Resource (HR)	→ Head - HR	**On-going Support**

Business Continuity Roles and Responsibilities		
TEAM	**MEMBERS**	**RESPONSIBILITIES**
	→ Executive - HR	→ To Handle Key personnel issues → Responsible for Internal Communications → To conduct internal trainings for fire-fighting, pandemic awareness etc. → To schedule BCP awareness training in consultation with the Management **<u>During Disaster</u>** → To provide necessary medical assistance to the employees, in case of emergency → To inform family members of the affected staff
Administration (Admin)	→ Head - Admin → Executive - Admin	**<u>On-going Support</u>** → To ensure that periodic mock drills are conducted within IGX → To ensure that a good level of hygiene is maintained within the premises (DR site and Primary Data Centre) → To keep in touch with Meteorological Department for any natural calamity and communicate the same to all concerned → Maintaining Physical Access Control at all the access points` → To manage and maintain company vehicles **<u>During Disaster</u>** → To arrange for necessary transportation at the time of disaster/ interruption → To make necessary physical security arrangements during the movements and transportation → To ensure food supplies and water for the team members, in case of continuity plans are invoked

Business Continuity Roles and Responsibilities		
Team	**Members**	**Responsibilities**
		→ To procure required assets for recovery from disaster / interruptions → Arrangement of Ambulance/ Hospital / hotel, if required → To provide necessary administrative support required by other teams

IGX - Business Continuity Strategy

IGX seeks to ensure that the critical business activities such as Market Operations, clearing & settlement and Customer Support related activities are continued, even in aftermath of a disruptive event. Therefore, any such event that prevents IGX from doing so will be met with immediate and appropriate corrective action. As a rule, the BMT shall assess all the risks to reduce the potential requirement to recover IGX operations.

The following initiatives have been taken by the IGX to establish a Business Continuity Plan that meets organization objectives in an effective and efficient manner:

→ The assets required to perform these business processes have been identified with the respective Maximum Allowable Outage (MAO), Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

RECOVERY STRATEGIES

1. RECOVERY MEASURES

Recovery measures adopted shall aim to minimize the impact of any unexpected occurrence - not only to the technology, but also to the entire organization. The priorities that must be established when planning for and coping with a disaster are:

- **Priority 1**—Safety of personnel (employees, visitors, contract staff).
- **Priority 2**—Safety of Trading files and Member records.
- **Priority 3**— Safety of own office records.
- **Priority 4**— Safety of office equipment, furniture, and fixtures.
- **Priority 5**— Preservation of profitability and productivity.

2. PROCESS CRITICALITY RATINGS

All critical processes are given preferences for recovery with their RTO and RPO. During the 'Business Recovery Phase', preference of restoration to operational status would be given to processes in the order of criticality rating with 1 being high criticality, and 3 being low.

Process Criticality			
Sr. No.	**Department**	**Processes**	**Critical Rating**
1.	Technology (Systems, Networking & IT)	Configuring Production Systems, Network, Firewall and other IT Infrastructure, Cloud for resuming operations.	1
2.	Market Operations	Starting Monitoring and Surveillance Activities	1
		Starting Clearing & Settlement Activities and Delivery Activities	1
3.	Finance & Accounts	Funds Pay-in & Pay-out	2
4.	Other Departments operations	Others	3

Exchange should go live with all critical operations within 2 hours. Application-wise Recovery Time Objectives are as follows:

MAO and Recovery Time Objectives for IGX IT Applications				
Sr. No.	**Application**	**Timeframe of MAO**	**Timeframe of RTO (Switch Over)**	**Timeframe of RPO**
1.	All Trading Applications (Forum Match, Custody,	1.5 Hour	1 Hour	5 Mins

MAO and Recovery Time Objectives for IGX IT Applications				
Sr. No.	Application	Timeframe of MAO	Timeframe of RTO (Switch Over)	Timeframe of RPO
	UTrade, Member Connectivity			
2.	Account Application	2 Hours	-	-
3.	Microsoft Office (Email, Sharepoint, OneDrive etc.)	2 Hours	30 Mins	15 Mins
4.	HR software	1 Day	1 Day	30 Mins
5.	Document Storage	1 Day	1 Day	-

3. Alternate Sites

In the event of any incident severely impacting the capability to operate from the Primary Data Centre (PDC), the operations will be continued from the DR Site

Address of the DR Site:

Indian GAS Exchange Ltd.

904, 9th Floor Meadows,
Sahar Plaza, JB Nagar,
Andheri Kurla Road, Andheri East
Mumbai

Mumbai (DR Site, TCL Private Cloud):

Mumbai: Tata Communication IDC, A Wing, 3rd Floor, Kashinath Dhuru Marg, Dadar West, Opposite Kiti Collage, Prabhadevi, Mumbai: 400028

4. BCP / DR Plan Location

A hard copy of the organization's BCP is located at the Primary Site and the DR site and may be accessed by contacting Head-IT. Latest electronic copy of this plan is located internally shared drive.

5. Succession Planning

Key personnel are endowed with specific authorities and responsibilities. They are usually people from the top management including directors, Head of Departments, and other staff who are accountable for directing the various functions of the exchange and whose unique knowledge and skills presumably add value to the exchange. Succession planning is very important factor of the BCP which enables an orderly and predefined transition of leadership within the organization.

Designee has been identified to ensure ability to manage and direct essential functions and operations. If none of the designees are available at the time of the declaration, the manager to which the key position normally reports should be notified and that manager will assign an appropriate designee from the staff available. The table below depicts the nominations of management personnel who shall take the charge in the absence of key person:

Key Positions and Lines of Succession

Succession Planning	
Key Person Title	**Designees Title**
Managing Director & CEO	Director
HOD – Market Operations	AVP – Market Operations
HOD – Business Development	AVP – Business Development
Chief Financial Officer	AVP - Finance
Head – IT/CTO	AVP - IT

RULES FOR DATA LOSS

IGX is committed to achieve minimal data loss (near to zero data loss) by implementing state-of-the-art DR solution.

Realtime data replication between PDC to DR site is implemented by using DB based replication.

There could be some scenarios where objective of “near to zero data loss” may not be achieved. Some of such scenarios are mentioned below: -

- Order received to the IGX Trading server but not written to database at the primary site.
- Order written to the Database at Primary Site but not written to database at DR Site
- Orders lost during transit between primary site and DR site.

In the worst-case scenario, if there is data loss when switching to the DR Site, the following guidelines shall be observed:

- If DR happens before 12.00 PM, post switching to DR site, Exchange will provide market to members to verify their orders/ bids.
- If any discrepancy found, members would be allowed to update their bid.
- If DR happens after 12.00 PM and before matching, post switching to DR site, Exchange will provide market to members to verify their orders by Exchange.
- If DR happens after 12.00 PM, post switching to DR site, Exchange will provide market to members to verify their orders/trades by Exchange.

- In case of any complaint/ claim by the Member arising from alleged data loss in the Exchange’s trading systems during the period of disaster at the Primary Data Centre, the Exchange, if it is satisfied upon verification of such complaint / claim about the need to do so, may take necessary corrective action(s).
- The Exchange shall provide its services on a best effort basis. However, the Exchange shall not be liable for failure of the system or for any loss, damage, or other costs arising in any way out of:
  - (a) Telecom network or system failures including failure of ancillary or associated support systems provided by the exchange or support agencies, or fluctuation of power, or other environmental conditions or destructions of any data.
  - (b) Accident, transportation, neglect, misuse, errors, frauds of the Trading Member / Participant or the agents or any third party.
  - (c) Act of God, natural calamity, fire, flood, war, act of violence or any other similar occurrence.

(d) Any incidental, special, or consequential damages.

ACTIVATION OF BUSINESS CONTINUITY PLAN

This section of the plan describes how the plan will be activated, and by whom. Activation will be dependent on the level of the incident, and the nature of the incident will decide which parts of the plan will be used.

The IGX BCP Management Team is responsible for deciding whether the BCP is to be invoked, wholly or partially.

It is expected that the plan will be fully invoked when it is apparent that access to the Trading operation building will be denied for more than three (3) hours during the trading hours.

Guidelines for Activation of BC Plan				
S#	Incident/ Circumstance	Alert raised by	BC Plan to be activated?	Activation/ authorized by
1.	Minor outages involving IT equipment failure	Engineer - IT	No	NA
Major Outages				
2.	Application Software Failure	Engineer - IT/MO	Yes	Authorised Members
3.	Network Link Failure	Engineer - IT	Yes	Authorised Members
4.	Cloud Infra Failure	Engineer - IT	Yes	Authorised Members
5.	Core Switch or Router Failure	Engineer - IT	Yes	Authorised Members
6.	Power Failure/ Electrical Mishap	Engineer - IT/ Executive - Admin	Yes	Authorised Members
Disastrous Events				
7.	Floods	Head - HR & Admin	Yes	Authorised Members
8.	Earthquake	Head - HR & Admin	Yes	Authorised Members
9.	Civil Unrest/ Riots	Head - HR & Admin	Yes	Authorised Members
10.	Terrorist Strike	Head - HR & Admin	Yes	Authorised Members
11.	Fire	Head - HR & Admin	Yes	Authorised Members
12.	Epidemics/Pandemics	Head - HR & Admin	Yes	Authorised Members

BCP PROCESS SEQUENCE

S#		Activity	Responsibility
001		**Disaster gravity**	
	001-a	If it is a life-threatening situation then implement 002, else 003	
002		**Evacuate area and notify the BCP Management Team**	Admin Floor Marshals
	002-a	In case of fire, begin to evacuate the building as per the procedures	
	002-b	In case of an earthquake, begin to evacuate the building as per the procedures	
	002-c	In case of a terrorist strike, begin to evacuate the premises as per the procedures	
	002-d	Notify the Incident Management Team and inform them of the emergency	
003		**Prepare to handle imminent emergencies**	
	003-a	In case of issuance of floods warning, follow the instructions as per the procedures	Admin
	003-b	In case of a pandemic outbreak, prepare for the emergencies as per the procedures	Admin
	003-c	In case of civil unrest / riots outbreak, prepare for the emergencies as per the procedures	Admin
004		**Handle medical emergencies**	Manager – HR & Admin
	004-a	Call the members of BCP Management Team and the required authorities	
005		**Shut down the equipment (Emergency Mode)**	Admin
	005-a	If an orderly shutdown is not feasible, switch off the main circuit breaker on the electrical panel, by breaking the protective glass covering	
	005-b	If an orderly shutdown is feasible, switch off the main circuit breaker.	
	005-c	Follow the activity as mentioned in 002-d	
006		**Equipment Protection**	IT
	006-a	Protect the critical equipment as per procedures defined for respective equipment	

S#		Activity	Responsibility
007		**Activation of the War Room**	AVP HR & Admin / Head - IT/CTO/CISO
	007-a	Notify the BCP Management Team about the incident and open a War Room	
	007-b	If unable to contact the Incident Management Team, assign activities to own team members	Authorised Members
	007-c	Advise the team of the potential disaster situation, as per Annexure - F, Guidance for War Room Members	
008		**Activation Of The Damage Assessment Team**	Damage Assessment Team
	008-a	Obtain approval from BCP Management Team and appropriate civic authorities for entering the site to assess the damage	
	008-b	Contact and assemble appropriate vendors as per Annexure - B Emergency Contact List	
	008-c	Conduct a detailed assessment of the site's condition, support services, equipment, and available supplies as per Annexure - H	
	008-d	Identify the equipment that has been damaged	
	008-e	Identify physical damage to site's environment	
	008-f	Identify usable equipment, documents, and supplies	
	008-g	Create a list of all property that must be replaced or repaired.	
	008-h	Confer with vendors and determine the minimum and maximum estimated period to recover the Exchange premises	
	008-i	Prepare Damage Assessment Form as per Annexure - I and forward the same to the BCP Management Team	
009		**Invoking DR Plan**	BCP Management Team
	009-a	The BCP Management Team shall decide to invoke the DRP after receiving the damage assessment reports / intimation for facilities and technology from the Damage Assessment Team / Incident Management Team	
	009-b	If DRP needs to be invoked, carry out the activities as per IGX DR Plan	
010		**Transporting Employees and Assets To Disaster Recovery Site**	Admin
	010-a	Inform concerned employees about starting operations recovery at the disaster recovery site as per Mobilization Procedure	
	010-b	Arrangements shall be made for transport and accommodation of the concerned team and the required documents, backup, etc.	
011		**Communication**	
	011-a	Notify all the members of the exchange as per Annexure - K Member Communication Procedure	Head - Market Operations
	010-b	Communicate to the News Media; as required, as per procedure defined in Annexure - J News Media Statements	MD & CEO

DETAILED PROCEDURE FOR MAJOR DISASTERS

1. FIRE

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Conduct an awareness session for all employees on Fire Protection and Fighting	Awareness on Fire Protection	Admin
Visibly display Do's and Don'ts within the Exchange Premises and the DR Site	Display fire do's and don'ts	Admin
Visibly display Emergency Contact List and Chain-of-Command, in case of any emergency (Annexure - B Emergency Contact List)	Display Emergency Contact List	Admin
Clearly demark the Emergency Escape Routes and Exit Doors	Mark Emergency Escape Routes	Admin
Document and publish Emergency Evacuation Procedure to all staff including individual's role and responsibility, in case of an emergency	Emergency Evacuation procedure	Admin
Appoint Floor Marshal at each floor and conduct trainings for them to combat an emergency situation	List of Floor Marshals	Admin
Publish and communicate the List of trained Floor Marshal to all concerned staff (As per Annexure - C)	List of Floor Marshals	Admin
Install smoke detection system and water sprinklers		Admin
Conduct periodic testing (yearly) of the smoke detection and water sprinkler systems	Testing of smoke detection	Admin
Timely renewal of the AMC and insurance for all equipment.		Respective department
Keep a fireproof safe with adequate capacity at the Primary Data Centre with one set of keys available with the Security Guard and another at an off-site location.		Admin
Conduct a periodic (Yearly) mock drill of emergency evacuation and submit the results to the BMT	Yearly Mock drill	Admin

Procedures	Action Plan	Responsibility
Keep First-Aid kit containing all necessary medicines and first aid material with the Security Guard and with the Admin at Primary and DR Site	First aid kit	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency Publish the contact details to all staff		Admin

B. PROCEDURE IN CASE OF FIRE EXPLOSION

i. On detection of fire

- Raise the alarm by breaking the glass of the nearest fire alarm call point.
- Inform **Fire Brigade on 101.**
- If trained, douse the fire with the appropriate extinguisher - but only if there is no risk to oneself.
- Leave the building by the nearest available exit route if unable to douse the fire or if instructed accordingly.

ii. Evacuating the affected site during fire

Instructions for Floor Marshals

- Take responsibility immediately as per the training provided.
- Wear the fluorescent jackets, for easy identification.
- Guide staff during evacuation and lead them through the designated Emergency Exit. Before leaving the area, ensure that all doors and windows are closed.
- Evacuate all staff using the "nearest" fire exit only. Before leaving, check that no staff are trapped or left behind.
- Assist physically challenged staff, and women to evacuate, and ensure they leave the affected area on priority.
- Instruct staff to remain calm, "Walk Briskly" and not "Run".
- If trained, douse the fire with the appropriate extinguisher - but only if there is no risk to oneself.
- Dial 101 – Give the Brigade distinct information concerning the fire:
  - Name and Telephone number
  - Exact location of the fire
  - Nature of fire
- Assist all occupants to evacuate the premises as soon as possible.
- Quickly co-ordinate with each department personnel for Roll Call.
- Inform Fire Brigade on arrival, in case anyone is missing.

Instructions for on-duty security personnel

- Security personnel shall check restrooms, copier rooms, closet, etc. to ensure that all employees, visitors, and contract staff have evacuated the site.
- Ensure that fire-proof cabinet/room storing critical documents and digital media having critical data is locked.

- Security personnel shall carry with him, the following, while leaving the affected site:
    - Visitors' register
    - Contract staff attendance register
    - First aid kit

Instructions for all employees, and contract staff

DO's in case of Fire

- Stay CALM.
- Stop all electronic appliances / gadgets.
- Leave the premises immediately – don't stop to collect any belongings.
- While leaving, close doors behind you, and pull the nearest fire alarm that you may pass.
- Alert others who may not be aware of the Fire.
- Avoid using lifts, use the staircase to leave.
- Follow the instructions given by the Floor Marshall.
- Assist disabled persons, women, and anyone who requires aid to vacate the premises.
- If trained in using the Fire Equipment, try extinguishing the Fire with the help of the Security Personnel.
- Walk towards the designated assembly point.
- If you are caught in an area filled with smoke, stay low, and crawl until you reach the exit. This helps in reducing smoke inhalation.
- Cool burns quickly with water and get medical attention immediately.
- If your clothes catch fire, stop and roll over covering your face and mouth, to put out the fire.
- Once outside, move away from the building to allow room for firefighters and their equipment.
- Look for your colleagues and intimate the Floor Marshall in case you find any one missing.
- If you cannot leave the premises because all exits are obstructed, crawl or stay low to the floor, where there is cleaner and cooler air. Get to a phone, and call, to let someone know where you are.

DON'Ts in case of Fire

- Don't ignore Fire Alarms.
- Don't run or panic when evacuating.

- Don't create confusion or spread rumors.
- Don't use elevators.
- Don't re-enter the premises, for any reason.
- Don't run if your clothes catch fire. Running will fan the fire and cause it to intensify.

iii. Assembly Points during fire

- ➢ Assembly point for employees is "Opposite the Main Entrance of the building"

iv. Activities at Assembly Points

Instructions to all employees, contract staff

- ➢ No employee shall leave the assembly point without permission from their immediate superior/concerned Floor Marshall.
- ➢ All employees shall stand with the department/team members in an orderly line.
- ➢ No employee or contract staff shall communicate with a non-employee, or media personnel.

Instructions to Department Heads and Administration

- ➢ Department Heads shall assist the Floor Marshals for obtaining a roll call of their respective teams, to ensure that no employee is trapped inside the affected site.
- ➢ Admin shall ensure that a roll call is obtained of all visitors and contract staff to ensure that no visitor or contract staff is trapped inside the affected site.
- ➢ The BCP Management Team and Fire Brigade shall be notified of any such person/s who may have been trapped inside the affected site.
- ➢ Department Heads and Admin shall take possession of all critical assets of IGX, such as files, documents, and so on, which employees may have collected on their way to the assembly point. These critical assets shall be maintained in safe custody with respective process owners till business operations resume.
- ➢ First-Aid shall be provided to all injured employees, visitors, and contract staff.
- ➢ Medical assistance shall be provided to the seriously injured and traumatized employees, or visitors and contract staff, at the earliest.

2. Floods

Procedures	Action Plan	Responsibility
A. Preventive Actions / Precautions to be Taken		
Keep track over the news warnings issued by the Meteorological department regarding flood	Visit Meteorological department site	Admin
Create an awareness amongst all employees about flood stages		Admin & HR
Emergency equipment like Generator, etc. shall not be placed at a location prone to water logging. For e.g. basement of the building. The same shall be placed at a safe location to ensure its availability in case of water logging or flood problems.	Generator installation	Admin
During the monsoon season, tentative bookings with nearby hotels/or in the building with necessary sleeping bags shall be made by the Admin department to ensure the availability of critical staff in case of water logging in the nearby business critical premises.	Hotel tie-ups / bookings	Admin
Adequate stock of food and other necessary amenities shall be ensured especially during the monsoon season for all the staff.	Food stock & other amenities	Admin
Ensure that adequate diesel is stocked by the Building administration to operate the DG Sets.	Stock of diesel	Admin
Emergency escalation and contact list indicating the chain of command and contact information in flood / water logging situation shall be defined and appropriately displayed at various locations.	Display of Emergency contact list and escalation list on all floors	Admin & HR

B. Procedure in case of Floods

Instructions to all Employees and Contract Staff during Floods

- In the case when water logging occurs near around IGX premises, the appropriate Admin personnel should be informed, as specified in the Emergency escalation & contact list.
- Wherever possible, water shall be pumped-out / removed with the help of water pumps. For e.g. in the case of waterlogging in the basement.
- If water logging affects the power supply of the Exchange, all critical business functions shall be protected by Uninterrupted Power Supply (UPS) and DG Sets to resume the activities of the Exchange.
- Disconnect all the electrical appliances in case water logging takes place inside the building. Don't touch electrical equipment while standing in water. Also, do not touch any electrical equipment which has been submerged in water.
- If required to walk through water, walk where the water is not flowing. A stick may be used to check the firmness of the ground.
- Floodwaters are to be avoided since it may be contaminated by oil, gasoline or raw sewage.
- Employees should return home only when authorities give a safety indication.
- Extreme caution is to be observed when returning to the flood damaged area. Floors may be slippery from water and mud. Check out for loose flooring, and dislodged nails. Stay clear of any electrical power cables.
- If operations have to be moved to the DR site, transportation logistics for relocation of operations should be considered.

3. EARTHQUAKE

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Ensure that the equipment at the Data Center is properly sited and racks are tightly affixed.	Check rack status	IT
Prepare and display Emergency contact list containing contact details of the personnel to be contacted, in case of power failure (As per Annexure - B)	Emergency Contact List	Admin
Keep an emergency kit consisting of: → First aid kit and essential medicines → Toolkit for emergency repairs	Emergency Kit	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency Publish the contact details to all staff	Contact List	Admin
Conduct periodic review of AMC, insurance copies of various emergency equipment's	AMC Renewal Insurance Renewal	IT/ Admin Finance & Accounts

B. PROCEDURE IN CASE OF EARTHQUAKE

Unlike other emergencies, the procedures to deal with an earthquake are much less specific. Since an earthquake magnitude cannot be pre-determined, emergency precautions shall be initiated within seconds after the initial tremor is felt, assuming the worst possible scenario.

The best earthquake instruction is to take precautions before the earthquake (e.g., secure or move objects placed above you, which could probably fall during an earthquake).

i. Emergency Action

- Remain calm and act, don't react.
- If indoors, seek refuge under a desk or table or in a doorway, and hold on. Stay away from windows, shelves, and heavy equipment.
- If outdoors, move quickly away from buildings, utility poles, overhead wires, parking garages, and other structures.
- Avoid downed power or utility lines as they may be energized. Do not attempt to enter buildings until you are advised to do so by the appropriate authorities.

ii. After the initial tremor

- Be prepared for aftershocks. Aftershocks are usually less intense than the main quake, but can cause further structural damage.
- Protect yourself at all times by not leaving the building during an earthquake due to falling masonry and glass.
- Take refuge under a desk or table or stand within a doorframe.
- Evaluate the situation and call the Admin team for assistance, if necessary.
- Do not use lanterns, torches, lighted cigarettes, or open flames, since gas leaks could be present.
- Open windows, etc., to ventilate the building. Watch out for broken glass.
- If the earthquake causes a fire, implement the fire procedures as documented in the earlier section.
- Determine whether anyone has been caught in the elevators or has been trapped by falling objects. If so, call the Admin Team for assistance.
- If the structural integrity of the premises appears to be deteriorating rapidly, evacuate the building.

iii. If trapped inside the building during the earthquake

- Stay calm!

- If a window is available, place an article of clothing (shirt, coat, etc.) outside the window as a marker for rescue crews.

iv. Evacuating the affected site during an earthquake

Instructions for Department Heads

- Department Heads shall ensure that all employees in the department evacuate the affected area.

Instructions for on-duty Security personnel

- Security personnel shall check restrooms, closet, etc. to ensure that all employees, visitors, and contract staff have evacuated the site.
- Security personnel shall carry with him, the following, while leaving the affected site:
  - Visitors’ register
  - Contract staff attendance register
  - First aid kit

Instructions for all employees, and contract staff

- Alert others in the vicinity.
- If possible collect the identified critical assets as per Annexure - A
- Allow physically disabled persons, visitors, and female employees to leave the affected area first.
- Determine whether anyone has been caught in the elevators or has been trapped by falling objects. If so, call the Admin Team for assistance.
- Counsel and guide traumatized employee to safety.
- Do NOT stop to collect bags and other personal belongings.
- Do NOT touch / switch any electrical points.
- Do NOT run but WALK to safety.
- Exit quickly and calmly.
- Lift / elevators should NOT be used.
- Be aware of hazards such as fallen live electrical wires or ruptured gas lines.
- Reach the assembly point.
- Do NOT return to the affected site without prior permission from immediate superior.

v. Assembly Points during an earthquake

- Assembly Point for Primary Site and DR site is “Opposite the Main Entrance of the building”

vi. Activities at Assembly Points

Instructions to all employees, and contract staff

- No employee shall leave the assembly point without permission from the immediate superior/concerned Floor Marshall.
- All employees shall stand with the department/ team members in an orderly line.
- No employee or contract staff shall communicate with a non-employee, or media personnel.

Instructions to Department Heads and Administration

- Department Heads shall assist the Floor Marshals for obtaining a roll call of their respective teams, to ensure no employee is trapped inside the affected site.
- Admin shall ensure that a roll call is obtained of all visitors and contract staff to ensure that no visitor or contract staff is trapped inside the affected site.
- The BCP Management Team shall be notified of any such person/s who may have been trapped inside the affected site.
- Department Heads and Admin shall take possession of all critical assets of IGX, such as files, documents, and so on, which employees may have collected on their way to the assembly point. These critical assets shall be maintained in safe custody with respective department heads till business operations resume.
- First-Aid shall be provided to all injured employees, visitors, and contract staff.
- Medical assistance shall be provided to the seriously injured and traumatized employees, visitors, and contract staff at the earliest.

4. CIVIL UNREST/RIOTS

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Keep track over the news published regarding any event that can cause civil unrest or riots	Physical security	Admin
Ensure that all the entries to the building premises are secured to restrict unauthorized entries: → depute Security Guards → Isolate office areas from the public areas such as reception through Access Control → Isolate sensitive areas such as Data Center, Trading Room from office areas through Biometric control	Physical security	Admin
Ensure that all important documents, records are kept in a secured cabinet, preferably in a fire-proof vault	Team level Continuity Plans	Respective Department Heads
Keep an emergency kit consisting of: → First aid kit and essential medicines → Water containers → Ready to eat food such as canned food, biscuits etc.	Emergency Kit	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency Publish the contact details to all staff	Contact List	Admin

B. PROCEDURE IN CASE OF CIVIL UNREST/ RIOTS

Political, religious or labor disturbances can lead to uncontrollable situations, resulting in civil unrest/ riots.

i. Receiving information about civil unrest/sensing attack in nearby area

- Information about demonstration/ a mob attack may be received through the News or through Telephonic information.
- The personal attending the call shall remain calm, listen carefully, and let the caller complete communicating the message/ news.
- The person attending the call shall note the message/news and obtain details such as the location of the unrest, nature of it, reasons for it and the severity of the same.
- The person shall immediately escalate the information to the Head – HR & Admin.
- The Head – HR & Admin shall ensure the genuineness of the information by verifying with the nearest police station.
- The Head – HR & Admin shall notify all the members of the BCP Management Team to take further action.
- To avoid causing undue concern to others, do not publicize till confirmation of imminent attack/ public demonstration/riots.

Instructions for Administration

- Immediately direct Security Guards to close all entry points to the building, if the demonstration is likely in the nearby area
- Inform nearest police station and ask for police presence in the premises
- Inform BMT
- Inform the employees, visitors and contract staff about the situation. Information should be brief so as not to cause alarm.
- Ensure that female staff is gathered in a safe location in the premises during the attack.
- Do not allow any employee, visitor or contract staff to leave the premises till situation is normal.

Instructions for Department Heads

- Counsel traumatized colleagues and ensure that operations are carried out as per instructions from BCP Management Team

Instructions for Employees and Contract Staff

- Stay calm
- Counsel traumatized colleagues

- Do not create panic and chaos from rumors spreading through telephonic calls, SMS and emails.
- Try to maintain “business-as-usual” environment
- Await instructions from BCP Management Team

5. TERRORIST STRIKE

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Ensure that all the entries to the Exchange premises are secured to restrict unauthorized entries: → depute Security Guards → Isolate office areas from the public areas such as reception through Access Control → Isolate sensitive areas such as Data Center, Trading Room from office areas through Biometric control	Physical Security	Admin
On-duty Security Guard to check the bags and luggage of all the visitors at the time of entering the building premises	Physical Security	Admin
Monitor the Exchange premises through CCTV camera to immediately detect and act upon suspicious movements of employees/ visitors; if any	Monitoring through CCTV	Admin
Ensure that First aid Kit is kept with the reception and with the Admin team with all the essential medicines.	First Aid Kit	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency Publish the contact details to all staff	First Aid Kit	Admin
Ensure that all important documents, records are kept in a secured cabinet, preferably in a fire-proof vault		Respective Department

B. PROCEDURE IN CASE OF TERRORIST STRIKE

i. On noticing any suspicious movement within the Exchange premises

- On-duty security personnel may notice suspicious movement of a visitor or staff through the surveillance camera or as reported by the staff.
- Suspicious movements may include, but not limited to, - attempt to access sensitive areas within the premise, attempt to bring-in weapons or similar gadgets, attempt to avoid security checks at the entrance and so on.
- Security personnel shall immediately notify the Head - HR & Admin about any such suspicious movements.
- The Head - HR & Admin shall ensure that the alert is immediately attended to senior personnel from the Admin Team.
- Prima facie, if the event is serious, then the Admin team shall notify the BCP Management Team, and the **National Anti-Terror Squad using the hotline number 1090**, as advised by the BCP Management Team.
- If required, all staff and visitors shall be moved into a safer zone or evacuated from the Exchange premises immediately.

ii. Responding to a prominent terrorist strike

- In case of a prominent strike by any terrorist of similar group, the On-duty security guard and Admin team shall try to evacuate the staff/ visitors through the Emergency Exit as soon as possible.
- The activity shall be immediately reported to **National Anti-Terror Squad using the hotline number 1090.**
- Affected personnel shall be given medical assistance by rushing them to the nearest hospital.

Instructions for Administration

- Immediately direct Security Personnel to close all entry points to the Exchange, if any suspicious movement is observed.
- Inform the nearest police station and ask for police presence in the premises.
- Inform the BCP Management Team.
- Inform all employees, visitors, and contract staff about the situation.
- Ensure that all personnel are evacuated immediately and moved to a safer zone.
- Contact the nearest hospital to assist the affected employees.

Instructions for Department Heads

- Provide counseling to traumatized colleagues if possible and ensure that operations are carried out as per instructions from the BCP Management Team.

Instructions for Employees and Contract Staff

- Stay calm.
- Evacuate the premises as soon as the alert is raised by the Admin team.
- Do not halt or wait to collect any paper or information.
- Counsel traumatized colleagues.
- Do not create panic and chaos by spreading information through telephonic calls, SMS, or emails.
- Do not communicate with the media directly if you are not an authorized spokesperson.
- Await instructions from the BCP Management Team.

6. POWER FAILURE/ ELECTRICAL MISHAP

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Alternate source of power supply shall be maintained to ensure continued power supply to all equipment	Installation of UPS and DG sets	Admin
Ensure that maintenance agreements are in place for all the supporting utilities	AMC for all supporting utilities	Admin
Conduct periodic testing of UPS and DG sets to ensure that they support, in case utility power is disrupted	Testing of UPS and DG sets	Admin
Ensure that necessary tie-up is made with the agencies to replenish fuel, in case of emergency Ensure that the contractor supplies fuel within a reasonable period of time during monsoon		Admin
Keep portable diesel pump in the custody of security guard for fuel pumping, especially during monsoon	Provision of portable diesel pump	Admin
Develop and maintain standard instructions to be followed by the concerned Admin staff, in case utility power is cut	Standard Instructions for Admin in case of power cut	Admin
Prepare and display Emergency contact list containing contact details of the personnel to be contacted, in case of power failure contact the Admin personnel (As per Annexure - B)	Emergency Contact List	Admin
Ensure that adequate training is imparted to the concerned Admin staff and security guards to execute instructions, in case of power failure	Training to Admin staff and Security Guards to operate DG sets	Admin
Ensure that smoke detection system and fire suppression systems are periodically tested to combat electrical mishap, if any	Testing of smoke detection system	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency Publish the contact details to all staff	Contact List	Admin

PROCEDURES	ACTION PLAN	RESPONSIBILITY
Ensure that all important documents, records are kept in a secured cabinet, preferably in a fire-proof vault		Respective Department

B. PROCEDURE IN CASE OF POWER FAILURE/ ELECTRICAL MISHAP

i. In case of extended power failure

- On-duty security personnel/ IT Engineer/ Admin personnel shall raise an alert regarding utility power failure and notify Admin Representative immediately.
- Admin personnel in consultation with the IT Team shall ensure that all IT load is switched to UPS power successfully.
- Admin Representative shall investigate whether the power failure is within the IGX premises or due to utility failure.
- In case of internal failure, the Admin Representative shall immediately inform BMT, Electrical Contractor personnel, and Utility officials as required.
- In case power failure is due to utility failure, the Admin Representative shall contact utility authorities to gather information on the reason for power failure and the expected time of restoration.
- If an extended outage is expected, the Admin personnel shall ensure a smooth transition to DG power, in consultation with the BMT.
- The Admin shall contact the concerned supplier to ensure that fuel is replenished to support trading operations.
- The operations may be switched to DR site, as discussed and authorized by the BMT in the War Room Meeting.

ii. In case of electrical mishap

- Due to any incident due to electrical mishap, there shall be an alarm raised either by personnel noticing the incident or by smoke detection system.
- In case there is fire due to electrical mishap, the same shall be handled as per the procedure documented in the earlier section.
- In case of any damage to equipment or extended power outage, the Admin personnel shall immediately notify the BMT.
- The operations shall be shifted to DR site, if extended outage is expected affecting trading hours.

Instructions for Administration

- Immediately assess the failure conditions and notify all concerned accordingly
- Inform the concerned officials of the Electrical Contractor for repairs and fuel replenishment, as required.
- Inform BMT.
- Inform the employees, visitors and contract staff about the situation.
- Ensure that all personnel are evacuated immediately, if there is fire in the premises.

- Contact the nearest hospital to assist the affected employees.

Instructions for Department Heads

- Await instructions from the BMT.
- Shift operations to DR Site as per the documented in the Procedure, if authorized by the BMT.

Instructions for Employees and Contract Staff

- Evacuate the premises as soon as the alert is raised by the Admin team.
- Do not halt or wait to collect any paper or information, if there is risk to human life.
- Do not talk to media directly, if you are not an authorized Spokesperson.
- Await instructions from BCP Management Team.

7. EPIDEMICS

PROCEDURES	ACTION PLAN	RESPONSIBILITY
A. PREVENTIVE ACTIONS / PRECAUTIONS TO BE TAKEN		
Ensure that good hygiene prevails in the Exchange premises and business areas are kept clean and sanitized.	Effective Housekeeping management	Admin
Ensure that only purified water is served to employees for drinking purpose.	Provision of purified water	Admin
Provide medical insurance to employees as per IGX Policy	Medical Insurance	HR
Admin to keep check on the news related to seasonal pandemic outbreak published by the Health Department and create awareness amongst employees through newsletters/ e-mails	Keep a check on pandemic outbreak	HR
In case of any epidemic / pandemic attack in the local region, Admin shall ensure adequate stock of emergency medicines and other quarantine measures (e.g. masks) for immediate use and distribution.	Emergency medicines and quarantine measures	Admin
Ensure necessary contacts with nearby hospitals to receive immediate support and relief, in case of an emergency. Publish the contact details to all staff.		HR/Admin
Ensure that standard operating procedures are developed and maintained for all operational activities.	Department-wise SOPs	Respective Department Heads
Ensure that all team members are trained to execute cross-functional responsibilities within the department.	Department-wise SOPs	Respective Department Heads

B. PROCEDURE IN CASE OF A PANDEMIC OUTBREAK

A pandemic can start when three conditions have been met:

- The emergence of a disease new to the population.
- The agent infects humans, causing serious illness.
- The agent spreads easily and sustainably among humans.

E.g. Influenza, COVID-19

i. <u>In case of Pandemic Outbreak</u>

- Admin shall keep a tag over the alerts published by the Health Department about any pandemic outbreak.
- Admin shall notify the BCP Management Team about the outbreak and the local regions affected by the same.
- If the outbreak directly affects IGX point of presence, Admin shall conduct an awareness session in consultation with the healthcare organizations.
- Admin shall inform all staff about the symptoms of the disease and the prevention mechanism to reduce likelihood of contracting a pandemic virus.
- If the prevention medicines/ vaccines are available, Admin shall provide all staff with the same.
- Admin shall also consider other non-pharmaceutical interventions in consultation with the medical advisors, as applicable.
- Department Heads shall maintain track of team members' health conditions and request them to stay at home, if symptoms are observed.
- Department Heads shall consult the BCP Management Team, as required.
- The Head – HR & Admin shall ensure provision of food supplies, and purified water for the staff who is executing continuity options.

Instructions for Administration

- Monitor news/ information published by national/ international healthcare organization on pandemic outbreak.
- Ensure good hygiene prevails within the Exchange premises.
- Create awareness amongst employees about the pandemic outbreak and precautions to be taken.
- Co-ordinate with the healthcare organizations and provide all staffs and their families with the prevention medicines/ vaccines.
- Provide medical insurance to employees as per IGX Policy.

- Provide purified water and food supplies to all staff who are executing continuity options.

Instructions for Department Heads

- Develop standard operating procedures for all operational activities and ensure that all team members are trained to perform cross-functional activities within the department.
- Await instructions from the BMT Instructions for Employees and Contract Staff.
- Do not attend work place, if symptoms of pandemics are observed.
- Immediately consult the nearest medical advisor/ physician to seek medical assistance.
- Inform the immediate supervisor about the health conditions.
- Attend work, only if health is recovered to normal and advised by the physician.

8. MOBILIZATION PROCEDURE

The Head – HR & Admin shall receive the lists of employees and assets that have to be transported to the DR site from the Disaster Recovery Team/HODs, if any and perform the following activities:

a. To mobilize staff and assets from the Exchange Premise bldg.to DR Site, the Admin team shall arrange alternative mode of transportation.

b. Arrangements for adequate seating and processing capacity shall be made at DR Site.

c. The Executive - HR shall arrange to contact the employees who need to be transported to DR site based on the contact numbers in the list.

d. Each employee shall be informed the following:

→ Requirement to operate from DR site
→ Reporting date and time
→ Expected duration of work at the DR site
→ Contact person and number at the DR site

e. The Head – HR & Admin shall arrange for required cash in hand at the DR Site in consultation with the BMT for emergency expenses, if any.

DISASTER RECOVERY PLAN (DRP)

IGX will prepare a detailed Disaster Recovery Plan for all the critical components required to continue from an alternate site.

Training & Awareness

1. Induction Training

1. The business continuity aspects shall be an inherent part of the induction program conducted for newly recruited employees.
2. The concerned Department Head shall ensure that the contract staff/ outsourced employees are inducted on business continuity aspects.
3. The induction training shall at a minimum contain:
   - → Business continuity requirements at IGX
   - → Details of DR Site
   - → Staff role and responsibilities during disaster
   - → Emergency Contact List
   - → List of trained Floor Marshalls
4. Records pertaining to the same shall be maintained by the HR Department.

2. Workshop For BCP/ DR Teams

1. BCP Workshops shall be conducted on yearly basis for team members who will be active part of DR execution.
2. The respective Department Heads in co-ordination with HR will organize the detailed workshop. The industry experts may be hired for conducting detailed workshops on BCP.
3. The workshop shall at a minimum contain the following topics:
   - ➢ Recovery priorities and strategies.
   - ➢ Team Specific roles and responsibilities.
   - ➢ Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases).
   - ➢ Incident-based procedures.
   - ➢ Other information such as Emergency Contact details, list of floor marshals, vital records etc.
   - ➢ Testing and maintenance of BC Plan.
   - ➢ Updates in the BC and DR Plan.
4. Effectiveness of the workshop shall be measured through case study or similar tests for the participant.
5. HR shall maintain the records of workshops conducted for the employees on BCP.

3. Awareness Program

1. HR will initiate awareness campaign on business continuity in co-ordination with other departments such as market operations, Admin, Finance, and IT.

2. A periodic newsletter/ e-mail shall be sent to employees reinforcing the awareness on business continuity planning.
3. HR will send newsletters specific to events such as mailers in cyclonic seasons or during pandemic outbreak.
4. HR will maintain records of newsletters and periodic updates sent to all employees and update the same to the BCP Management Team.

TESTING AND MAINTENANCE OF BC/DR PLAN

1. PLAN TESTING

BCP / DR plan needs to be tested for adequacy. It is an exercise that must be carried out periodically and BCP Management shall ensure that the business continuity arrangements and plans are current at all times by exercising each plan as per the following table.

SCHEDULE OF PLAN TESTING		
Area	**Activity**	**Frequency**
System and Networking	DR Plan - Network, application servers, database servers	Annually
	DR Plan-Systems and Networking (Part of Member/ Trading Mock)	Annually
HR & Admin	DR Plan - Fire & Emergency Evacuation, Power Outages	Annually
		Annually
Market Operations	Member / Trading mock drill (DR Drill)	Annually

1. In addition to the above-mentioned schedule, BCP /DR plan may be tested in the following scenarios as well
   i. Every time the plan is revised.
   ii. When a system is added to the processes.
   iii. When a system in the process is changed.
   iv. When any scheduling changes occur in the business activities.
   v. When a process falls in the scope of the plan, changes.
   vi. When a requirement arises for reporting on the adequacy of the plan.
   vii. When a report is required on the preparedness of the business continuity team.
2. The BCP Management Team shall announce BC / DR Plan Testing schedule to all concerned teams.
3. The concerned teams shall be responsible to conduct testing as per the schedule and the results of the same shall be submitted to the BMT as per Annexure - L.
4. The Market Operations department shall ensure that appropriate information is conveyed to the members through a circular to participate in the member mock drills. (Refer Annexure - M)

2. PLAN MAINTENANCE

1. The BC and DR Plans shall be updated due to occurrence of one of the following:
   - → Change in technology infrastructure
     - ○ Additions, deletions, or upgrades to hardware platforms.
     - ○ Additions, deletions, or upgrades to system software.
     - ○ Changes to applications software affected by the plan.
     - ○ Changes that affect the availability/usability of the hot site location.
   - → Change in business requirements.
   - → Change in regulatory requirements or regulatory instructions.
   - → Change in process and operational activities.
   - → Periodic review of the plan (yearly).
2. The concerned team effecting a change shall raise a Change Request to update BC and/ or DR Plan and submit the same to the members of BMT.
3. The Change Request shall also include the sections requiring amendments and the details of testing, as applicable.
4. The BMT shall review the Change Request and authorize the same based on the results of testing.
5. The BMT will notify the following:
   - → Concerned HOD – to implement the required changes.
   - → Head – IT/CTO – to update the required documents.
   - → Head – HR – to include in training and awareness program.
   - → Head – Market Operations – to communicate the same to all concerned.

3. RESPONSIBILITIES TO MANAGE THE CHANGES

The responsibilities to manage and updating changes at DR site is as mentioned below: -

Sr. No.	Changes	Responsibility	Activity	Time period
1.	Application Releases	Information Technology	All release, patches to be updated at DR site on next working day	Next working Day
2.	Database	Information Technology	Any changes done on parameter files/database structure are replicated through Archival/manually at DR site.	Same Day
3.	System related changes (including OS patches, etc.)	Information Technology	Any changes done on the system configuration files to be replicated	Next working Day
4.	Networking	Information Technology	Any changes done on the network configuration files to be replicated	Same Day
5.	Passwords	Respective Systems owner	Changes in password of any systems (Applications, OS, DB, FW) or equipment to kept in sealed envelope at DR site	Same Day
6.	Hardware	Information Technology	Any changes done on the hardware to be done after proper cost benefit analysis	As per BMT / IT-Head’s instruction
7.	Facilities	Admin	Any changes required at DR site to be done immediately	As per BMT / Admin-Head’s instruction

ANNEXURE TO BC PLAN

ANNEXURE - A CRITICAL ASSETS

Department	Type of Records	Storage Location
Market Operations	Outlook Checklist	Kept on File Server
	Format of Approval	Kept on File Server
	Members, Mutrade Admin, C&S, IGX Email database, Trading Email Database	Kept on File Server
	SFTP Folders (old reports)	Kept on File Server
Clearing & Settlement	Collateral securities files and relevant details	Fireproof vault
	Emails related to Trading and Clearing Members	Kept on File Server
	Fax Copies from Members	File Cabinet
	Agreements with various parties	File Cabinet
	User ID and Passwords of Banks - SFTP	File Cabinet
	Trade Files EOD shortage report Initial margin requirement	Kept on File Server
	SOD/EOD Checklists	File Cabinet
Delivery	Fax Copies from Members	File Cabinet
	Delivery Files, Checklist	Kept on File Server
	User ID and Passwords	File Cabinet
	pst file, Workstation data	Kept on File Server
BD & Membership	Documents sent by Members	File Cabinet
	Members' File, Interview Register Other registers such as Cheque/ FDR/ BG Other documents on Team Members' Workstations	File Cabinet
Human Resources	Candidate Database	Kept on File Server
	Database of recruitment agencies	Kept on File Server

Department	Type of Records	Storage Location
	Necessary Forms & Templates	Kept on File Server
	New joinees details	Kept on File Server
	Back-up of Induction Contents	Kept on File Server
	Attendance Sheets, feedback forms	Kept on File Server
	Questionnaires of the ISO Training,	Kept on File Server
	Other working files used within the department	Kept on File Server
Administration	Agreements with various parties	File Cabinet
	Database : CCTV Surveillance Gate pass	Kept on File Server
	Insurance Policies, Rate contracts	File Cabinet
IT Department	Checklists -network, security and application, Vendor Escalation Matrix	File Cabinet
	Asset Inventory	Kept on File Server
	Agreements with various parties	File Cabinet
	Inventory	Kept on File Server
	Hardening Guidelines	Kept on File Server
	BCP & DR documents	Kept on File Server
	All Production Databases	Kept on SAN storage
	Daily Checklist Formats	Kept on File Server
	Network Diagrams	Kept on File Server
	Device Configuration Files	Kept on File Server
	User ID and Passwords of all IT Equipment	File Cabinet
Finance and Secretarial	Tax related records such as Challans, TDS Certificates Vouchers Accounting & Taxation Documents	File Cabinet
	Bank User ID and Password	File Cabinet
	Files and Work Sheet in common folder	Kept on File Server
	Data on Excel	Kept on File Server
	Accounts Database	Kept on File Server

Department	Type of Records	Storage Location
Communications	Database of all domestic and international associations, media contacts, vendors and agencies	Kept on File Server

All the checklist or document used at Primary Site for day to day operation needs to be kept at Disaster Recovery Site also.it should be replaced as and when updated at Primary Site.

Note:

1. With respect to human resources detailed list is identified in “Disaster Recovery Plan” which states dedicated staff at DR Site and staff needs to be mobilized post disaster at DR site.
2. Employees who are not handling critical operations will be provided work from home solution to carry out their non-critical operations. Resources identified/required at DR site will be having required skill and knowledge to carry out operations from DR site. In case of new recruitment, employees will be trained adequately so that they can function on short notice at DR Site.

Annexure - B Emergency Contact List

S#	Name	Designation	Contact No
1.	Mr. Prasanna Rao	HOD - Market Operation	+91 9582049473
2.	Mr. Mritunjay Srivastava	AVP - Market Operation	+91 9999472556
3.	Mr. Sangh Suman Gautam	CTO	+91-9810539993
4.	Atul Mishra	AVP IT	+91 9910299208
5.	Vineet Harlalka	VP - Finance & Accounts	+91 9873089282
6.	Samir Prakash	Head - Admin & HR	+91-9999788435

EMERGENCY CONTACT LIST OF LOCAL AUTHORITIES		
Authorities		**Contact Details**
Fire Services	:	101
Police Station (Hotline)	:	100
National Anti-Terror Squad	:	1090
Emergency Ambulance	:	102 / 1298
Blood Banks	:	1910

EMERGENCY CONTACT LIST OF VENDORS			
Support Type	**Service Area**	**Service Provider**	**Contact Details**
Network	Cloud Infra	TCL IZO	https://customer.tatacommunications.com/
	Routers and Switches	Cisco/HP	https://support.hpe.com/hpesc/public/home/signin
	Firewall & VPN	Pulse Secure	support@pulsesecure.net
	ISP	Airtel	1800-10-2001/1800-10-22244
	ISP	TCL	1 800 2660 660
Application	Software Development	GMEX	
		UTRADE	
Hardware	Servers	Tech9Labs	+91 9667916999

ANNEXURE - C LIST OF TRAINED FLOOR MARSHALS

Sr. No.	Name	Contact
1	Ram Kumar Yadav	7289096696
2	Amit Sharma	9899028376
3	Anuj Jain	8373902309

ANNEXURE - E GUIDELINES FOR MANAGEMENT

Introduction

→ The BCP Management Team (BMT) comprises of Management representatives in likes of

- Managing Director
- Head – Market Operation
- Head – IT/CTO
- Head - Finance
- Head-Legal and compliance.
- Head-HR & Admin

→ The major responsibilities of the BCP management team (BMT) are

- Reviewing results of Business Impact Analysis
- Allocating resources for effective management and enhancement of BC initiative.
- Advise various teams on business continuity plan conflicts, incongruities, etc.
- Monitor progress on implementation of BCP/DRP
- Approval of overall BCP and changes therein

→ During Disaster or Emergency, BMT open a War Room to analyze the details and invoke a BC Plan. For details on Guidance for War Room Members refer Annexure - F .

→ If trading and clearing operations are hampered by the incident or disaster, it is vital that accurate and timely information is conveyed to the members of the Exchange.

→ All media statements must come from the **MD** or his appointed alternate spokesperson. For details refer section Annexure – J News Media Statements

Handling of Personnel

Allow personnel to deal with all personal issues and family matters that arise because of the disaster. Only once they have these matters are in hand, can they turn their mind to the problems at the work site.

In an extended disaster, it may be necessary to get personnel to work in shifts. Schedule and manage personnel efficiently. Be careful not to set up conflicting team assignments and time frames and watch for signs of excessive stress and fatigue. It is important personnel have adequate rest, as even exceptionally good performers reach a point where they no longer can think clearly and are prone to error.

Keep employees away from the news media by designating a single spokesperson and channeling information through this source.

Use non-technical personnel to communicate with customers and families of personnel. Keep families informed on the situation and on the well-being of their loved ones

Keep technical personnel free from interruption and having to answer unnecessary questions.

Keep personnel regularly informed on recovery efforts. All personnel in the company are working to a common aim and it is important for their morale they know the wider picture and do not feel isolated.

Remember some personnel members may not be able to work outside of their “normal” hours because of family commitments.

Identify “at risk” employees - those deeply affected by the trauma. Do not leave them alone but move them to a safe environment under the care of counselors, friends, or family, and assess the need for professional intervention.

Make all meetings mandatory. It is not uncommon for those who need help most to be the ones least likely to seek it.

Expect a period of uncharacteristic thoughts, feelings, and behavior amongst personnel. Violence, harassment, or inappropriate expressions of anger should never be tolerated.

In the aftermath of a crisis, managers should consider the effects of the disaster on personnel and be wary of taking severe forms of disciplinary action.

Consider providing onsite counseling and post-incident debriefings through trained specialists.

Be honest and open with employees. Talk about the incident and reinforce the company commitment to a safe work environment.

Annexure - F Guidance For War Room Members In A Major Disaster

→ The War Room members comprise of the Business Continuity Management Team (BMT).

→ Members can meet at a convenient place or virtually, depending on the situation.

→ During Disaster, this team advises various teams on the execution of the BC and the DR Plan.

→ They also ensure timely communication about the emergency to the Regulator, members, ISVs, and Media.

→ They oversee the overall execution of the BC Plan.

Factors that the War Room Members need to consider in the face of a major crisis:

1. The primary role is to provide corporate direction in resolving the incident, and to minimise the impact on employees, corporate reputation, the community, and the share value.
2. It is important to immediately confirm the actual situation. Getting accurate information is sometimes difficult under mounting pressure; however, analysing the facts to identify response actions has to be a key objective in the early stages.
3. Two streams of action are needed, one stream to manage the crisis response, and one stream to manage the daily business. Although a crisis can stop an organisation in its tracks, business resumption is essential, and is a part of the immediate recovery process.
4. Always take into consideration the corporate position. Confirm a consistent message strategy and ensure that the common spokesperson is providing a clear message across all stakeholder audiences.
5. Confirm how the crisis is affecting the company's audiences. Research can be very important here and employing research to monitor attitudes to the response can be invaluable on the road to recovery.
6. Take the initiative.
7. Be prepared to tell it as it is. Show the stakeholders what you are doing and why you are doing it. Emphasise and use language the community understands. Clarify information rather than promise results.
8. Take good legal advice but avoid being gagged on disclosure.
9. Keep a watchful eye on your competitors. They will use your crisis time as an opportunity.

10. Stay ahead of your financial audience before they are led by business analysts, academics, and financial journalists. Assist the financial analysts, the banks and your insurers in understanding the seriousness of your problem and do all they can to support your recovery.

11. Think ahead. Use lateral thinking to interpret both unintended consequences and how the business may finish up. Direct your recovery team to start building IGX and repairing reputation.

12. If the event is long and drawn out, be sure to get rest and keep stress at bay.

Annexure - G Insurance Claims

Procedure

If an insurance claim is probable, carry out the following procedures:

1. Visually check the damage and determine if an insurance claim is indeed likely. Pass your findings to the BCP Management Team
2. If submitting a claim:
   - Ensure the insurance company is informed of the situation and the known damage
   - Arrange to meet the insurance assessor at the site
3. Follow the points below wherever possible:
   - Make notes and take photographs of the damage.
   - Do not move any damaged property unless it is a safety risk or likely to incur further damage.
   - Do not allow personnel or service personnel to power on equipment or attempt repairs as this may worsen the problems and invalidate any insurance claims you wish to make.
   - Escort insurance assessor around the damage. Take notes of meeting and take further photos if deemed necessary.

Note: It is likely that the assessor may organize professional restoration companies to come onsite to inspect and deal with the problems. This is especially so if water, smoke or gases have affected computers and specialized electronic equipment.

Act as directed by the Insurance Assessor.

Points to Remember:

1. Take photographs of the damage before moving equipment or making repairs. This may be vital evidence that is needed, if disputes or challenged claims are made.
2. Keep full documentation, including costs where known, on actions taken to combat the disaster. Keep a diary of events and note the times that decisions were made, and actions were taken.
3. Insurance companies expect you to take all reasonable measures to safeguard the assets from further damage and to take no actions that will increase the cost of the claim.
4. If you have income protection insurance, your relocation and one-off costs may be covered by insurance. Liaise with your insurance company.

ANNEXURE - H DAMAGE ASSESSMENT TEAM (DAT)

1. Role

- Arrange for the physical protection of the assets.
- Appoint security guards to protect and secure site.
- Liaise with site specialists, such as engineers and insurance assessors.
- Document what losses have occurred.
- Arrange for salvageable material to be removed and properly stored or returned to its owners.
- Procurement of required IT Infrastructure.

2. Start a diary of events

- Note down times and actions. This will become important later for insurance claims and similar follow-ups.
- Establish contact with the emergency services.
- Identify your role. Seek permission to enter the area when it is pronounced safe.
- Perform a damage assessment of the site.
- Establish the extent of the damage to premises and equipment and update the information as required in the Annexure – I Damage Assessment Form.
- Take note of site security and where appropriate, organize immediate security for the site.

3. Report to BCP Management Team with the results of the initial assessment

→ Cover such topics as:

- The extent of the damage
- Estimated time before the area can be reoccupied
- Contractors needed: security, cleaners, electrical etc.
- Follow up on decisions made by the BCP Management Team

4. Escort personnel onsite to collect personal belongings

- Once the go ahead has been given to re-enter the building, allow personnel back to collect their personal belongings.

5. Obtain from the BCP Management Team decisions on:

- Whether the offices are to be re-occupied or relocation to the DR site.
- What insurance issues are involved?
- Whether contractors will be needed for the restoration of the site.

6. **Carry out an Insurance Assessment**

- Review and build up a quick list of the damage. Liaise with the Insurance Company as per Annexure - G.

7. **Salvage and removal of material**

- If an insurance claim is involved, then insurance company permission will be necessary before allowing contractors to come on site.
- Develop a list of contractors required, i.e., cleaners, carpenters, specialist companies, electricians etc. Insurance assessors will be able to assist in this area.
- If damage has occurred to documents and records, contact companies who specialize in the protection of records and documents. Salvaged records will need to be accounted for and stored in a secure area.
- If safe, arrange for personnel to come on site and remove personal belongings and salvageable records.
- Keep register of all damaged equipment removed. Check off against the asset register, if one is available.

Special Note:

Electronic Equipment damage

After a fire, electronic equipment such as monitors, photocopiers, document scanners, computers, printers and faxes, may appear undamaged, but may still have suffered smoke and contamination damage.

Specialist companies are the best groups to evaluate if equipment can be salvaged. All contact and liaison with them should be done in conjunction with the insurance company.

It is ***strongly recommended*** that equipment is not turned on until an evaluation has been completed by these specialist companies. If the equipment is contaminated, and it is turned on it can do irreparable damage to it.

Points to Consider

- If equipment or computer media is wet, immediately disconnect power supplies and backup batteries.
- Remove smoke from premises.
- Take extensive photographs as evidence, as they can be important should there be subsequent disputes.
- Separate burned and/or melted components, having limited salvage value, from the undamaged equipment.
- Record serial/model numbers.
- Ensure power is off, then wipe off surplus water, open up chassis doors etc., and where possible move undamaged equipment to a clean, dry room.
- Lower humidity in the room to below 40% RH and avoid introducing any other contaminants. Any commercial humidifier can do this. They normally can be easily hired.
- Remove wet carpets, curtains, ceiling tiles, etc. and remove all water from the floor or from under the false floor.
- If damage to the room is extensive, isolate the room and erect temporary barriers to shield the equipment from the outside elements.
- Seek advice on the computer equipment from a specialist equipment recovery company.
- After a fire, computer hardware companies will normally remove any hardware from maintenance till a restoration company checks it out.
- Never switch on equipment before specialist advice is received, as this is likely to increase contamination of the equipment.

Treat all equipment as damaged, and ensure the vendors are aware of the conditions to which the equipment has been exposed. Ensure service personnel do not power on equipment without authority, or before technical experts have been consulted.

Damage to Documents and Records

Preventative Measures:

- Good storage will go a long way to prevent damage to documents.
- Keep them in protective enclosures such as metal filing cabinets.
- Keep the storage enclosures shut, especially at night when the office is unoccupied.
- Have a record of your files and their location.

When Damage occurs:

If water damage:

- Prevent further damage by covering in plastic sheet.
- As early as possible wrap in plastic bags and remove as much air as possible.
- Do not separate or open up.
- Package files and books in reinforced boxes.
- Place in vertical position - book spines down.
- Identify by type and location.
- Relocate documents to a humidity-controlled environment - keep dry.
- Call a company specializing in document recovery from water damage.
- Seek advice from your local public health office if the water has been contaminated with health-threatening materials such as sewage.

Note:

If documents or computer files have escaped damage but are in a room where there is water around, remove them from the room as soon as possible. The dry material will absorb moisture from the air.

PROCUREMENT PROCESS IN CASE OF DISASTER

In case of any damaged product, if new procurement required to be initiated following procedure is followed:

1) Check damaged product from Inventory.
2) If the Product has been damaged and same needs to be procured.
3) Float the requirement to have quotation on immediate basis.
4) Submit quotation to BCP Management Team for approval.
5) Upon approval, send the Purchase Request to the Procurement Department.
6) If Purchase Request Management System (Omni flow) is unavailable, a hand written request to be sent to the Procurement Department. All such procurement requests will be physically signed by the BCP Management Team.
7) The Procurement Team will raise Purchase Order.
8) The Procurement Team will follow up with the selected supplier for delivery as per the agreed schedule.

ANNEXURE - I DAMAGE ASSESSMENT FORM

S#	Asset	Usable / Workable (Y/N)	If Not Usable Then Repairable (Y/N)	Acceptable downtime (Hours)	Expected Recovery Time (Hours)	Recovery Cost (RS)
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Annexure - J

News Media Statements

Managing the News Media

In a major incident, it is inevitable that the news media will become involved. If the event is obvious, such as building damage or a location-based event the news media will appear at that location, seeking answers. Be aware of this and make sure there is someone present at the location to aid the reporters.

All media statements must come from the **MD** or his appointed alternate spokesperson.

ANNEXURE - K COMMUNICATION TO MEMBERS

In a major incident affecting trading and clearing operations, it is vital that accurate and timely information is conveyed to the members of the Exchange. The following guidelines must be observed while communicating the details of the incident and the recovery mechanism to all members:

1. All statements must come from the **Head of Communication** or his appointed alternate spokesperson.
2. The information conveyed to all members must include
   - A brief description of the incident
   - Expected duration of the outage; if any
   - Recovery measures
   - Alternate work methods
   - Expected time of resumption
   - Emergency contact details
3. The information shall be conveyed through the appropriate channels such as web flash, member circulars, telephonic/ IVR message; as technically feasible.

ANNEXURE - L BC PLAN TESTING RESULTS

Type of Test : Table top/ Mock Drill	**Members Participation :** Yes / No
Business Area/Team:	
Test conducted from :	
Phases of Test :	

Test Objectives:
1.
2.
Scope/Boundaries: 1.
Scenarios:

Date, Time, and Location of Test:	**Scheduled duration of Test:**

Test Participants:

Sr. #	Teams	No. of Team Members	Responsibility
1.			
2.			

Action Tasks List with timelines:

S#	Activity	Responsibility	Proposed Date / Timeline	Actual Date / Time	Remarks / Status
1.					
2.					
3.					
4.					
5.					

Results:

S#	Observation Summary
1.	
2.	
3.	
4.	

MONITORING OF DEFINED RTO

S#	Application/ Component	Defined RTO	Actual RTO	Remarks (if any)
1.				
2.				
3.				
4.				
5.				

RPO is met by ensuring zero data loss.

Lessons / Findings / Areas of Improvement:

S#	Finding	Action	Responsibility and Date
1			

Status of Previous Test Findings

S#	Finding	Status	Date of Closure

Prepared By

Reviewed By

Enclosures:
SOD\EOD Checklist

ANNEXURE - M SPECIMEN OF CIRCULAR FORMAT FOR MEMBER MOCK DRILL

Circular No. <Number> **<Date>**

Mock Trading from Disaster Recovery (DR) Site on <day>, <date>

In terms of provisions of the Rules, Bye-Laws and Regulations of the Exchange, members of the Exchange are notified as under:

The Exchange is conducting a mock trading session on <day>, <date> from the DR Site to test the readiness.

Schedule for Mock Trading:

Particulars	Timings
Log-in time	
Mock trading timing	
Trade modification end time	

Live Re-login Activity:

Particulars	Timings
Live Re-login start time	
Live Re-login close time	

Members may note that the trades resulting from such mock trading will not attract any margin obligation, pay-in and pay-out and do not create any rights and liability on members. Members are requested to participate actively in the Mock Trading Session.

Procedure for downloading the files for participating in mock trading is specified in Annexure

For any clarifications, contact Customer Service on following numbers or send an email at < @IGXindia.com>

Regular Number (DC)	DD/MM/YYYY (DR; Mock day)	

For and on behalf of
XXX

Head - Market Operations

Encl: As above

Annexure-1

Steps for downloading files for participating in Mock Trading.

a) <Provide Steps>

GLOSSARY

Business	The day-to-day operational, administrative and support activities that enable and facilitate the attainment of an entity's Mission, Goals and Vision.

Business Continuity Plan (BCP)	A Plan by an organization to respond to unforeseen incidents, accidents, and disasters that could affect the normal operations of the organization's critical operations or functions.
Disaster Recovery Plan (DRP)	Plans by an organization to respond to unforeseen incidents, accidents and disasters that could affect the normal operation of a computerized system.
Entity	A governmental agency or jurisdiction, private or public company, partnership, not for profit organization, or other organization that has disaster/emergency management and continuity of operations responsibilities.
Critical Activity	The critical operational and/or business support activity without which the organization would quickly be unable to achieve its business objectives.
Critical Record	All administrative and operational records in any form (paper, microfilm, digital or electronic format), which are critical and essential to the resumption of business operations after a disruption.
Mitigation	Activities taken to eliminate or reduce the probability of the event, or reduce its severity or consequences, either prior to or following a disaster/emergency.
Preparedness	Activities, programs, and systems developed and implemented prior to a disaster/emergency that are used to support and enhance mitigation of, response to, and recovery from disasters/emergencies.
Recovery	Activities and programs designed to return conditions to a level that is acceptable to the entity.
Response	In disaster/emergency management applications, activities designed to address the immediate and short-term effects of the disaster/emergency.
Risk Assessment (RA)	An activity to help identify potential causes of interruption to an organization, the probability of occurrence and the potential impact of the threat.
Strategy	Broad term usually referring to the formation of a vision and direction, setting mission statements, identifying objectives so that the organization's objectives and goals can be achieved.

Vital Record	Records essential to protect the critical financial, legal, and operational functions of the organization and its customers, employees, shareholders, or other client group’s information without which the business could not operate. *Uniqueness* and *irreplaceability* must also be considered.

ABBREVIATIONS

Abbreviation	Definition/ Expansion
Admin	Administration
BCP	Business Continuity Plan
BMT	Business Continuity Management Team
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
DAT	Damage Assessment Team
DG	Diesel Generator
DR	Disaster Recovery
DRS	Disaster Recovery Site
DRP	Disaster Recovery Plan
DRT	Disaster Recovery Team
EOD	End of Day
IGX	Indian GAS Exchange Ltd.
HOD	Head of Department
HR	Human Resource
IMT	Incident Management Team
Kmph	kilometer per hour
MAO	Maximum Allowable Outage
MD	Managing Director
MPLS	Multiprotocol Label Switching
PDC	Primary Data Centre
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOD	Start of Day
SOP	Standard Operating Procedure
TnS (T&S)	Trading and Surveillance
UPS	Uninterrupted Power Supply

--- End of Document ---