POLICY FOR OUTSOURCING OF INFORMATION TECHNOLOGY SERVICES

RECORD OF REVIEW:

Document Number	01
Version Number	02
Document Classification	External
Originally formulated	March 30, 2023
Created by	IT Department
Reviewed by	IT Strategy Committee
Approved by	Board of Directors of the Company

Version No	Created/Modified Date	Created/modified by	Approved by
1	March 30, 2023	IT Department	Board of Directors
2	May 30, 2023	IT Department	Board of Directors

1. BACKGROUND:

Berar Finance Limited ("BFL" or "Company") is a Public Limited Company incorporated under the Indian Companies Act, 1956 and is registered with the Reserve Bank of India ("RBI") as a deposit taking non-banking finance company ("NBFC").

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:

i. Outsourcing of Information Technology ("IT") Services: '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. ROLE IN OUTSOURCING OF IT SERVICES- REGULATORY AND SUPERVISORY REQUIREMENTS:

4.1 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.

4.2 Outsourcing of any activity of the Company shall not diminish its obligations, including its Board and Senior Management, who shall be ultimately responsible for the outsourced activity. The Company 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 the Company if the same activity was not outsourced. Accordingly, the Company shall not engage an IT service provider that would result in reputation of the Company being compromised or weakened.

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

4.4 The Company shall ensure that the service provider shall neither impede/ interfere with the ability of the Company to effectively oversee and manage its activities nor impede the supervising authority in carrying out the supervisory functions and objectives.

4.5 The Company 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 the Company, 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 there under 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.

5. GRIEVANCE REDRESSAL MECHANISM:

5.1 The Company shall have a robust grievance redressal mechanism as provided in the Grievance Redressal Mechanism Policy, which in no way shall be compromised on account of outsourcing i.e., responsibility for redressal of customers' grievances related to outsourced services shall rest with the Company.

5.2 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.

6. GOVERNANCE FRAMEWORK:

6.1 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.

6.2 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.

7. ROLE OF THE BOARD: The Board shall be responsible, *inter alia*, for:

7.1 approving a framework to evaluate the risks and materiality of all existing and prospective IT outsourcing arrangements as also policies that apply to such arrangements;

7.2 putting in place a framework for approval of IT outsourcing activities depending on risks and materiality; and

7.3 setting up suitable administrative framework of Senior Management for the purpose of these directions.

Further the Board may delegate the above responsibilities to IT Strategy Committee of the Company.

8. ROLE OF THE SENIOR MANAGEMENT: The Senior Management shall, *inter alia*, be responsible for:

8.1 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 and in line with the enterprise-wide risk management of the organization approved by the Board and its implementation;

8.2 prior evaluation of prospective IT outsourcing arrangements and periodic evaluation of the existing outsourcing arrangements covering performance review, criticality and associated risks of all such arrangements based on the policy approved by the Board;

8.3 identifying IT outsourcing risks as they arise, monitoring, mitigating/managing and reporting on such risks to the Board/ Board Committee in a timely manner;

8.4 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;

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

8.6 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

8.7 Creating essential capacity with required skillets within the organization for proper oversight of outsourced activities.

9. ROLE OF IT FUNCTION: The responsibilities of the IT Function shall, *inter alia*, include:

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

9.2 ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, auditors and supervisors;

9.3 effectively monitor and supervise the outsourced activity to ensure that the service providers meet the laid down performance standard and provide uninterrupted services, and report to the Senior Management; Co-ordinate periodic due diligence and highlight concerns, if any; and

9.4 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.

10. EVALUATION AND ENGAGEMENT OF SERVICE PROVIDERS:

10.1 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.

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

10.3 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.

11. OUTSOURCING AGREEMENT:

11.1 The Company shall ensure that its rights and obligations and those of each of its service providers are clearly defined and set out in a legally binding written agreement. 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.

11.2 The terms and conditions governing the contract shall be carefully defined and vetted by the Company's 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.

11.3 The agreement shall also bring out the nature of legal relationship between the parties, i.e., whether agent, principal or otherwise.

11.4 Some key areas that should be covered by the agreement (as applicable to the scope of Outsourcing of IT Services) are as follows:

a. details of the IT 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. continuous monitoring and assessment of the service provider by the Company, so that any necessary corrective measure can be taken immediately; including termination clause and minimum period to execute such provision, if deemed necessary;

d. type of material adverse events (e.g., data breaches, denial of service, service unavailability etc.) and incident reporting requirements to the Company to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines;

e. compliance with the provisions of IT Act, other applicable legal requirements and standards to protect the customer data;

f. the deliverables, including Service-Level Agreements ("SLAs") formalizing 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 the Company and its customers) captured, processed and stored;

i. controls for maintaining confidentiality of data of the Company and its customers', and incorporating service provider's liability towards the 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 the Company'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 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. Recognizing 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) authorized by it to access the Company'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 to 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 of the Company outsourced to the service provider through specific contractual terms and conditions specified by the Company.

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

s. Termination rights of the Company, 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 the Company;

u. provision to consider resources of service provider who provide core services as "essential personnel" so that a limited number of staff 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;

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

x. Provide training to the employees of the Company wherever required.

The Company has the right to extend the above clauses of the agreement to any agencies to which the service provider sub-contracts any activity related to IT services outsourced by the Company.

12. RISK MANAGEMENT:

12.1 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.

12.2 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, Board Committees, Senior Management and IT Function. Such risk assessments shall be subject to internal/ external quality assurance on a periodic basis.

12.3 The Company shall be responsible for the confidentiality and integrity of data / information pertaining to the customers that is available to the service provider. Also, access to data at Company's location / data centre by service providers shall be on need-to-know basis, with

appropriate controls to prevent security breaches and/or data misuse.

Public confidence and customer trust in the Company is a prerequisite for their stability and reputation. Hence the 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".

12.4 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's data, systems, records or resources.

12.5 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 Information, documents, records and assets. The Company shall ensure that a Non-Disclosure Agreement ("NDA") is in place even after the contract expires/is terminated.

12.6 The Company shall ensure that cyber incidents are reported to the Company 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 Third-Party Service Provider.

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 the supervising authority in the event of breach of security and leakage of confidential customer related information. In these eventualities, the Company shall adhere to the baseline expectations of Incident Response and Recovery Management.

12.7 Management of concentration risk – the 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.

13. BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN:

13.1 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.

13.2 In establishing a viable contingency plan, the 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.

13.3 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 its IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

13.4 The Company shall ensure that service providers are able to isolate the Company's information, documents and records and other assets. This is to ensure that in adverse conditions and/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 in order to continue its business operations, or deleted, destroyed or rendered unusable.

14. MONITORING AND CONTROL OF OUTSOURCED ACTIVITIES:

14.1 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/ resources, service availability, adherence to SLA requirements, incident response mechanism, etc.

14.2 The 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's internal auditors or external auditors appointed to act on Company's behalf. Such periodic audits shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws/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.

14.3 The Company, depending upon the risk assessment, may also rely upon globally recognized third-party certifications made available by the service provider in lieu of conducting independent audits. However, this shall not absolve the Company of its responsibility in ensuring assurance on the controls and procedures required to safeguard data security (including availability of systems) at the service provider's end.

14.4 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. Such due diligence reviews shall highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

14.5 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.

14.6 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 authorized under law.

15. OUTSOURCING WITHIN A GROUP/ CONGLOMERATE:

15.1 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.

15.2 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.

15.3 The 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.

16. ADDITIONAL REQUIREMENTS FOR CROSS-BORDER OUTSOURCING:

16.1 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 the service provider's country's government policies and its political, social, economic and legal conditions on a continuous basis, and 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 supervising authority will not be affected even in case of liquidation of the service provider.

16.2 In principle, arrangements shall only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement shall also be clearly specified. However, the jurisdiction of the courts outside India, where data is stored and/ or processed, shall not extend to the operations of the Company in India, on the strength of the fact that the Company's data is being stored and/ or processed there, even

though the actual transactionsare undertaken in India.

16.3 The right to conduct audit/ inspection of the service provider based in a different jurisdiction shall be ensured.

16.4 The arrangement shall comply with law/ regulations issued by RBI from time to time.

17. EXIT STRATEGY:

17.1 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

Below suggests some factors for consideration in exit strategy. This is not conclusive: each contract / supplier relationship should be considered on its own merits.

a. Continuing Service Requirements:

An exit strategy should set the service requirements when the parties are transitioning out of the relationship. These requirements may include:

- An obligation on the supplier to continue service performance during the transition period. During transition these services must stay at the same quality level and continue to comply with all contract obligations.
- The provision of parallel services for a certain period. This term can be extended as necessary to resolve issues before the final changeover.
- A supplier obligation to maintain the same supplier team during the transition period.
- Confidentiality on any communications regarding the termination of the relationship.

b. Data Security and Privacy:

Data privacy and security are critical. The Exit Strategy should consider provision for:

- The vendor should transfer all data belonging to the Company, including any customer information;
- An acceptable method for the supplier to destroy and remove the Company's proprietary information; and
- The supplier destroying and removing sensitive information from all media. The supplier must ensure no information is disclosed to other individuals or other entities.

c. Knowledge and Documentation Transfer:

Strict documentation and knowledge transfer contract requirements will be advantageous. Following points need to be considered in this regard:

- Clearly state responsibilities i.e. which party owns the work performed by the supplier and which party is responsible for the transfer of ownership.
- Fully document the service description for any transition period additional services. These are services required from the supplier e.g. employee training, training new supplier personnel.
- Require the supplier to provide the Company with copies of information copies of data, procedures, access logs, error logs, documentation and other information generated as a part of providing the contract services. The supplier should also grant the right to provide this information to potential successor suppliers.

d. Costs:

Transition, termination and timing are a key part of the financial aspects of an exit strategy. Be sure the contract:

- Will not penalise the Company for an early exit. This is especially if the termination is due to the supplier's failure to perform the contract.
- Specifies when compensation should be paid and how much. This includes compensation for any continuing base services and transition activities.
- Specifies the return of any pre-paid fees for services which have not been supplied.

e. Personnel:

An exit strategy should cover personnel issues, such as:

- Ensuring supplier personnel and key resources remain on the project and committed during the transition. This ensures relevant knowledge and expertise is retained during transition.
- Defining the exit-strategy team and its roles.

17.2 The Company shall ensure that the agreement has necessary clauses on safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the Company and new service provider(s) to ensure there is smooth transition and to agree to not to erase, purge, revoke, alter or change any data during the transition period, unless specifically advised by the regulator/ concerned Company.

17.3 The Company shall require the service provider to preserve documents as required by law and take suitable steps to ensure that Company's interests are protected, even post termination of the services. The Company may execute a non-disclosure agreement with respect to information retained by the service provider.

18. STORAGE, COMPUTING AND MOVEMENT OF DATA IN CLOUD ENVIRONMENTS- USAGE OF CLOUD COMPUTING SERVICES:

The Company shall adopt the following requirements for storage, computing and movement of data in cloud environments:

18.1 While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

18.2 In engaging cloud services, the Company shall ensure, *inter alia*, that the agreement addresses the entire lifecycle of data, i.e. covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The Company shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

18.3 In adoption of cloud services, The Company shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attended risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the Company and the Cloud Service Provider (CSP). The Company may refer to some of the cloud security best practices, for implementing necessary controls, as per applicability of the shared responsibility model in the adoption of cloud services.

18.4 **Cloud Governance:** The Company shall adopt and demonstrate a well-established and documented cloud adoption Policy. Such a policy should, *inter alia*, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

18.5 **Cloud Service Providers ("CSP"):**

Considerations for selection of CSP: The Company shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. The Company shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements cast under Indian laws and the rights available there under to the Company, including those relating to aspects such as data storage, data protection and confidentiality.

18.6 **Cloud Services Management and Security Considerations:**

a. **Service and Technology Architecture:** The Company shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognised architecture principles and standards. The Company shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the Company. The architecture should provide for a standard set of tools and processes to manage containers, images and releases. Multi- tenancy environments should be protected against data integrity and confidentiality risks and against co-mingling of data. The architecture should enable smooth recovery and any failure of any one or combination of components across the cloud architecture should not result in data/ information security compromise.

b. **Identity and Access Management ("IAM"):** IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user- access and privileged-access roles in the cloud-hosted applicationirrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges' and require the Company's approval and monitoring. In addition, multi-factor authentication should be implemented for access to cloud applications.

c. **Security Controls:** The Company shall ensure 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-premise application. This includes ensuring - secure connection through appropriate deployment of network security resources and their configurations; appropriate and secure configurations, monitoring of the cloud assets utilized by the Company; necessary procedures to authorize changes to cloud applications and related resources.

d. **Robust Monitoring and Surveillance:** The Company shall accurately define minimum monitoring requirements in the cloud environment. The Company should ensure to assess the information/ cyber security capability of the cloud service provider, such that, the

a. CSP maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats;

b. CSP is able to maintain its information/ cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment;
c. nature and frequency of testing of controls by the CSP in respect of the outsourced services is commensurate with the materiality of the services being outsourced by the Company and the threat environment; and
d. CSP has mechanisms in place to assess the sub-contractors with regards to confidentiality, integrity and availability of the data being shared with the sub-contractors, where applicable.

e. Appropriate integration of logs, events from the CSP into the Company's SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for real-time incident reporting and handling of incidents relating to services deployed on the cloud.

f. The Company own efforts in securing its application shall be complemented by the CSP's cyber resilience controls. The CSP / Company shall ensure continuous and regular updates of security-related software including upgrades, fixes, patches and service packs for protecting the application from advanced threats/ malware.

g. Vulnerability Management: The Company shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.

18.7 Disaster recovery & cyber resilience:

a) The Company business continuity framework 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.

b) The Company shall ensure that the CSP puts in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them. This should be systematically ensured *inter alia* through robust incident response and recovery practices including conduct of Disaster Recovery ("DR") drills at various levels of cloud services including necessary stakeholders.

18.8 The following points may be evaluated while developing an exit strategy:

a) the exit strategy and service level stipulations in the SLA shall factor in, *inter alia*,
   i) agreed processes and turnaround times for returning the Company's service collaterals and data held by the CSP;
   ii) data completeness and portability;
   iii) secure purge of Berar Financial Limited information from the CSP's environment;
   iv) smooth transition of services; and
   v) Unambiguous definition of liabilities, damages, penalties and indemnities.

b) Monitoring the ongoing design of applications and service delivery technology stack that the exit plans should align with.

c) 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 Company's business, while maintaining integrity and security.

d) All records of transactions, customer and operational information, configuration data should be promptly taken over in a systematic manner from the CSP and purged at the CSP-end and independent assurance sought before signing off from the CSP.

18.9 Audit and Assurance:

The audit/ periodic review/ third-party certifications should cover, as per applicability and cloud usage, *inter alia*, aspects such as roles and responsibilities of both the Company and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response and resilience preparedness and testing, etc.

19. OUTSOURCING OF SECURITY OPERATIONS CENTER ("SOC"):

Outsourcing of SOC operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider ("MSSP") to which the Company have lesser visibility. To mitigate the risks, in addition to the controls prescribed, the Company shall adopt the below mentioned requirements in the case of outsourcing of SOC operations:

a) Unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);

b) ensure that the Company has adequate oversight and ownership over the rule definition, customization and related data/ logs, meta-data and analytics (specific to the Company);

c) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;

d) integrate the outsourced SOC reporting and escalation process with the Company incident response process; and

e) Review the process of handling of the alerts / events.

20. TECHNOLOGY AND DATA REQUIREMENT:

20.1 Collection, usage and sharing of data with third parties:

a. The Company shall ensure that any collection of data by its Digital Lending Apps (DLAs) and DLAs of its Lending Service Providers (LSPs) is need-based and with prior and explicit consent of the borrower having audit trail. In any case, the Company shall also ensure that DLAs desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, etc. A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only, with the explicit consent of the borrower.

b. The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data.

c. The purpose of obtaining borrowers' consent needs to be disclosed at each stage of interface with the borrowers.

d. Explicit consent of the borrower shall be taken before sharing personal information with any third party, except for cases where such sharing is required as per statutory or regulatory requirement.

20.2 Storage of data:

a. The Company shall ensure that LSPs/DLAs engaged by them do not store personal information of borrowers except some basic minimal data (viz., name, address, contact details of the customer, etc.) that may be required to carry out their operations. Responsibility regarding data privacy and security of the customer's personal information will be that of the Company.

b. The Company shall ensure that clear policy guidelines regarding the storage of customer data including the type of data that can be stored, the length of time for which data can be stored, restrictions on the use of data, data destruction protocol, standards for handling security breach, etc., are put in place and also disclosed by DLAs of the Company and of the LSP engaged by the Company prominently on their website and the apps at all times.

c. The Company shall ensure that no biometric data is stored/ collected in the systems associated with the DLA of Company/ their LSPs, unless allowed under extant statutory guidelines.

d. The Company shall ensure that all data is stored only in servers located within India, while ensuring compliance with statutory obligations/ regulatory instructions.

20.3 Comprehensive privacy Policy:

a. The Company shall ensure that their DLAs and LSPs engaged by them have a comprehensive privacy policy compliant with applicable laws, associated regulations and RBI guidelines. For access and collection of personal information of borrowers, DLAs of Company/LSPs should make the comprehensive privacy policy available publicly

b. Details of third parties (where applicable) allowed to collect personal information through the DLA shall also be disclosed in the privacy policy.

20.4 Technology standards:

The Company shall ensure that they and the LSPs engaged by them comply with various technology standards/ requirements on cybersecurity stipulated by RBI and other agencies, or as may be specified from time to time, for undertaking digital lending.

21. REVIEW:

The Policy shall be reviewed by the Board once every year. The Policy is subject to change in accordance with guidelines/ directions issued by the RBI.

****