DATA BACKUP, STORAGE AND SECURITY POLICY

Data Backup, Storage and Security Policy

A. Applicability of the Policy

This Data Backup, Storage and Security Policy ("**Policy**") is adopted by Chiranjiv Capital Services Limited ("**Company**") and shall be applicable to every person associated with the Company in the business of merchant banking, including the Board of Directors to the Key Managerial Personnel, employees and every staff working in the Company.

The purpose of this Policy is:

- To ensure that the Company's securely stores all data and information and can retrieve it when needed;
- To protect Company's data by ensuring that it's handled and stored in a secure manner; and
- To define the procedures and responsibilities for backing up Company's data to ensure its availability in case of data loss.

B. The Policy

a) Company's Data/Information Storage and Security

1. All employees of the Company must ensure that information and data are stored securely and appropriately based on their format and security classification. This will help protect against physical damage, degradation, loss, unauthorized access, and hacking attempts throughout the data's lifecycle.
2. Client information and other Company data, whether original or duplicate, must not be stored outside of corporate systems (such as on PC hard drives, CDs, or removable media) unless it is a temporary offline copy needed for legitimate business purposes or for authorized transfers to other users or systems.
3. All Company business data and information, in any format, should be stored in two separate physical locations. This helps protect against potential threats to their physical integrity, such as wear and tear, fire, flooding, magnetic interference, and extreme environmental conditions. The specific locations will be determined by Company management to ensure safety and ease of retrieval.
4. Data no longer needed for routine operations and which need not be retained in an archive will be destroyed in a timely manner.
5. When electronic data is to be erased but the medium is left intact, it must be deleted to the extent appropriate to the security classification, e.g. by over-writing files or reformatting disks.
6. Information/data will be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.
7. 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

8. information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats.
9. 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.
10. 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 and the passwords should be changed periodically.
11. On-roll employees should refrain from making duplicate copies or shadow files of authoritative data resources.
12. Temporary duplicate copies of electronic data created for legitimate reasons must be protected in a like manner to the authoritative data, and removed in a timely manner.
13. 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 damage.
14. Unneeded non-authoritative data such as duplicate copies, outdated records, and- related files, that accumulate in operational locations need to be removed when no longer needed.
15. Installation of software on Company's computing devices operated within the Company's network by any employee is subject to approval by the IT department in writing or via e-mail.
16. Conducting periodic reviews and audits to identify and rectify potential vulnerabilities.

b) Data Backup

Backup and maintenance of data are critical to the viability and operations of the Company. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

The Backup aspect of this Policy applies to all data hardware, and software in the organization's information systems and is as follows:

Aspect	Details
Backup schedule	The Company shall maintain a regular backup schedule for all critical data. Full backups are to be performed weekly, with incremental backups occurring daily. All backups must be encrypted and stored in a secure, off-site location.
Roles and Responsibilities	The IT department is responsible for executing backups as scheduled. The department head will ensure that backup procedures are followed and reviewed regularly.
3-2-1 rule of Backup	At least three copies of the data: the original production data and two backups. At least two different types of media to store copies of your data (e.g. local disk, tape and external hard disk). At least one backup offsite (in the cloud or in a remote site).
Backup Procedures	The IT department must use software and hardware. Data to be backed up includes, but is not limited to, investor information, financial records, and operational data.
Data Retention	Retain the backup data for five years or as required by law or industry regulations.
Disaster Recovery	In the event of data loss, the IT department shall follow the disaster recovery plan to restore data from the most recent backup.
Review and Testing	Review the backup policy and procedures annually. Test the backup and restoration procedures quarterly to ensure they are effective.

CHINESE WALL POLICY

The Company has adopted a Chinese Wall Policy to Ensure strict segregation of sensitive information and to prevent any conflict of interest in the course of its Merchant Banking and related business activities.

Key Provisions:

1. Information Barriers: Distinct functional areas are created to separate advisory, capital raising, and research activities, ensuring that Unpublished Price Sensitive Information (UPSI) does not flow across divisions.
2. Access Control: Only authorized personal on a "need -to-know" basis are permitted to access sensitive information, with role-based restrictions and monitoring in place.
3. Physical & Electronic Safeguards: Separate workspaces, Restricted IT Permissions, and secure communication channels are maintained to upload confidentiality.
4. Compliance Oversight: The Compliance Officer monitors adherence to the Chinese Wall framework and records all instances where wall-crossing is permitted under regulatory approval.
5. Fair Market Conduct: The Policy ensures that decisions regarding advisory, underwriting, or investment services are taken independently and free from influence of other business functions.

   Through this mechanism, the Company ensures confidentiality, independence, and regulatory compliance, thereby protecting client interests and maintaining integrity of the capital markets.

For ***Chiranjiv Capital Services Limited***

For CHIRANJIV CAPITAL SERVICES LIMITED

Director

Sumit Bajaj
Director
DIN : 10815454

(This policy will be reviewed on an annual basis as per the needs and requirements)