

<b>Version</b>	<b>2024/01.02</b>
<b>Review Date</b>	<b>05/04/2024</b>
<b>Review &amp; Approved by</b>	<b>Reviewed by Technology Committee &amp; Approved by Board of Directors</b>

## 1 OVERVIEW

The Company is in the business of Securities Market Broking and uses Front end Trading System and Back Office system (hereafter referred as "network") to expand its network and facilitate clients.

Back up is an important aspect of computer data security. This policy defines the backup policy for computers owned and operated by company which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the database server, the application server, the mail server, and the web server.

## 2 Purpose

This policy is designed to protect data in the organization, and make the management be sure that it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

## 3 Scope

This policy applies to all equipment and data owned and operated by Company.

## 4 Definitions

- 4.1** Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- 4.2** Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- 4.3** Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

## 5 Timing

The data of the Critical Servers shall be backed up on a daily basis on all working days.

## 6 Policy

- 6.1** General Back up Policy:
  - 6.1.1** Daily Integrated back up of all data in database server, web server, application server & mail server, operating system and utility files including all patches, fixes and updates shall be taken on a daily basis.
  - 6.1.2** Media: The media on which the backup shall be taken may comprise of External Hard Disks, Tapes, or any other media being used by the company.
  - 6.1.3** The back-up media should be labeled with information related to data stored, server name and the type of data.
  - 6.1.4** Back up data shall be stored on site in a fire proof cabinet and a copy of the same shall be at maintained at an off site location.

## 6.2 Guideline for Backup:

The following registers should be maintained and signatures of the responsible persons should be taken with date and time stamp:

### Illustrative Draft

#### a) Inward/Outward Register for Backup Media

Date	Handover time	Particulars of Media and Data therein	Name of the person delivering the media	Sender's Signature	Name of the receiver	Receiver's Signature
------	---------------	---------------------------------------	---	--------------------	----------------------	----------------------

#### b) Back-up Register

Date and Time	Name of the person responsible	Nature of Data backed up	Signature
---------------	--------------------------------	--------------------------	-----------

## 7 Back-up Procedure

The IT administrator shall ensure that the following servers, applications and databases are backed-up compulsorily. (All critical servers as per list of Critical assets)

1. Trading – Front end Software Server
2. Back office Software
3. Database
4. Web Server
5. Mail Server

The back-up of the trading files is transferred to a separate back-up server on every Saturday i.e. on a weekly basis. The back-up on the database server and trading server are copied to a separate HDD on a monthly basis and the HDD are stored at Managing Directors' residence. The updates and releases are received through e-mail and are accessed by the authorized person. The older version of the application is backed-up.

## 8 Responsibility

The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

## 9 Testing

The integrity of the data is tested at the time of backing-up by enabling the integrity check function. The data stored on the backup server may be tested at the time of mock trading.

## 10 Archives

Archives are made at the end of every quarter in March, June, September and December. User account data associated with the file and mail servers are archived one month after they have left the organization.

## 11 Restoration

In order to restore the files user must submit a written request to the IT department which shall be authorized by head of the relevant department. Request should also state the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

## 12 Review and update

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