DISASTER RECOVERY & BUSINESS CONTINUITY POLICY & PROCEDURE

CONTINENTAL CAPITAL MANAGEMENT (PRIVATE) LIMITED

DISASTER RECOVERY & BUSINESS CONTINUITY POLICY & PROCEDURES

POLICY STATEMENT

The overall objectives of the Disaster/Business Recovery Plan (DRP) are to protect Continental Capital Management (Pvt) Limited (CONCAP) resources and employees, to safeguard the organization's vital records, and to ensure the ability of the company to function effectively in the event of a severe disruption to normal operating procedures. The primary role of the DRP is to document CONCAP's plan for response, recovery, resumption, restoration, and returnafter severe disruption.

A disaster is defined as the occurrence of any event that causes a significant disruption in the company's capabilities to carry on its ongoing operations. The central theme of the Plan is to minimize the effects of disasters that it will have upon on-going operations.

Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective

ASSUMPTIONS OF THE DISASTER RECOVERY PLAN

1. Recovery for anything less than complete destruction will be achievable by using the plan.
2. Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.
3. Recovery of a critical subset (recovery workload) of the company's critical functions and applications systems during the recovery period will allow the company to continue critical operations adequately.
4. A disaster may require clients to function with limited automated support and some degradation of service, until full recovery is made.

DISASTER RECOVERY & BUSINESS CONTINUITY POLICY & PROCEDURES

PREVENTION

The best way to prepare for a disaster is to avoid the disaster. Therefore, we should look for any potential problems we can find and put them to order.

Some areas to look for include:

- **Maintain good general housekeeping:**
  Keep areas clean and free of obstructions and fire hazards. Eliminate any obviously overloaded electrical circuits. Employees shall be prohibited from installing any non-business electrical appliances such as coffee pots and fans. These appliances can cause electrical fires by shorting out themselves or overloading circuits not designed for these appliances.

- **Observe physical security procedures:**
  Access to office premises by outsiders and restricted access in some areas even for employees such as Server room, Dealing Room, etc.

- **Observe information security procedures:**
  Its concerns computers and data at our facility, and encourage increased security wherever appropriate. Here issues can include the following: activated screen-saver passwords and at least 6-character passwords used for accessing the network by each employee.

- **Backup Maintenance of all crucial data**
  We shall ensure that our company has arrangements to ensure we do obtain onsite and offsite backup of all crucial data. As such the following analysis has been performed to determine the company has adequate procedures in place to ensure backup of all crucial data is obtained on regular basis.

ONSITE AND OFFSITE BACKUP AND RECOVERY PROCEDURES

Review and documentation of current backup and recovery procedures, along with recommendations, where inadequate procedures have been adopted.

Daily backup of critical files of Settlement Department is obtained and stored at File/Data Server.

DISASTER RECOVERY & BUSINESS CONTINUITY POLICY & PROCEDURES

As per the Law's requirement we are supposed to maintain Voice recordings of all the trades that has been executed as such we have deployed a voice recording machine capable of maintaining recording of up to the time period specified by regulations. The backup of this is maintained.

SECURITY AND BACK UP OF CRITICAL SYSTEMS/APPLICATIONS/FUNCTIONS

Gathering security information is crucial in determining risks. For our critical functions, systems and/or applications, the physical security, backup security, and data security are reviewed and documented. Further, we have provided recommendations where we feel it's necessary to ensure the protection of these functions, systems and/or applications.

Critical System/Application/Function	Physical Security	Backup Systems	Data Security
Back office systems The system is used for settlement operations and for accounting purpose	Back office system is placed in psychically secured room.	Back up of back office server shall be maintained outside the premises on daily basis, whereby the company can obtain and store the Backup of the Back Office System at any needed time.	Access to data is password protected and is role based.
KATs Terminal These Terminals are important for order Execution of the trades.	Access to Dealing Room shall be restricted.	CONCAP has obtained remote DR terminal, which shall be used	KATs Terminals are password protected.

		if incase access to our main office is denied for any reason. This will ensure the continuity of our operations.	
CDC and NCSS Terminal These Terminals are used for Settlement's operation.	These Terminals are lying in Settlement Department, which is locked after office timings.	CONCAP has obtained access to global terminals of NCSS and CDS, which Shall be utilized in case of emergency and or disaster. These Terminals will ensure the continuity of our operations in case if we face any disaster (of any form) at our main office.	These Terminals are password Protected.

PLAN MAINTENANCE

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the

updated Plan; and training personnel. The Business Continuity Management Team Coordinators are responsible for this comprehensive maintenance task. Quarterly, the Disaster Recovery Planning Project Coordinator/Leader shall ensure that the Plan undergoes a more formal review to confirm the incorporation of all changes since the prior quarter. Annually, the Disaster Recovery Planning Project Coordinator/Leader shall initiate a complete review of the Plan, which could result in major revisions to this document. These revisions will be distributed to all authorized personnel, who exchange their old plans for the newly revised plans. At that time the coordinators will provide an annual status report on disaster recovery planning to the management.

MANAGEMENT REVIEW:

The Disaster Recovery Plan will be reviewed annually by senior management to ensure its continued relevance, effectiveness, and alignment with organizational objectives, regulatory requirements, and technological advancements. Updates will be incorporated based on test results, incident reports, and changes in business processes or infrastructure. Management approval will be documented, and revised versions will be distributed to all authorized personnel. Quarterly reviews will also be conducted by the Disaster Recovery Planning Project Coordinator to address interim changes.