TOURISM FINANCE CORPORATION OF INDIA LIMITED
NEW DELHI

IT OUTSOURCING POLICY

1. Introduction

Tourism Finance Corporation of India Limited (TFCI) is a Non-Banking Non-Deposit Taking Systemically Important Financial Company (NBFC-ND-SI) regulated by Reserve Bank of India (RBI).

RBI has issued Master Direction on Outsourcing of Information Technology Services on 10th April 2023 advising NBFCs (classified as 'Top Layer', 'Upper Layer', and 'Middle Layer') to formulate IT outsourcing policy in line with the RBI directions and implement the policy by 1st October 2023.

In the era of digitalization and advancements in information technology, TFCI recognizes the importance of outsourcing IT services to maintain efficiency and competitiveness. TFCI, in accordance with the RBI Master Directions, has formulated 'IT Outsourcing Policy' as detailed in the ensuing paragraphs.

2. Objective of IT Policy

The core objective of IT Outsourcing Policy is to establish a robust framework to manage potential risks and to ensure that any outsourcing arrangements do not compromise TFCI's capacity to meet its commitments to Stakeholders, Customers and Regulators, or interfere with effective business and regulatory procedures. The policy is intended to support legal compliance, enforceability of outsourcing contracts, data confidentiality, and integrity, while also promoting transparency and accountability in IT outsourcing relationships.

As part of this policy, TFCI will adopt prudent selection criteria for choosing service providers, emphasizing that the chosen provider must employ the same high standard of care in executing the services as TFCI would if the activities were conducted internally rather than outsourced. To ensure this, committee of senior executives will be constituted to select IT service providers, shortlisted and recommended by the IT Department. This policy also aims to provide guidelines for effective monitoring and control of outsourced IT activities.

3. Effective Date of IT Policy:

IT Outsourcing Policy shall be effective from 1st October 2023. All IT Contracts commencing before 1st October 2023, must conform to the provisions of Policy either by the renewal date or within 12 months the RBI Master Direction's issuance date of 10.4.2023.

TFCI's System Administrator/CTO shall ensure the comprehensive dissemination of this policy among all relevant stakeholders, fostering a culture of compliance and awareness.

4. Definitions:

For the purpose of this IT Outsourcing Policy, the following definitions shall apply:

a) "Outsourcing" / "IT Outsourcing" refers to the delegation of an organization's IT-related activities, functions, or processes to a third party, either affiliated within a corporate group or external to the group, to perform these tasks on a continuing basis, either partially or completely. This may include agreements or letters for a limited period.

b) "Service Provider" refers to a third-party entity engaged by TFCI to perform IT-related activities, functions, or processes that would otherwise be carried out in-house by the organization.

c) "Material Outsourcing" refers to the outsourcing of IT-related activities, functions, or processes that have a significant impact on the organization's Business operations or on its customers in event of any unauthorized access, loss or theft of customer information.

d) "Outsourcing Agreement" refers to a legally binding contract between TFCI and a service provider, outlining the terms, conditions, roles, responsibilities, and expectations of both parties involved in the outsourcing relationship.

e) "Due Diligence": Due diligence is a comprehensive and systematic process conducted by TFCI to evaluate the qualifications, capabilities, reputation, and financial stability of a potential service provider before entering into an outsourcing agreement. This assessment considers various aspects, including but not limited to, the service provider's financial stability, technical capabilities, management expertise, regulatory compliance, data protection measures, business continuity plans, and exit strategies. While this policy highlights specific areas of focus for due diligence, it is not an exhaustive list, and TFCI may consider additional factors or information as deemed necessary to ensure a well-informed decision-making process.

f) "Risk Assessment" refers to the identification, evaluation, and prioritization of potential risks associated with IT outsourcing, including operational, financial, reputational, legal, and regulatory risks, to ensure that appropriate mitigation measures are in place.

g) "Confidentiality" refers to the obligation of the service provider to protect sensitive information and data shared by TFCI, ensuring that such information is not disclosed to unauthorized parties.

h) "Security" refers to the measures taken by the service provider to safeguard TFCI's information, data, systems, and networks from unauthorized access, misuse, and potential threats.

i) "Business Continuity" refers to the service provider's ability to maintain essential IT services and operations in the event of unforeseen disruptions or disasters, ensuring the resilience and continued functionality of TFCI's business processes.

j) "Offshore Outsourcing" refers to the practice of engaging a service provider located in a foreign country to perform IT-related activities, functions, or processes on behalf of TFCI.

K) "Arm's length" refers to the practice of conducting business transactions as if they were between unrelated parties, to ensure that there is no preferential treatment given to a particular entity within the group. This is done to ensure transparency and fairness in the outsourcing process.

5. IT Outsourcing Activities: In-Scope, Out-Scope and Identification

5.1 In-Scope: The scope of this policy covers all aspects of IT outsourcing. Outsourcing of IT Services shall include following activities:

- IT infrastructure management, maintenance and support (hardware, software or firmware)
- Network and security solutions, maintenance (hardware, software or firmware);
- Application Development, Maintenance and Testing
- Application Service Providers (ASPs)
- Services and operations related to Data Centres
- Cloud Computing Services
- Managed Security Services

5.2 Out-Scope:

Any activity which if outsourced would lead to increased reputational risk and/or regulatory non-compliance risk. TFCI shall review the list of activities that are not to be outsourced periodically and update it based on the changing circumstances and regulatory guidelines.

5.2.1 Indicative Services/Activities not considered under "Outsourcing of IT Services":

- Corporate Internet Banking services
- External audits like Vulnerability Assessment/Penetration Testing (VA/PT), Information Systems Audit, and security review
- SMS gateways
- Procurement of IT hardware/appliances
- Acquisition of IT software/product/application on a license or subscription basis
- Maintenance services for IT infrastructure or licensed products provided by the Original Equipment Manufacturer (OEM)
- Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.
- Services obtained by an NBFC as a sub-member of a Centralized Payment Systems (CPS) from another NBFC
- Business Correspondent (BC) services, payroll processing, statement printing

5.2.2 Entities not considered as Third-Party IT Service Providers:

- Vendors providing business services using IT
- Payment System Operators authorized by the RBI
- Partnership-based Fintech firms providing co-branded applications, services, or products
- Services of Fintech firms for data retrieval, validation, and verification, such as bank statement analysis, GST returns analysis, vehicle information fetching, digital document execution, data entry, and call centre services
- Telecom Service Providers from whom leased lines or similar infrastructure are availed for data transmission
- Security/Audit Consultants appointed for certification/audit/VA-PT related to IT infrastructure, IT services, or Information Security services.

5.2.3 Identification of IT Outsourcing Activities

TFCI shall identify IT activities to be outsourced based, inter-alia, on the following parameters:

- Criticality: IT activities critical to TFCI's business shall be identified, and its outsourcing if needed shall be done with utmost care.
- Complexity: IT activities that require high technical expertise and knowledge not available in-house shall be identified, and its outsourcing shall be done to service providers who possess the required skill set.
- Cost: IT activities that can be outsourced to reduce cost of operations without compromising on quality shall be identified.
- Legal and Regulatory Compliance: IT activities that require compliance with certain legal and regulatory requirements not available with TFCI shall be identified, and its outsourcing shall be done only to service providers who meet such compliance requirements.
- Strategic Importance: IT activities that are crucial to TFCI's strategic goals shall be identified, and its outsourcing may be considered with a focus on long-term sustainability.

6. Role of TFCI in IT Outsourcing

6.1 Regulatory and Supervisory requirements:

a) Outsourcing of any activity shall not diminish TFCI's obligations as also of its Board and Senior Management, who shall be ultimately responsible for the outsourced activity.

b) TFCI shall take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by TFCI, if the same activity was not outsourced.

c) TFCI shall not engage an IT service provider that would result in reputation of TFCI being compromised or weakened.

d) Notwithstanding whether the service provider is located in India or abroad, TFCI shall ensure that outsourcing should neither impede nor interfere with its ability to effectively oversee and manage activities. Further, TFCI shall ensure that the outsourcing does not impede the RBI in carrying out its supervisory functions and objectives.

e) TFCI shall ensure that the service provider, if not a group company, shall not be owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of TFCI, or their relatives. The terms 'control', 'director', 'key managerial personnel', and 'relative' have the same meaning as assigned under the Companies Act, 2013 and the Rules framed thereunder from time to time. However, an exception to this requirement may be made with the approval of Board/Board level Committee, followed by appropriate disclosure, oversight and monitoring of such arrangements. The Board shall *inter-alia* ensure that there is no conflict of interest arising out of third-party engagements.

f) TFCI should consider the following additional requirements pertaining to usage of cloud computing services:

- Analyze the business strategy, goals, and IT application costs to determine cloud adoption suitability.
- Address the entire data lifecycle, from data generation to permanent deletion, in the IT outsourcing policy.
- Consider multi-tenancy and multi-location data storage risks when establishing a risk management framework.

- Adopt a well-documented cloud adoption policy that includes due diligence and monitoring of cloud service providers (CSPs).
- Prefer secure container-based data management with encryption keys and Hardware Security Modules under TFCI control.
- Establish Identity and Access Management (IAM) agreements with CSPs to ensure role-based access to cloud-hosted applications.
- Implement security controls in cloud-based applications to achieve similar or higher degrees of control as on-premise applications.
- Define minimum monitoring requirements in the cloud environment and integrate logs and events from the CSP into the TFCI's SOC.
- Ensure CSPs have a well-governed approach to manage threats and vulnerabilities, and implement robust incident response and recovery practices, including disaster recovery (DR) drills.

g) TFCI shall adopt the following requirements when outsourcing Security Operations centre (SOC) operations to mitigate risks associated with data storage, processing, and management by a third party (Managed Security Service Provider (MSSP)):

- Clearly identify the owner of assets utilized in providing the services, such as systems, software, source code, processes, and concepts.
- Ensure that TFCI maintains adequate oversight and ownership overrule definition, customization, and related data/logs, metadata, and analytics specific to the organization.
- Periodically assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored/processed.
- Integrate the outsourced SOC reporting and escalation process with TFCI's incident response process.
- Review the process of handling alerts/events within the outsourced SOC operations.

6.2 Comprehensive assessment of need for outsourcing and attendant risks TFCI 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. TFCI 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.

6.3 Compliance with all applicable statutory and regulatory requirements

TFCI 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.

6.4 Grievance Redressal Mechanism

a) TFCI shall continue to 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 TFCI.

b) Outsourcing arrangements shall not affect the rights of a customer against TFCI, including the ability of the customer to obtain redressal as applicable under relevant laws.

6.5. Inventory of Outsourced Services

TFCI shall create an inventory of services provided by the service providers (including key entities involved in their supply chains). Further, TFCI shall map their dependency on third parties and periodically evaluate the information received from the service providers.

7. Governance Framework in IT Outsourcing:

Role of IT Function:

The responsibilities of the IT Function headed by CTO shall, *inter alia*, include:

a) assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation;

b) ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Senior Management, Auditors, IT Committee, Board and Regulators;

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.

e) 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 organisation approved by the Board and its implementation;

f) 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.

g) identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the MD/WTD and IT Committee in a timely manner;

h) 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;

i) ensuring effective oversight over third party for data confidentiality and appropriate redressal of customer grievances in a timely manner;

j) ensuring an independent review and audit on a periodic basis for compliance with the legislations, regulations, policy and reporting the same to MD/WTD and IT Committee; and

k) creating essential capacity with required skillsets within TFCI for proper oversight of outsourced activities and carrying the outsourced work.

8. Evaluation and Engagement of Service Providers

8.1. Due Diligence on Service Providers

a) In considering or renewing an Outsourcing of 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.

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

c) Due diligence shall take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. Where possible, TFCI shall obtain independent reviews and market feedback on the service provider to supplement its own assessment.

d) TFCI shall also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.

8.2. Aspects to be considered

Due diligence shall involve 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 TFCI 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 TFCI'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.

9. Outsourcing Agreement

9.1 Legally binding agreement

a) TFCI 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 TFCI, 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 TFCI's legal counsel for their legal effect and enforceability. The agreement shall be sufficiently flexible to allow TFCI 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.

9.2. Aspects to be considered in agreement

The agreement at a minimum should 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 RE 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 RE for continuous management of the risks holistically, so that any necessary corrective measure can be taken immediately;

d) type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to TFCI to enable it 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 (related to TFCI and its customers) captured, processed and stored;

i) controls for maintaining confidentiality of data of TFCI and its customers', and incorporating service provider's liability to TFCI in the event of security breach and leakage of such information;

j) types of data/ information that the service provider is permitted to share with TFCI's 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 sub-contractors) by TFCI, 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 TFCI;

n) right to seek information from the service provider about the third parties engaged by the former;

o) recognising the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow RBI or person(s) authorised by it to access the TFCI's 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;

p) including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors;

q) 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 TFCI;

r) clauses requiring prior approval/ consent of TFCI for use of sub-contractors by the service provider for all or part of an outsourced activity;

s) termination rights of TFCI, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable;

t) obligation of the service provider to co-operate with the relevant authorities in case of insolvency/ resolution of TFCI;

u) 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);

v) clause requiring suitable back-to-back arrangements between service providers and the OEMs; and

w) clause requiring non-disclosure agreement with respect to information retained by the service provider.

10. Monitoring and Control of Outsourced Activities

a) TFCI 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) TFCI 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 TFCI's internal auditors or external auditors appointed to act on behalf of TFCI.

c) 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 TFCI 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 IT Committee/Board for information.

d) TFCI 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 TFCI 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.

e) TFCI 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.. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality, and security, and in operational resilience preparedness.

f) In the event of termination of the outsourcing agreement for any reason in cases where the service provider deals with the customers of TFCI, the same shall be given due publicity by TFCI so as to ensure that the customers stop dealing with the concerned service provider.

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

11. Outsourcing within a Group/ Conglomerate

a) TFCI 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) TFCI, at all times, shall maintain an arm's length relationship in dealings with their group entities. Risk management practices being adopted by TFCI while outsourcing to a group entity shall be identical to those specified for a non-related party.

11.2 Additional requirements for Cross-Border Outsourcing

a) The engagement of a service provider based in a different jurisdiction exposes TFCI to country risk. To manage such risk, TFCI 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 TFCI 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 TFCI 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.

12. Exit Strategy:

a) The Outsourcing of IT Services policy shall contain a clear exit strategy with regard to outsourced IT activities/ IT enabled services, while ensuring business continuity during and after exit. 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, TFCI shall, *inter alia*, identify alternative arrangements, which may include performing the activity by a different service provider or TFCI itself.

b) TFCI shall ensure that IT outsourcing agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. The service provider shall be legally obliged to cooperate fully with both TFCI and new service provider(s) to ensure there is a smooth transition. 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 TFCI.

*****