OUTSOURCING POLICY OF

SATTVA HOLDING AND TRADING PRIVATE LIMITED

OUTSOURCING POLICY

INTRODUCTION:

The purpose of this document is to define the outsourcing policy for the company Sattva Holding and Trading Private Limited (hereinafter referred to as "Sattva"/" Company") is a Private Limited Company incorporated under the Companies Act, 1956 and is registered with RBI as Middle Layer ("Middle Layer") engaged in activities of Core Investment Company

Being a Core Investment Company, Sattva can have exposures to entities falling within the definition of "companies in the same group" as per RBI, for the purpose of investment or lending.

PREAMBLE:

This Policy shall be termed as Outsourcing Policy of Sattva. The terms in this policy shall be considered as defined by the Reserve Bank of India in its various directions, guidelines as issued and may be issued from time to time and, or as defined herein below.

Outsourced services may include such activities that may need expert advise, opinion and attention which shall help conducting Sattva, its operations in a smooth, efficient and effective manner.

OUTSOURCING:

'Outsourcing' is defined as the company's use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the company itself, now or in the future.

'Continuing basis' includes agreements for supply of financial services which is provided, or agreed to be provided, continuously or on recurrent basis, under a contract, for a period exceeding three months with periodic payment obligations.

'IT Outsourcing' may be defined as the company's use of a service provider to perform activities as listed below on a continuing basis (including limited period agreements). Outsourcing of IT Services mainly covers the following areas but not limited to:

a) IT infrastructure management, maintenance and support (hardware/ software/ firmware);

b) Network and security solutions maintenance (hardware/ software/ firmware);

c) Application Development, Maintenance and Testing;

d) Services and operations related to Data Centers;

e) Cloud Computing Services;
f) Managed Security Services;
g) Application Service Providers (ASPs) including ATM Switch ASPs5 ; and
h) Management of IT infrastructure and technology services associated with payment system ecosystem.

The policy is designed with objective to:

i. Guide the entity in vendor selection, relation for outsourcing activities (including IT Outsourcing)
ii. Identify and manage the risks associated with outsourcing activities agreements including Strategic Risks, Reputation Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Contractual Risk, Access Risk, Concentration and Systematic Risk.

ACTIVITIES THAT SHOULD NOT BE OUTSORCED:

The Company shall not outsource core management functions including Risk Management, Strategic and Compliance functions and decision-making functions for management of investment portfolio. The activities which shall weaken or compromise Internal Control, Business Conduct or Reputation shall not be outsourced.

ROLES AND RESPONSIBILITY

Board of Directors

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing activities and the policies that apply to such arrangements;
- Deciding on business activities of a material nature to be outsourced and approving such arrangements;
- Setting up suitable administrative framework of senior management for the purpose of these directions;
- Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, safety and soundness;
- Shall take the responsibility for the actions of their service provider

Senior Management

The discretion for outsourcing activities will rest with Management of the Company, who will be responsible for the following:

- Evaluating the risks and materiality of all existing and prospective outsourcing, based on the policy and norms approved by the Board;
- Developing and implementing efficient and effective outsourcing policies and

procedures commensurate with the nature, scope and complexity of the outsourcing activities;

- Communicating information pertaining to material outsourcing risks to the Board in a timely manner;
- Ensuring that suitable business continuity plans based on realistic and probable disruptive scenarios, including exit of any third-party service provider, are in place and tested periodically;
- Ensuring effective oversight over third party for data confidentiality, appropriate redressal of customer grievances in a timely manner and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy and performance standards

IT Function (for IT Outsourcing)

- Assisting the Senior Management in identifying, measuring, mitigating and managing the level of IT outsourcing risk
- Maintain a central database of all IT outsourcing
- Effective mechanisms for monitor and supervise the outsourced activity and corresponding reporting to the Senior Management
- Develop and maintain vendor relationship documentation i.e. vendor appointment, due diligence, etc.

MATERIAL OUTSOURCING:

Material outsourcing arrangements are those which, if disrupted, have the potential to significantly impact the business operations, reputation or profitability. Materiality of outsourcing would be based on:

1. The level of importance to the Company of the activity being outsourced as well as the significance of the risk posed by the same;
2. The potential impact of the outsourcing on the Company on various parameters such as earnings, solvency, liquidity and risk profile;
3. The likely impact on the Company's reputation and brand value, and ability to achieve its business objectives, strategy and plans, should the service provider fail to perform the service;
4. The cost of the outsourcing as a proportion of total operating costs of the Company; and
5. The aggregate exposure to that particular service provider, in cases where the Company outsources various functions to the same service provider and the significance of activities outsourced

"Companies in the Group" means an arrangement involving two or more entities related to each other through any of the following relationships, viz. Subsidiary – parent (defined in terms of AS 21), Joint venture (defined in terms of AS 27), Associate (defined in terms of AS 23), Promoter-promotee [as provided in the SEBI (Acquisition of Shares and Takeover) Regulations, 1997] for listed companies, a related party (defined in terms

of AS 18) Common brand name, and investment inequity shares of 20% and above).

Note:

1. *The company shall not obtain any off-shore outsourcing services.*
2. *The company does not intend to utilize cloud computing services such as Information as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS), and hence has excluded the same from it from the policy document.*
3. *Further, List of activities specified in Annexure A shall never be considered as IT outsourcing.*

OTHER FORMALITIES TO BE CONDUCTED:

AGREEMENTS: The terms and conditions governing the contract between the Company and the service provider shall be carefully defined in written agreements and vetted by the Principal Officer and Company Secretary on their legal effect and enforceability.

Apart from being a legally binding agreement other clauses to be incorporated in the agreement are:

1. The contract shall clearly define what activities are going to be outsourced including appropriate service and performance standards along with Materially Adverse Events. It shall further include specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;
2. The Company must ensure it has the ability to access all books, records and information relevant to the outsourced activity available with the service provider and relevant clause to conduct audit (by Internal Auditor/External Auditor/Agents of the company) and to obtain a report for such an audit;
3. The contract shall provide for continuous monitoring and assessment by the Company of the service provider so that any necessary corrective measure can be taken immediately;
4. Adequate controls to be adopted by the Vendor for ensuring the customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information shall be incorporated. Types of data/ information that the service provider (vendor) is permitted to share with any party, if any.
5. A termination clause and minimum period to execute a termination provision along with clause requiring suitable back-to-back arrangements, if deemed necessary, shall be included;
6. Clause for prior Approval for use of a sub-vendor to provide the full or part of the services under agreement including clauses making the service provider contractually liable for the performance and risk management practices of its sub-vendor

7. Clauses to allow the Reserve Bank of India or persons authorised by it to access the company's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time;
8. A clause to recognise the right of the Reserve Bank therewith to cause an inspection of a service provider/sub-Vendor of the company and its books and account by one or more of its officers or employees or other persons; and
9. Maintenance of the customer data confidentiality even after the expiry of the tenure of the agreement
10. obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the company
11. Special Matters forming part of IT outsourcing Agreements:

- compliance with the provisions of Information Technology Act, 2000 and other essential legal requirements and standards
- storage of data only in India as per extant regulatory requirements
- provision to consider skilled resources of service provider who provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies
- Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised by the regulator

12. Such other provisions deemed necessary by the Board / Principal Officer / Company Secretary or such mandated by any law considering the kind of activities and size of the operations of the Company.

EVALUATION OF OUTSOURCING SERVICE PROVIDER

As a part of comprehensive outsourcing risk management programme, the Risk Management Committee shall assess the materiality of the outsourced activity and conduct due diligence of service provider including but not limited to the following factors:

1. Past experience and competence to implement and support the proposed activity over the contracted period
2. Financial soundness and ability to service commitments even under adverse conditions
3. Business reputation and culture, compliance, complaints and outstanding or potential litigation
4. Conflict of interest, if any.

5. Security and internal control, audit coverage, reporting and monitoring environment, business continuity management

6. ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities

7. Ensuring due diligence by service providers of its employees and sub-vendors

8. Compatibility of service providers systems with the company and acceptability of standards of performance in terms of customer service

9. Issues relating to undue concentration of outsourcing arrangements with a single service provider

10. Independent reviews and market feedback on service provider

11. external factors like political, economic, social and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance

12. Additional considerations for IT outsourcing:

a. evaluate details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements;
b. Information/ cyber security risk assessment;
c. ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and company's access to the data which is processed, managed or stored by the service provider

Due Diligence shall take into consideration qualitative and quantitative, financial, operational and reputational factors. Enhanced due diligence of the service provider as well as its management will be conducted, as deemed fit by the Risk Management Committee.

Risk Management Committee, shall decide whether the Company will benefit overall by outsourcing the function.

Additionally, following shall form pre-requisite conditions for the Company to enter into an outsourcing arrangement with a service provider:

- The service provider is materially in compliance with the applicable regulations, guidelines, conditions of approval, license and / or registration, etc.

- The service providers have established and maintain contingency plans, developing and establishing a robust framework for documenting, maintaining and testing business continuity and recovery procedures.

- The service provider periodically tests the Business Continuity and Recovery Plan and also permits to undertake occasional joint testing and recovery exercises with the Company.

- The company can retain an appropriate level of control over the outsourcing activities and the right to intervene with appropriate measures to continue its business operations without any additional expenditure and break in the operations or services.

- The company holds viable possibility of bringing the activity back in-house in an emergency and the costs, time and resources that would be involved.

- The service providers are able to isolate the company's information, documents, records and other assets.

- The company can, in all appropriate situations, remove all documents, records of transactions and information given to the service providers from their possession in order to continue its business operations, or deleted, destroyed or rendered unusable.

The result of the risk assessment of outsourcing arrangements entered into shall be presented to the Board of Directors for ratification in the form of a report in the ensuing Board Meeting.

MAINTENANCE OF RECORDS

The records relating to all activities outsourced shall be preserved centrally i.e. at the Corporate / Head office so that the same is readily accessible for review by the Board and / or Risk Management Committee as and when needed. IT Function shall ensure that such records are updated promptly and yearly reviews shall be placed before the Board. All original records shall be continued to be maintained in India (in case the activities are outsourced offshore).

REVIEWS BY INTERNAL OR EXTERNAL AUDITORS

The Audit Committee, in consultation of the Risk Management Committee shall mandate periodic audits by Internal or External Auditors of the service providers, outsourcing policies, risk management practices adopted in overseeing and managing the outsourcing arrangement and compliance with Risk Management Framework.

ACCOUNTABILITY

1. The company shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the services were provided in-house.

2. The Company will ensure that the outsourcing arrangements do not affect the rights of customer against the Company in any manner. The Company shall be liable to the customers for the loss incurred by them due to the failure of the third party and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the third party, as covered under the agreement with the customer.

3. The facilities / premises and data / information that are involved in carrying out the outsourced activity by the third party shall be deemed to be those of the Company and that the Company itself shall have the right to access the same at any point of time.

4. The Company shall make necessary disclosures in the product literature / brochures stating that it may use the services of third-party service providers.

MONITORING OF OUTSOURCED ACTIVITIES

1. The Risk management committee shall, on an ongoing basis, monitor the efficiency and accuracy of the outsourced activities, along with continuously considering and updating the outsourcing risks.

2. The company shall, at a period specified by the Risk Management Committee, but at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue meet its outsourcing obligations. Such review shall highlight any deterioration or breach in performance standards, confidentiality and security and in business continuity preparedness.

3. The company shall ensure reconciliation of transactions with the service provider are carried out in a timely manner and ageing analysis of entries pending reconciliation with service providers shall be placed before Board of Directors and company shall make efforts to reduce the old outstanding items at the earliest

4. The Company shall impart necessary training to the service providers to handle their

responsibilities with proper care and sensitivity viz. soliciting customers, hours of calling, privacy of customer information etc.

5. The Company shall also monitor, on a periodic basis, compliance of the Company's Fair Practices Code and Code of Conduct by the service providers.

6. The company shall conduct regular audits either individually or jointly with other entities of service providers (including sub-vendors) with regard to the activity outsourced by it. Such audits may be conducted either internal auditors or external auditors appointed to act on the company's behalf

7. The Company shall ensure that the service provider grants unrestricted and effective access to a) data related to the outsourced activities; b) the relevant business premises of the service provider; subject to appropriate security protocols, for the purpose of effective oversight use by the company, their auditors, regulators and other relevant Competent Authorities, as authorised under any law

CONFIDENTIALITY AND SECURITY:

The Company shall seek to ensure the preservation and protection of confidential data and documents.

GRIEVANCE REDRESSAL

Any grievances with respect to the outsourced activities of the Company shall be addressed to the Grievance Redressal Mechanism of the Company formulated under the Fair Practice Code and headed by the Grievance Redressal Officer. The contact details of the Grievance Redressal Officer of the Company shall be disclosed on the Company's website, all printed material issued by the service provider on behalf of the Company as well as every place of business of the Company and the Service provider.

REGULATORY APPLICABILITY ON SERVICE PROVIDERS

The Company shall intimate the service providers of the applicability of regulatory purview of the following nature on them by entering into an outsourcing arrangement (including recovery agent, Direct Sales Agent, KYC Collection Agencies and any other entity appointed for perform a part of the Lending/KYC process):

a. Compliance with Fair Practices Code (Code of Conduct) of the Company

b. Compliance with the Company's KYC & PML Policy

c. Information Technology Act 2000

d. The Service provider shall be subject to inspection and / or review of information / documentation by RBI, if so desired by the regulator.

e. The service provider shall not impede or interfere with the ability of the Company to effectively oversee and manage its activities nor shall it impede the Reserve Bank of India in carrying out its supervisory functions and objectives.

Suitable clauses in the agreements shall be inserted to specifically cover the above, in addition to the general principles prescribed under this policy.

BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN (FOR IT OUTSOURCING ACTIVITIES)

1. IT function of the company shall ensure that service providers shall develop and establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DRP requirements.

2. In establishing a viable contingency plan, shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

3. In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, the company shall retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

4. IT Function shall ensure that service providers are able to isolate the information, documents and records and other assets. This is to ensure that, in adverse conditions or termination of the contract, all documents, record of transactions and information with the service provider and assets of the company be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.

REPORTING OF TRANSACTIONS TO FIU-Ind

The company shall be responsible for making Currency Transactions Reports and Suspicious Transactions Reports to FIU or any other competent authority in respect of the company's customer related activities carried out by the service providers.

OUTSOURCING WITHIN A GROUP/CONGLOMERATE

The company may outsource a part of the its core management function to its group companies, subject to the following conditions being fulfilled:

1. The company may have back-office and service arrangements/ agreements with group entities e.g. sharing of premises, legal and other professional services, hardware and software applications, centralize back-office functions, outsourcing certain financial services to other group entities, etc.

2. Identical risk management practices as laid down in the policy shall be adhered when outsourcing activity to a related party

3. The company shall enter into service level agreements/arrangements with their group entities, which shall also cover demarcation of sharing resources i.e. premises, personnel, etc.

4. Following Caution points shall be required in case the activities is outsourced to a entity within the group:

    a. Outsourced Activity are appropriately documented in written agreements with details like scope of services, charges for the services and maintaining confidentiality of the customer's data
    b. Clear physical demarcation of the space where the activities of the NBFC and those of its other group entities are undertaken
    c. Do not compromise the ability to identify and manage risk of the NBFC on a standalone basis
    d. Do not prevent the Reserve Bank from being able to obtain information required for the supervision of the company or pertaining to the group as a whole
    e. Incorporate a clause under the written agreements that there is a clear obligation for any service provider to comply with directions given by the Reserve Bank in relation to the activities of the company.

5. Prior to outsourcing, Board shall evaluate that the company's ability to carry out their operations in a sound fashion would not be affected, if premises or other services (such as IT systems, support staff) provided by the group entities become unavailable.

EXIT STRATEGY (FOR IT OUTSOURCING)

A clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit shall be determined by the Senior Management. The strategy should include exit strategy for different scenarios of exit or termination of services with stipulation of minimum period to execute such plans, as necessary. In documenting an exit strategy shall, inter alia, identify alternative arrangements, which may include performing the activity by a different service provider or in-house.

Senior Management shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable (including service provider's obligation to cooperate fully with both the company and new service provider(s) to ensure there is a smooth transition).

WEBSITE:

The Board Approved-Outsourcing Policy will be hosted on the Company's website i.e. www.sattvaholding.com.

Outsourcing Vendors with whom new agreements have been executed as well as the agreements terminated to the extent the activities outsourced pertain to communication with the client shall be updated on the company's website to ensure customer protection.

UPDATE AND REVIEW:

The policy as well as its components (including agreements) shall be reviewed and updated by the board atleast annually.

Annexure A

Services / Activities not considered under "Outsourcing of IT Services" for the purpose of this policies:

1. Corporate Internet Banking services obtained by regulated entities as corporate customers/ sub members of another regulated entity
2. External audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review
3. SMS gateways (Bulk SMS service providers)
4. Procurement of IT hardware/ appliances
5. Acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a licence or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the RE.
6. Any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the RE.
7. Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.
8. Platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.
9. Any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the regulated entity wherein only a license is procured with no/ minimal customization
10. Business Correspondent (BC) services, payroll processing, statement printing