Date created	**11-09-2024**
Date Effective	**11-09-2024**
Document Author	**Vinod Singh**
Version	**1.0**

IT OUTSOURCING POLICY

INTRODUCTION

This IT Outsourcing Policy has been formulated in accordance with the Reserve Bank of India (RBI) Master Direction on Outsourcing of IT Services (DoS.CO.CSITEG/SEC.1/31.01.015/2023-24) ("Master Direction") and is applicable to Fintree Finance Private Limited (Company). The purpose of this Policy is to establish a comprehensive framework for the outsourcing of IT services, ensuring data security, risk management, and compliance with regulatory requirements.

The Reserve Bank of India (RBI) has consistently recognized the critical role of information technology (IT) in the financial sector and its impact on the overall stability and efficiency of the financial institutions system. In line with the evolving technological landscape and to ensure the robustness of IT systems and data security in the banking and finance industry, RBI has issued the Master Direction on Information Technology Outsourcing Policy. This policy framework aims to provide guidelines and directives for banks and financial institutions outsourcing their IT functions and services.

SCOPE OF THE POLICY

This policy would govern the broad principles and process adopted for appointment of service provider for outsourcing of technology operations in the Fintree Finance Private Limited. The policy incorporates the criteria for selection of the activities that may be outsourced, risks arising out of IT outsourcing and management of these risks, due diligence of outsourcing service providers, systems to monitor and review the operations of these activities.

OBJECTIVE

The primary objective of this Policy is to ensure the secure and efficient outsourcing of IT services while safeguarding the interests of the Company, its customers, and stakeholders. The Policy aims to establish guidelines for selecting service providers, managing risks associated with IT outsourcing, and maintaining the confidentiality, integrity, and availability of data.

APPLICABILITY

This Policy is applicable to all IT outsourcing arrangements entered into by the Company with third-party service providers, including vendors, partners, and contractors. It covers all functions and activities that involve the processing, storage, or management of Company data and IT systems.

OUTSOURCING ACTIVITIES

Outsourcing involves the use of a third-party service provider in any number of operational IT functions to perform ongoing activities (including agreements for a limited period). This policy is designed to manage the risks associated with IT outsourcing agreements.

Outsourcing of IT Services refers to the engagement of a third-party service provider by Company to perform specific IT-related activities on a continuing basis. The term 'continuing basis' encompasses both long-term contracts and those with a limited duration. While the scope of IT outsourcing is diverse, key areas covered include, but are not limited to:

1. **Infrastructure Services:** This category involves outsourcing components of an organization's IT infrastructure, including data centres, hardware provisioning, network management, cloud services, and disaster recovery solutions.
2. **Application Development and Maintenance:** Outsourcing the design, development, testing, and maintenance of software applications, ensuring alignment with business objectives and technological advancements.
3. **Help Desk and User Support:** Engaging service providers to deliver technical support, troubleshooting, and issue resolution for end-users, thereby enhancing user experience and minimizing disruptions.
4. **Cybersecurity and Compliance:** Outsourcing cybersecurity measures, including risk assessment, threat monitoring, incident response, and compliance management, to safeguard critical assets and ensure adherence to regulatory standards.
5. **Data Management and Analytics:** Externalizing data storage, management, and analytics processes to leverage advanced technologies, extract insights, and support data-driven decision-making.
6. **Business Process Outsourcing (BPO):** Integrating IT outsourcing with BPO for functions such as customer service, finance, and human resources, optimizing overall business operations.

MATERIALITY ASPECT IN OUTSOURCING

Outsourcing arrangements are material or significant, which if disrupted, have the potential to significantly impact the business operations, reputation, profitability or customer service. Materiality of outsourcing would be based by assessing the impact caused due to failure to perform the service as desired, on the Company's:

- earnings, solvency, liquidity, funding capital and risk profile;
- reputation and brand value, and ability to achieve its business objectives, strategy and plans; or
- ability in restoring services through another service provider or if done by the Company in-house.

Additionally, the cost of the outsourcing as a proportion of total operating costs of the Company, could be an indicator of materiality of the outsourced activity or all outsourced activities. The aggregate exposure to a particular service provider, in cases where the Company outsources various functions to the same service provider and the significance of activities outsourced in context of customer service and protection, would also make the outsourcing material.

ROLE AND RESPONSIBILITY

BOARD OVERSIGHT:

- The Board of Directors of the Company shall be responsible for

overseeing and approving all IT outsourcing arrangements based on risks and materiality.

- **Putting in place a framework for approval of IT outsourcing activities depending on risk and materiality.**
- **Setting up suitable administrative framework of Senior Management.**

SENIOR MANAGEMENT:

The Senior Management of the Company shall be responsible for preparing a framework of selection of outsourcing activities and partners, and regular monitoring of risks. Some of the components for the framework and risk assessment, may encompass the following activities:

- Preparing and implementing sound and prudent outsourcing policies and procedures, commensurate with the nature, scope, and complexity of the outsourcing, in accordance with the applicable laws and the guidelines prescribed by RBI.
- Preparing evaluation framework for risks associated with outsourcing of business-related activities, based on nature, scope and complexity, materiality of risks associated with the outsourcing activity.
- Ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested.
- Ensure effective governance of outsourced processes.
- Undertaking periodic review of outsourcing arrangements to identify new material outsourcing risks, as they arise.
- Ensuring independent review of the above.

Risk Assessment and Due Diligence: Prior to entering into any IT outsourcing arrangement, the Company shall conduct a comprehensive risk assessment and due diligence of the prospective service provider. This shall include an evaluation of the service provider's financial stability, track record, data security practices, and compliance with relevant laws and regulations.

Risk Management and Compliance: The Company shall implement a comprehensive risk management framework to identify, assess, and mitigate risks associated with IT outsourcing. Regular audits and assessments shall be conducted to ensure the service provider's compliance with the outsourcing agreement and regulatory requirements.

Contractual Framework: A well-structured contract should outline the rights, responsibilities, and expectations of both parties. Key aspects include service-level agreements (SLAs), data ownership, confidentiality clauses, dispute resolution mechanisms, and exit strategies.

RISK MANAGEMENT FOR OUTSOURCED POLICY

Need for an Outsourcing Policy: Outsourcing opportunities may be considered for better efficiency, lack of resources and requirement of specialized skills. The outsourcing decision must align with the overall strategic plan and corporate objectives of the Company. All outsourcing contracts/agreement must be in writing and must be vetted by the legal counsel of the organization for legal effect and enforceability.

Risks posed to the Company by Outsourcing all or part of its Activities and Evaluation of Risk: The key risks in outsourcing that need to be evaluated are: -

a) Reputation Risk – Poor service from the service provider, its customer interaction not being consistent with the overall standards of the Company.
b) Compliance Risk – Privacy, consumer and prudential laws not adequately complied with.
c) Operational Risk – Arising due to technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/or provide remedies.
d) Legal Risk – includes but is not limited to exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the service provider.
e) Country Risk – Due to political, social or legal climate creating added risk.
f) Contractual Risk – arising from whether or not the Company has the ability to enforce the contract.
g) Concentration and Systemic Risk – Due to lack of control of individual Company over a service provider, more so when overall banking industry has considerable exposure to one service provider.

Evaluating Capability of Service Provider: In considering or renewing an outsourcing arrangement, appropriate due diligence should be performed to assess the capability of the service provider to comply with the obligations in the outsourcing agreement. Due diligence should take into consideration qualitative and quantitative, financial, operational and reputational factors. Due Diligence may involve evaluation of all available information about the service provider, including but not limited to:

a) Past experience and demonstrated competence to implement and support the proposed IT activity over the contract period;
b) financial soundness and ability to service commitments even under adverse conditions;
c) business reputation and culture, compliance, complaints and outstanding or potential litigations;
d) conflict of interest, if any;
e) 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;
f) details of the technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan;
g) capability to identify and segregate Company's data;
h) quality of due diligence exercised by the service provider with respect to its employees and sub-contractors;
i) capability to comply with the regulatory and legal requirements of the Outsourcing of IT Services arrangement;
j) information/cyber security risk assessment;
k) ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and RE's access to the data which is processed, managed or stored by the service provider;
l) ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and
m) ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection and confidentiality.

The Outsourcing Agreement: The terms and conditions governing the contract between the Company and the service provider should be carefully defined in written agreements and vetted by legal counsel on their legal effect and enforceability. Every such agreement should address the risks and risk mitigation strategies. The agreement should be sufficiently flexible to allow the Company to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures

to meet legal and regulatory obligations. The agreement should also bring out the nature of legal relationship between the parties.

Hosting Services: The Company shall develop a process to avail Infrastructure Services from a Third Party for expanding/ augmenting its infrastructure. In such cases the following will have to be considered:

- In case of hardware is provided by the vendor then it will have to be hosted in a caged and separate enclosure. In case the infrastructure is shared, and virtualised, logical separation will have to be established.
- The infrastructure that is contracted will have to be clearly identified.
- "The location of the Infrastructure for Onefin -AWS CLOUD which is based in India & for Sperdian – Control S in Bangalore . We have deployed Firewall at our Premises & the Data center is Level 4 data center" .
- All system admin activities will be done under supervision of Company Staff. Access Management will be controlled by Company. All conditions related to Third Party Outsourcing shall be followed.

Cloud Application Services: Company may avail Application Services where the Application is not owned or licensed to Company. The services are offered on a subscription basis and are hosted on Cloud in a Third-Party Data Centre. In case such services are availed, the following may be considered:

- Data segregation should be implemented.
- Access to applications should be controlled by Company Backup and restore options should be available.
- Provider should not use the data for any other purposes like analytics without the permission of Company.
- Ensure implementation of security controls in the cloud-based application
- Ensure appropriate deployment of network security resources and their configurations.
- Ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards.
- The Cloud architecture should enable smooth recovery and any failure should not result in data/information security compromise.
- Providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access.
- Access provisioning should be governed by principles of 'need to know' and 'least privileges' and require the RE's approval and monitoring.
- Multi-factor authentication should be implemented for access to cloud applications.

SERVICE LEVEL AGREEMENT / OUTSOURCING AGREEMENT (SLA)

All Service Providers, prior to selection, must be given clarity on the level of service that the Company expects from them. The terms of the Service Level Agreement ("SLA") shall be decided by the Company and mutually agreed upon by the Service Provider. For Service Providers providing same or similar services, the terms of the SLA shall be identical to ensure equity and parity amongst the Service Providers.

Every SLA shall include the following provisions:

- Nature of Legal relationship between the parties i.e., whether agent, principal or otherwise.
- What activities are going to be outsourced? (Including appropriate service and its performance standards including for sub-contractors,if any).

- Determine the ability to access all books, records and information relevant to the outsourced activity available with the Service Provider.
- Ability for continuous monitoring and assessment of the Service Provider by the Company so that any necessary corrective measure can be taken immediately.
- Controls to ensure customer data confidentiality and the Service Providers' liability in case of breach of security and leakage of confidential customer related information.
- Have a contingency plan to ensure business continuity.
- Termination clause and minimum period to execute a termination provision (Notice Period).
- Limited access of data to the employees of the Service Provider only on a "need to know" basis and availability of adequate checks and balances at the end of the Service Provider to ensure the same.
- Requirement of prior approval/ consent from the Company for use of sub-contractors by the Service Provider for all or part of an outsourced activity and includes, where necessary, conditions of sub-contracting by the Service Provider in order to maintain a similar control over the risks by the Company.
- Must have a confidentiality clause to ensure protection and confidentiality of customer data even after the SLA expires or gets terminated.
- Provides for the Company with the right to conduct audits on the Service Provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the Service Provider in conjunction with the services performed for the Company.
- Provides for the RBI or persons authorized 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.
- Provides for right of the RBI to cause an inspection to be made of a Service Provider of the Company and its books and account by one or more of its officers or employees or other persons.
- Requirement of the Service Provider to preserve documents as required by law and take suitable steps to ensure that the Company's interests are protected in this regard even post termination of the services.

BUSINESS CONTINUITY AND MANAGEMENT OF DISASTER RECOVERY PLAN

Company should have developed and set up a robust documented and tested framework for business continuity and recovery procedures which shall be reviewed time to time. For instance:

1. Company should ensure alternative Service Providers are available or there is a possibility of bringing the outsourced activity back in-house in case of emergency.
2. To mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, REs 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.

Company 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 can be removed from the possession of the service provider, or deleted, destroyed or rendered unusable.

CLOUD COMPUTING AND SECURITY OPERATIONS CENTER ("SOC")

Company shall follow directions and comprehensive compliance requirements to avail cloud computing services offered by third parties and outsource SOC services. These measures *inter alia* include:

- Taking into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/processing of data, etc., and attendant risks, while establishing appropriate risk management framework.
- Adopting and demonstrating a well-established and well-documented cloud adoption policy.
- Selecting the cloud service providers ("CSP") based on a comprehensive risk assessment of the CSP.
- Ensuring sound service and technology architecture that supports cloud-based applications which are built in adherence to globally recognised architecture principles and standards.
- Ensuring that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/by an on-premises application.
- Accurately defining minimum monitoring requirements in the cloud environment.
- To have a business continuity framework that shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the Company can continue its critical operations with minimal disruption of services while ensuring integrity and security; and
- Ensuring that the Company has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics.

NO CONFLICT OF INTEREST

The Company is required to ensure that its IT service providers are not owned or controlled by any Director, or Key Managerial Personnel, or Approver of the outsourcing arrangement of the Company, or their relatives. However, an exception to this requirement may be made with the approval of the Board/Board level Committees, followed by appropriate disclosure, oversight and monitoring of such arrangements. The Board of Directors of the Company must ensure that there is no conflict of interest arising out of third-party engagements.

EXIT STRATEGY

A well-defined exit strategy must be established while entering into agreement to ensure a smooth transition in case of termination or expiry of the outsourcing arrangement. The Company shall have access to all critical data and systems during and after the transition process. The Company may consider following points while developing an exit strategy:

- Secure purge of RE's information from the CSP's environment.
- Smooth transition of services.
- Unambiguous definition of liabilities, damages, penalties and indemnities.
- Agreed processes and turnaround times for returning the RE's service collaterals and data held by the CSP.
- Contractually agreed exit/termination plans should specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the RE's business, while maintaining integrity and security.
- Ensure that after the termination of the contract, the Company can take back all the documents, records of transactions and information given to the Service Provider to continue its business operations, or otherwise delete, destroy or render unusable the same.

MONITOR / CONTROL OUTSOURCING ACTIVITY

The Company should establish a robust monitoring and oversight mechanism to ensure service providers adhere to agreed-upon terms. This involves periodic reviews of performance, security audits, and assessments of compliance with regulatory requirements. The Company shall have in place a management structure to monitor and control its outsourcing activities. It shall ensure that outsourcing

agreements with the service provider contain provisions to address their monitoring and control of outsourced activities.

REDRESSAL OF GRIEVANCE

The Company has adopted the following grievance redressal mechanism for speedy redressal of grievances of its customers in time bound manner:

1. **Level 1 Escalation:** Customers may register their complaints/ grievances with the "Grievance Redressal Cell"through any of the following modes which shall be attended within 10 days:

Email	wecare@fintreefinance.com
Online	Contact Us – Fintree (fintreefinance.com)
Write to us	Grievance Redressal Cell, Fintree Finance Pvt. Ltd. Engineering Centre 4th Floor, 9 Matthew Road, Opera House, Mumbai – 400004
Call Us	1800 267 8111 (Toll-free Number, 11.00 AM to 05.00 PM, Monday to Friday)

2. **Level 2 Escalation**: If customers are not satisfied with the resolution provided by the Grievance Redressal Cell or they do not receive any response from the Grievance Redressal Cell within 15 days as mentioned above, the customers may further escalate their complaints/ grievances to the Nodal Officer who shall attend the same within 7 days:

   Ms. Sweta Parekh
   Fintree Finance Pvt. Ltd.
   Engineering Centre 4th Floor,
   9 Matthew Road, Opera House,
   Mumbai – 400004
   Phone Number-18002678111
   Email- sweta.parekh@fintreefinance.com

3. **Level 3 Escalation:** If customers are not satisfied with the resolution provided by the Nodal Officer or they do not receive any response from the Nodal Officer within the aforesaid 7 days, they may escalatetheir complaints/ grievances by writing to the **Appellate Authority-Grievance Redressal** at below mentioned address who shall attend the same within 10 days:

   The Appellate Authority-Grievance Redressal
   Fintree Finance Pvt. Ltd.
   Engineering Centre 4th Floor,
   9 Matthew Road, Opera House,
   Mumbai – 400004

   The **Appellate Authority-Grievance Redressal** is constituted of the following:

   1. Head of Departments/Chief Business Officers of respective Lines of Business (LoBs)
   2. Chief Financial Officer
   3. Head – Compliance and/or Legal

4. CEO.

The responsibilities of the Appellate Authority-Grievance Redressal are as under:

1. Ensure adherence to the grievance redressal policy and procedure laid down in this Policy, monitor its implementation and initiate corrective action wherever needed.
2. Decide upon matters requiring immediate attention and follow up for timely redressal of grievances wherever delay is observed.
3. Take appropriate action to avoid any such delays in the future.

4. If the complaint/ grievance of the customer is not redressed within a period of 4 weeks, the customer may appeal to Regional Office of DNBS of RBI, under whose jurisdiction the registered office of the Company falls:

The Officer In-Charge
Consumer Education and Protection Cell,
Reserve Bank of India
Main Building
Mumbai Regional Office,
Fort Mumbai - 400 001

The Nodal Officer shall ensure that this structured grievance redressal mechanism is displayed prominently, for the benefit of the customers, at all branches / places of the Company where business is transacted as well as on the website of the Company.

REVIEW OF THE POLICY

This Policy shall be reviewed periodically to ensure its effectiveness and alignment with regulatory changes. Any updates or amendments to this Policy shall be approved by the Board of Directors. The policy shall be reviewed at yearly intervals or as and when considered necessary by the Management of the Company.

CONFIDENTIALITY AND SECURITY

Public confidence and customer trust in the Company are a pre-requisite for the stability and reputation, and therefore, the respective Head of the Departments shall ensure that:

1. Outsourcing Arrangement shall ensure preservation and protection of the security and confidentiality of customer information in the custody or possession of the Service Provider.
2. Access of customer information to the staff of the Service Provider shall be on a 'need to know' basis i.e., limited to those areas where information is required in order to perform the outsourced function.
3. The Service Provider shall isolate and clearly identify the Company's customer information, documents, records and assets to protect the confidentiality of the information. In Instances, where the Service Provider acts as an outsourcing agent for multiple companies, care shall be taken to build strong safeguards so that there is no comingling of information/documents,records and assets.
4. Security practices and control processes of the Service Provider shall be reviewed and monitored on a regular basis and the Service Providers shall be required to disclose security breaches.
5. Any breach of security and leakage of confidential customer related information shall be notified to RBI.

WEBSITE

The Board Approved-Outsourcing Policy will be hosted on the Company's website i.e. https://fintreefinance.com/contact-us/ for our customer's information and benefit as mentioned in the RBI's circular.