VATSA CAPITAL VENTURE PRIVATE LIMITED

VATSA CAPITAL VENTURE PVT. LTD.

Policy on Data Backup, Storage and Security

(i) The document has been prepared in accordance with the Securities and Exchange Board of India (Merchant Bankers) Regulations, 1992, as amended from time to time as per the requirement.

(ii) The purpose of the Document is to provide essential information about the company in a manner to assist and enable the investors/clients in making an informed decision for engaging the company.

(iii) The document contains necessary information about the company required by an investors/client before availing services, and the investors/clients may also be advised to retain the document for future reference.

(iv) This Document is dated 27-02-2026

Details of the Company

Name of Merchant Banker	Vatsa Capital Venture Private Limited
Registered Office Address	4-C/6, 2nd Floor, New Rohtak Road, Karol Bagh, New Delhi-110005
Phone No(s)	01140456969
E-mail address	info@vatsacapitalventure.com
Website	https://vatsacapitalventure.com/

Details of the Compliance Officer

Name of Compliance Officer	CS Manish
E-mail Address	investors.grievances@vatsacapitalventure.com

VATSA CAPITAL VENTURE PVT. LTD.

Policy on Data Backup, Storage and Security

1. Objective

The purpose of this Policy is to establish a comprehensive and structured framework for data backup, storage, and information security to ensure the confidentiality, integrity, availability, and protection of data and information handled by the Company. This Policy is framed in compliance with applicable SEBI regulations, circulars, and guidelines, and is intended to safeguard client information, regulatory records, Unpublished Price Sensitive Information (UPSI), and critical business data from unauthorized access, loss, misuse, cyber threats, or system failures.

2. Scope and Applicability

This Policy applies to all data and information created, processed, stored, transmitted, or maintained by the Company in physical or electronic form. This includes, but is not limited to, client records, financial and accounting data, regulatory filings, transaction records, internal communications, employee information, and confidential business information. The Policy is applicable to all directors, officers, employees, consultants, and third-party service providers who have access to the Company's information systems or data.

3. Data Classification

For effective protection and handling, data shall be classified based on its sensitivity and criticality, including:

- Confidential and sensitive data such as client information, UPSI, financial records, and regulatory filings
- Internal operational data
- Publicly available information

Appropriate security controls shall be applied based on the classification of data to prevent unauthorized access or misuse.

4. Data Backup Policy

The Company shall ensure that all critical business, financial, operational, and client-related data is backed up at regular intervals through automated and secure backup systems. Backup frequency shall be determined based on the importance and criticality of the data and may include daily, weekly, or periodic backups. Backup data shall be stored in encrypted formats and maintained in secure locations, including off-site or cloud-based infrastructure, to protect against data loss arising from hardware failure, human error, cyber incidents, or natural disasters. Backup logs shall be maintained, and restoration procedures shall be periodically tested to ensure data recoverability.

VATSA CAPITAL VENTURE PVT. LTD.

5. Data Storage and Access Control

All sensitive and confidential information shall be stored only on secure servers, systems, or approved cloud environments authorized by the Company. Access to data shall be strictly controlled through role-based access mechanisms, ensuring that employees and users can access information strictly on a need-to-know basis. System access rights shall be reviewed periodically and immediately modified or revoked upon change in role, resignation, or termination of employment. Continuous monitoring mechanisms shall be implemented to detect unauthorized access, data breaches, or abnormal system activity.

6. Information Security Infrastructure

The Company shall deploy multi-layered security controls to protect its information systems, including but not limited to firewalls, intrusion detection and prevention systems, anti-virus and anti-malware solutions, endpoint protection, and network security tools. Sensitive data stored or transmitted electronically shall be protected through industry-standard encryption protocols. Remote access to systems shall be permitted only through secure channels with adequate authentication and authorization controls.

7. User Authentication and Password Controls

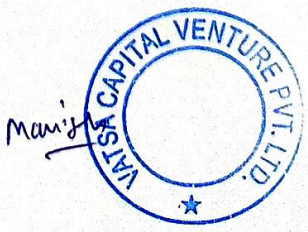
Access to systems and applications shall be protected through strong authentication mechanisms, including multi-factor authentication wherever feasible. Password policies shall mandate minimum complexity, periodic password changes, and restrictions on reuse of previous passwords. Sharing of user credentials shall be strictly prohibited.

8. Confidentiality and Protection of UPSI

All employees, directors, and management personnel shall be bound by strict confidentiality obligations to ensure that client data, internal information, and Unpublished Price Sensitive Information (UPSI) are not misused, leaked, or disclosed to unauthorized persons. Confidentiality obligations shall be incorporated into employment contracts, codes of conduct, and agreements with third parties. Any breach or suspected breach of confidentiality shall be reported immediately and addressed in accordance with internal procedures and applicable laws.

9. Business Continuity and Disaster Recovery

The Company shall maintain a Business Continuity Plan (BCP) and Disaster Recovery (DR) framework to ensure continuity of critical operations in the event of system failures, cyber-attacks, natural calamities, or other disruptive incidents. Disaster recovery mechanisms shall enable timely restoration of data and systems to minimize operational disruption. Periodic testing and drills shall be conducted to ensure the effectiveness of BCP and DR arrangements.



10. Third-Party Data Security

Where data storage, processing, or backup services are outsourced, the Company shall ensure that third-party vendors adhere to security and confidentiality standards equivalent to those followed by the Company.
Appropriate contractual safeguards, confidentiality clauses, data protection obligations, and audit rights shall be incorporated into agreements with such vendors to ensure regulatory compliance and data security.

11. Monitoring, Logging and Incident Management

The Company shall continuously monitor its IT systems and networks to identify security vulnerabilities, unauthorized access attempts, or data breaches. System logs shall be maintained for audit and investigation purposes.
Any cyber incident, data breach, or system compromise shall be promptly investigated, documented, and escalated to senior management. Where required, regulatory authorities shall be informed in accordance with SEBI guidelines and applicable laws.

12. Periodic Review and Audit

The data backup, storage, and security framework shall be reviewed periodically to address evolving cyber threats, technological changes, and regulatory updates.
Internal audits, vulnerability assessments, and security reviews shall be conducted at regular intervals to ensure continued effectiveness and compliance with SEBI regulations and industry best practices.

13. Training and Awareness

The Company shall conduct periodic training and awareness programs for employees and relevant stakeholders on data security, cyber risks, confidentiality obligations, and safe data handling practices to ensure effective implementation of this Policy.

14. Policy Review and Amendments

This Policy shall be reviewed periodically and updated as required to remain aligned with changes in SEBI regulations, cyber security standards, and operational requirements. Any amendments shall be approved by the competent authority of the Company.

Conclusion

Through this Policy on Data Backup, Storage and Security, the Company demonstrates its commitment to maintaining a secure, resilient, and compliant information management framework. These measures ensure protection of client interests, regulatory compliance, and uninterrupted business operations in line with SEBI's expectations and best industry practices.

M/s VATSA CAPITAL VENTURE PVT. LTD.