# Data Storage and Security Policy

## A. Applicability of the Policy

This policy shall be applicable on each and every person associated with the company in the business of merchant banking. Starting from the Board of Directors to the Key Managerial Personal and every staff working in the company

## B. The Policy

a) ***Company Data Storage and security Policy***

1. The every staff of the company should ensure that Information/data should be stored throughout its existence in an environment suited to its format and security classification, to ensure its preservation from physical harm or degradation and its security from loss or unauthorized access.

2. The company client Information and other data, whether original or duplicate, should never be kept outside corporate systems (e.g. on PC hard drives, on CDs or other removable media) except as a temporary off-line copy driven by a business need to work off-site or off-line, or for authorized transfer to other users or systems.

3. The company all business data and Information in all formats should be stored in two different physical locations to insulate any threat its physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. The physicals location shall be determined by the company management looking after its safety and easy retrieve.

4. Where electronic data is to be erased but the medium left intact, it must be deleted to the extent appropriate to the security classification, e.g. by over-writing files or reformatting disks.

5. Information will be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.

6. Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility through time. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats.

6. Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units, and by ensuring that files and computer monitors are not left open to general or casual view.

HOLANI CONSULTANTS PVT. LTD. JAIPUR

7. Protection from unauthorized access is password protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information.

8. Where information is stored on a mobile device (e.g. PDA, USB drive, laptop), special care is taken to ensure that the device is physically protected from theft, loss, or damages.

b) ***Company Data Backup Policy***

1. The Full backups of all company data should be performed weekly and if required according to circumstances then it should be taken on the daily basis depends on the activity taken place.

2. The activity of taking backups should be done preferably after office hours and should be completed before 8am on working days so that routine office should not be hampered.

3. The company Backups shall be stored in secure locations as determined by the Board. A limited number of authorized personnel who are appointed by the Board shall have access to the backup application and media copies.

4. The company backup shall be stored on two different backup devices, which shall be placed at the remote location on alternate days.

***This policy will be reviewed on an annual basis as per the need and requirements***