

Rainbow Investments Limited

Outsourcing of Information Technology (IT) services

1. Background:

Rainbow Investments Limited ("the Company") is a Public Limited Company incorporated under the Companies Act, 2013 and is registered with Reserve Bank of India ("RBI") as a Non-deposit taking Non-Banking Financial Company.

This policy is prepared as per the Reserve Bank of India (Outsourcing of Information Technology Services) Directions, 2023 bearing reference no. DoS.CO.CSITEG/SEC.1/ 31.01.015/2023-24 dated 10th April 2023 as amended on 28th November 2025 vide Notification no DOR.ORG.REC.No.282/21-04-158/2025-26..

The Company should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers nor impede effective supervision by the supervising authority. The Company desirous of outsourcing of IT and IT enabled services shall not require prior approval from RBI for outsourcing such activities. However, such arrangements shall be subject to on-site/ off-site monitoring and inspection/ scrutiny by the supervising authority.

2. Definition:

Outsourcing of Information Technology ("IT") Services:

- (i) 'Outsourcing of IT Services' may be defined as use of a service provider to perform activities, as listed below, on a continuing basis. 'Continuing basis' would include agreements for a limited period.

Outsourcing of IT Services mainly covers the following areas but not limited to:

- IT infrastructure management, maintenance and support (hardware/ software/ firmware);
- Network and security solutions maintenance (hardware/ software/ firmware);
- Application Development, Maintenance and Testing;
- Services and operations related to Data Centres;
- Cloud Computing Services;
- Managed Security Services;
- Application Service Providers ("ASPs") including and
- Management of IT infrastructure and technology services associated with payment system ecosystem.

ii. Service Provider: The term "Service Provider" means the provider of IT enabled services. Service Provider includes, but is not limited to, the vendors, agencies, consultants and / or representatives of the third parties. It also includes sub-contractors to whom the third-party service providers may further outsource some activity.

iii. Material Outsourcing of IT Services: Material outsourcing arrangements are those, which if disrupted / compromised, have the potential to:

1. Either significantly impact the Company's
 - (a) Business operations, reputation, strategic plans or profitability;
 - Or (b) Ability to manage risk and comply with applicable laws and

regulations. **Or**

2. In the event of any unauthorised access, loss or theft of customer information may have material impact on the Company's customers.

3. CRITICALITY OF OUTSOURCING OF IT SERVICES:

The Company shall evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks. In this process the Company shall consider important aspects, such as; (a) Determining need for outsourcing based on criticality of activity to be outsourced; (b) Determining expectations / outcome from outsourcing; (c) Determining success factors and cost-benefit analysis; and (d) Deciding the model for outsourcing.

4. Comprehensive assessment of need for outsourcing and attendant risks

Company shall evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks. Company shall inter-alia consider:

- a) determining the need for outsourcing based on criticality of activity to be outsourced;
- b) determining expectations and outcome from outsourcing;
- c) determining success factors and cost-benefit analysis; and
- d) deciding the model for outsourcing.

Compliance with all applicable statutory and regulatory requirements

The company shall consider all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration, when performing its due diligence in relation to outsourcing of IT services.

Grievance Redressal Mechanism

- a) The Company shall have a robust grievance redressal mechanism that shall not be compromised in any manner on account of outsourcing, i.e., responsibility for redressal of customers' grievances related to outsourced services shall rest with the company.
- b) Outsourcing arrangements shall not affect the rights of a customer against the company, including the ability of the customer to obtain redressal as applicable under relevant laws.

Governance Framework

IT Governance is not an isolated activity, but instead occurs within the context of the corporate governance of the organization and it is usually the responsibility of the Board and senior executives of the Company. It consists of the leadership and organizational structures and processes that ensure

that the enterprise's IT sustains and extends its strategies and objectives. The purpose of IT Governance is to direct IT endeavors to ensure that IT's performance meet the following objectives:

- Alignment of IT with the enterprise and realization of the promised benefits;
- Use of IT to enable the enterprise by exploiting opportunities and maximizing benefits;
- Responsible use of IT resources; and
- Appropriate management of IT-related risks;

Thus conceptualization of IT Outsourcing Governance is to focus on identifying objectives that must be achieved through the outsourcing arrangement.

Key Factors for IT outsourced vendor selection strategy:

Following are the key factor of effective IT outsourced vendor selection to meet the objectives within the organization's digital transformation agenda and reduce IT costs;

- The IT vendor should have ability to execute the vision/value proposition.
- There should be Effective Cost/Price analysis.
- Financial stability of the vendor.
- Service and support in terms of maintenance hours, response time, resolution time, security, disaster planning, and other service levels from the vendor.
- Range of Services: It is important that the outsourcing vendor is specialized in providing a range of services.
- Value for money: It is important that the outsourcing vendor provides the services at a reasonable price. The quality of services needs to be at par with the cost that Company is paying for them. The services need to bear the value for money.

Role of the Board

The Board of the company shall be responsible, inter alia, for:

- a) putting in place a framework for approval of IT outsourcing activities depending on risks and materiality;
- b) approving policies to evaluate the risks and materiality of all existing and prospective IT outsourcing arrangements; and
- c) setting up suitable administrative framework of Senior Management for the purpose of these Directions.

Role of the Senior Management

The Senior Management of the company shall, inter alia, be responsible for:

- a) formulating IT outsourcing policies and procedures, evaluating the risks and materiality of all existing and prospective IT outsourcing arrangements based on the framework commensurate with the complexity, nature and scope, in line with the enterprise-wide risk management of the organization approved by the Board and its implementation;

- b) prior evaluation of prospective IT outsourcing arrangements and periodic evaluation of the existing outsourcing arrangements covering the performance review, criticality and associated risks of all such arrangements based on the policy approved by the Board;
- c) identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board/ Board Committee in a timely manner;
- d) 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;
- e) ensuring (i) effective oversight over third party for data confidentiality and (ii) appropriate redressal of customer grievances in a timely manner;
- f) ensuring an independent review and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy and performance standards and reporting the same to Board/ Board Committee; and
- g) creating essential capacity with required skillsets within the organization for proper oversight of outsourced activities.

Role of IT Function

The responsibilities of the IT Function of the company shall, inter alia, include:

- a) assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organization;
- b) ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors;
- c) effectively monitor and supervise the outsourced activity to ensure that the service providers meet the laid down performance standards and provide uninterrupted services, report to the Senior Management; co-ordinate periodic due diligence and highlight concerns, if any; and
- d) putting in place necessary documentation required for contractual agreements including service level management, monitoring of vendor operations, key risk indicators and classifying the vendors as per the determined risk.

EVALUATION AND ENGAGEMENT OF SERVICE PROVIDERS:

In considering or renewing an Outsourced IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis. Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The Company shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single/ few service provider/s. Where possible, the Company shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.

A risk-based approach shall be adopted in conducting such due diligence activities.

Due diligence shall involve an evaluation of all available information, as applicable, 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) security risk assessment, including of the technology assets administered by the service provider;
- k) ensuring that appropriate controls, assurance requirements and possible contractual arrangements are in place to establish data ownership;
- 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 there under including those relating to aspects such as data storage, data protection and confidentiality.

Outsourcing Agreement

Legally binding agreement

- a) Company shall ensure that their rights and obligations and those of each of their service providers are clearly defined and set out in a legally binding written agreement.
- b) In principle, the provisions of the agreement should appropriately reckon the criticality of the outsourced task to the business of the company, the associated risks and the strategies for mitigating or managing them.
- c) The terms and conditions governing the contract shall be carefully defined and vetted by the Company legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow the company to retain adequate control over the outsourced activity and the right to intervene with appropriate measures to meet legal and regulatory obligations.
- d) The agreement shall also bring out the nature of legal relationship between the parties.

Aspects to be considered in agreement

The agreement may include (as applicable to the scope of Outsourcing of IT Services) the following aspects:

- a) details of the activity being outsourced, including appropriate service and performance standards including for the sub-contractors, if any;
- b) effective access by the company to all data, books, records, information, logs, alerts and business premises relevant to the outsourced activity, available with the service provider;
- c) regular monitoring and assessment of the service provider by the company for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;
- d) type of material adverse events and the incidents required to be reported to company to enable company to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;
- e) compliance with the provisions of Information Technology Act, 2000, other applicable legal requirements and standards to protect the customer data;
- f) the deliverables, including Service-Level Agreements (SLAs) formalising performance criteria to measure the quality and quantity of service levels;
- g) storage of data only in India as per extant regulatory requirements;
- h) clauses requiring the service provider to provide details of data captured, processed and stored;
- i) controls for maintaining confidentiality of data of Company and its customers', and incorporating service provider's liability to company in the event of security breach and leakage of such information;
- j) types of data/ information that the service provider (vendor) is permitted to share with Company customer and / or any other party;
- k) specifying the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties;
- l) contingency plan(s) to ensure business continuity and testing requirements;
- m) right to conduct audit of the service provider (including its subcontractors) by the company, 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 about the service provider in conjunction with the services performed for the company;
- n) right to seek information from the service provider about the third parties (in the supply chain) engaged by the former;
- o) recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding

- p) clauses to allow RBI or person(s) authorised by it to access the Company IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and/ or its sub-contractors in relation and as applicable to the scope of the outsourcing arrangement;
- q) including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors;
- r) obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the company;
- s) clauses requiring prior approval/ consent of the company for use of subcontractors by the service provider for all or part of an outsourced activity;
- t) termination rights of the company, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable;
- u) obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of the company;
- v) 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 (including pandemic situations);
- w) clause requiring suitable back-to-back arrangements between service providers and the OEMs; and
- x) clause requiring non-disclosure agreement with respect to information retained by the service provider

Risk Management

Risk Management Framework

- (a) A Risk Management framework for Outsourcing of IT Services shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation/ management and reporting of risks associated with Outsourcing of IT Services arrangements.
- (b) The risk assessments carried out by the company shall be suitably documented with necessary approvals in line with the roles and responsibilities for the Board of Directors, Senior Management and IT Function. Such risk assessments shall be subject to internal and external quality assurance on a periodic basis as determined by the Board-approved policy.
- (c) Company shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the service provider.
- (d) Access to data at Company location / data center by service providers shall be on need-to-know basis, with appropriate controls to prevent security breaches and/or data misuse.
- (e) Public confidence and customer trust in company is a prerequisite for their stability and

reputation. Hence, company shall seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the service provider. Access to customer information by staff of the service provider shall be on need-to-know basis.

- (f) In the event of multiple service provider relationships where two or more service providers collaborate to deliver an end-to-end solution, the company remains responsible for understanding and monitoring the control environment of all service providers that have access to the Company data, systems, records or resources.
- (g) In instances where service provider acts as an outsourcing agent for multiple company, care shall be taken to build adequate safeguards so that there is no combining of minformation, documents, records and assets.
- (h) The company shall ensure that cyber incidents are reported by the service provider without undue delay, so that the incident is reported by the company to the RBI within 6 hours of detection by the TPSP.
- (i) The company shall review and monitor the control processes and security practices of the service provider to disclose security breaches. The company shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, company shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.
- (j) Concentration Risk: company shall effectively assess the impact of concentration risk posed by multiple outsourcings to the same service provider and/or the concentration risk posed by outsourcing critical or material functions to a limited number of service providers.

Business Continuity Plan and Disaster Recovery Plan

- a) The Company shall require their service providers to 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 BCP/ DR requirements.
- b) In establishing a viable contingency plan, company 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.
- c) In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, 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.
- d) company shall ensure that service providers are able to isolate the company’ 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.

Monitoring and Control of Outsourced Activities

- a) The Company shall have in place a management structure to monitor and control its Outsourced IT activities. This shall include (as applicable to the scope of Outsourcing of IT Services) but not limited to monitoring the performance, uptime of the systems and resources, service availability, adherence to SLA requirements, incident response mechanism, etc.
- b) Company shall conduct regular audits (as applicable to the scope of Outsourcing of IT Services) of service providers (including sub-contractors) with regard to the activity outsourced by it. Such audits may be conducted either by Company internal auditors or external auditors appointed to act on Company behalf.
- c) While outsourcing various IT services, more than one company may be availing services from the same third-party service provider. In such scenarios, in lieu of conducting separate audits by individual company of the common service provider, they may adopt pooled (shared) audit. This allows the relevant company to either pool their audit resources or engage an independent third-party auditor to jointly audit a common service provider. However, in doing so, it shall be the responsibility of company in ensuring that the audit requirements related to their respective contract with the service provider are met effectively.
- d) The audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. The frequency of the audit shall be determined based on the nature and extent of risk and impact to the company from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management and in case of any adverse development, the same shall be put up to the Board for information.
- e) Company depending upon the risk assessment, may also rely upon globally recognised third-party certifications made available by the service provider in lieu of conducting independent audits. However, this shall not absolve company of their responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end.
- f) The company shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its Outsourcing of IT Services obligations. Company shall adopt risk-based approach in defining the periodicity. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience preparedness.
- g) In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of the company, the same shall be given due publicity by the company so as to ensure that the customers stop dealing with the concerned service provider.
- h) 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 law.

Outsourcing within a Group / Conglomerate

- a) The Company may outsource any IT activity/ IT enabled service within its business group/ conglomerate, provided that such an arrangement is backed by the Board-approved policy and appropriate service level arrangements/ agreements with its group entities are in place.
- b) The selection of a group entity shall be based on objective reasons that are similar to selection of a third-party, and any conflicts of interest that such an outsourcing arrangement may entail shall be appropriately dealt with.
- c) Company at all times, shall maintain an arm's length relationship in dealings with their group entities. Risk management practices being adopted by the company while outsourcing to a group entity shall be identical to those specified for a non-related party.

Additional requirements for Cross-Border Outsourcing

- a) The engagement of a service provider based in a different jurisdiction exposes the company to country risk. To manage such risk, the company shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk. This includes, inter alia, having appropriate contingency and exit strategies. Further, it shall be ensured that availability of records to the company and the RBI will not be affected even in case of liquidation of the service provider.
- b) The governing law of the arrangement shall also be clearly specified. In principle, arrangements shall only be entered into with parties operating in jurisdictions upholding confidentiality clauses and agreements.
- c) The right of the company and the RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction shall be ensured.
- d) The arrangement shall comply with all statutory requirements as well as regulations issued by the RBI from time to time.

Exit Strategy

Exit Strategy

An exit strategy is necessary to:

- identify possible risks;
- define potential losses; and
- ensure service continuity.

It should be a 'front end' activity i.e. considered when developing your commodity/service strategy. The exit strategy should be included in the procurement documents and contractual terms and conditions where possible. This may appear counterintuitive, but the Company need a strategy which

is consistent with overall sourcing strategy. Otherwise the risk being locked into an unsatisfactory contract.

If an exit strategy is in place at the start of a supplier relationship, The Company's needs should be included in the contract itself. This ensures minimum business and customer disruption if the relationship were terminated. Exit strategies should be reviewed annually, or when significant change occurs.

There are several considerations to be made when developing an exit plan, including:

- Continuing Service Requirements;
- Data Security and Privacy;
- Knowledge and Documentation Transfer;
- Costs; and
- Personnel