ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

BUSINESS CONTINUITY PLAN & DISASTER RECOVERY POLICY

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

1 Overview

In the e-age the information security is a very integral function for any business, more so in the broking industry. The broking business carries a lot of compliance and regulatory risk. Information and information systems are susceptible to a plethora of threats and vulnerabilities. The success of information security lies in protecting the confidentiality, integrity and availability of information.

For the purposes of this Plan a disaster is defined as any event (e.g. fire, explosion, serious flood, spillage/escape of hazardous substances) which requires evacuation of building and the attendance of the Emergency Services. There shall be substantial disruption to normal business in its aftermath, requiring mobilization of significant internal and external resources.

2 Scope

A Disaster Recovery Plan comprises of four parts:

2.1 Emergency Plan: This plan specifies the actions to be taken immediately after the disaster occurs. The following are the components of the emergency plan:

2.1.1 The plan shall show who is to be notified immediately when the disaster Occurs- management, police, fire departments, hospitals and so on

2.1.2 Actions to be undertaken, such as shutdown of equipment, removal of files and termination of power

2.1.3 Evacuation procedures shall be specified

2.1.4 Return and restart procedures shall be designated. In all cases the personnel responsible must be specified clearly.

2.2 Back-up Plan: This plan specifies the following information-

2.2.1 The type of back-up to be kept

2.2.2 The periodicity of the back-up

2.2.3 The procedure to be followed

2.2.4 The location of resources

2.2.5 The site where these resources can be assembled and operations restarted

2.2.6 The personnel who are responsible for gathering back-up resources and restarting operations

2.2.7 The priorities to be assigned in recovering systems

2.2.8 The time frame in which recovery of each system must be affected

2.3 Recovery Plan: The objective of this plan is to restore an organization's information systems to its full capabilities. The key focus is to identify a recovery committee who will be responsible for working out the modalities.

2.4 Test Plan: The emergency plan, back-up plan and recovery plan must be regularly tested using test plan.

3 Steps Involved in BCP/DRP

3.1.1 Initiate a business continuity plan work group and develop a BCP Strategy

3.1.2 Perform a risk assessment exercise to identify threats and exposures to each of the core business processes

3.1.3 Identify recovery strategies and identify recovery teams for each core business process

3.1.4 Test and validate the BCP/DRP plans.

4 BCP/DRP Team

4.1 The BCP/DRP team would consist of the following personnel

1. Chief Information Security Officer
2. IT Head
3. IT Executive
4. Compliance Officer

5 Basic Requirements for BCP/DRP:

5.1 The first step is the risk assessment that assists in finding the most important processes that support the business. The business activities shall be classified under 3 broad categories A, B and C.

5.1.1 Category A: These include those business functions which cannot be performed unless they are replaced by identical capabilities. They cannot be replaced by manual methods. Tolerance to interruption is very low and therefore the cost of interruption is very high. Examples: Secondary Market Trading activities, Depository Participant functions

5.1.2 Category B: These are vital functions which can be done at the end of the day. There is a higher tolerance to interruption and therefore the costs involved are lower than the critical functions. Examples: E-Mail Activities, Contract Notes in the back-office

5.1.3 Category C: These functions are less crucial and can be managed for a brief period of time. Examples: Web-site, documents preparation.

5.2 Location for disaster recovery site: There are various factors involved in this decision like the distance from the main site, transportation and accommodation of the staff, seismic zone, political factors etc. Being not falling in criteria set for recovery site as defined by SEBI and Stock Exchanges (i.e. Minimum 50000 active clients required) , we have not opted for recovery site.

6 Recovery Strategies

6.1 Hot Sites:

6.1.1 In this particular site there would be complete replication of data as that of the main active site. In the event of disruption, this site shall be fully configured and be ready to operate in several hours. The equipment, network and systems are fully compatible with the primary site. The only additional needs are staff, programs, data files and documentation.

6.1.2 There are two options available for making a hot site:

6.1.2.1 Create an own redundant hot site with the entire IT set-up same as the existing one

6.1.2.2 Use a third party hot-site.

6.2 Warm-Sites: These are partially configured, usually with network connections and equipments like disk drives, tape drives and controllers but without the main computer. The assumption behind the warm site is that the computer can usually be obtained quickly for emergency installation and since the computer is the most expensive unit such an arrangement is less costly than a hot site.

6.3 Cold-Sites: They have only the basic environment to operate an information processing facility reducing the cost. Activation of the site may take several weeks.

7 Proposed Plan

The plan shall identify the teams with their assigned responsibilities in the event of a disaster/ incident. To implement the strategies that have been developed for business recovery and key decision making, IS and end- user personnel shall be identified. IT teams shall be made and they shall be assigned specific jobs. The teams may include:

7.1 Incident response team: This team shall receive information about every incident that can be considered as a threat to assets/processes

7.2 Emergency action team: They are the first responders, designated fire wardens whose function is to deal with fires and other emergency response scenarios

7.3 Damage Assessment team: They assess the extent of damage following the disaster. The team shall include staff expert in systems and networks and trained in safety regulations and procedures

7.4 Off-site storage team: responsible for obtaining, packaging and shipping media and records to the recovery facility.

7.5 Applications team: Travels to the recovery site and restores user packs and applications program on the back-up system

7.6 Security Team: Continually monitors the security of the system and communication links, resolves any security conflicts that impede the expeditious recovery of the system

7.7 Emergency operations team: Consists of shift operators and shift supervisors who will reside at the systems recovery site and manage systems operations during the entirety of the disaster

7.8 Network recovery team: Responsible for rerouting wide-area voice and data communications traffic, reestablishing host network control and access at the system recovery site

7.9 Communications team: Travels to the recovery site where they work in conjunction with the remote network recovery team to establish a user/system network

7.10 Data preparation and records team: Working from terminals that connect to the user recovery site and update the applications database

7.11 Administrative support team: Provides clerical support to the other teams and serves as a message centre for the user recovery site

7.12 Legal affairs team: Responsible for handling the legal issues arising for various reasons due to any incident

7.13 Recovery test team: Responsible for testing of various plans developed. We have formed the BCP/DRP team and have specified the functions for the team members. The following matrix explains the nature of functions assigned to the staff members and the support team of the vendors in the event of a disruption or disaster at the server station:

Designation	Function assigned
IT Head	Damage Assessment team
IT Manager	Recovery test team
Back-office Head	Applications Team
Compliance Officer	Legal Affairs team
Customer Relations Officer	Emergency Operations team
Compliance Executive	Incident Response Team
IT Head	Security Team
IT Manager	Network Recovery Team
IT- Executive	Offsite Storage Team
Customer Relations Officer	Administrative Support team

8 Testing BCP/DRP Plan

The BCP/DRP plan shall be tested during a time that will minimize disruptions to normal operations. It is important that Key Recovery Team members be involved in the test process.
The test shall accomplish the following tasks.

8.1.1 Verify the completeness and precision of the business continuity plan.
8.1.2 Evaluate the performance of the personnel involved in the exercise.
8.1.3 Appraise the training and awareness of non business continuity team members.
8.1.4 Evaluate the coordination among the business continuity team and external vendors and suppliers.
8.1.5 Measure the ability and capacity of the backup site to perform prescribed processing.
8.1.6 Evaluate the state and quantity of equipment and supplies relocated to the recovery site.
8.1.7 Measure the overall performance of operational and information systems processing activities related to maintaining the business entity.

9 Documentation of Results

During every phase of the test, detailed documentation of the observations, problems and resolutions shall be maintained.

10 Review and update

This policy shall be reviewed and updated on an annual basis or on any special event or circumstance.