PFSPL/FY2026-27/1.0

PAHAL FINANCIAL SERVICES PRIVATE LIMITED

Policy on Outsourcing of Information Technology (IT) Services

Registered Office: 7th Floor, Binori B Square – 2, Opp. Hathising ni Vadi, Ambli Iscon Road, Ahmedabad – 380054

Email: ho@pahalfinance.com Website: www.pahalfinance.com Ph. No.: +91 2717 479169

Policy on Outsourcing of Information Technology (IT) Services

1. Preamble

This Policy shall be termed as the Policy on Outsourcing of Information Technology (IT) Services for Pahal Financial Services Private Limited (hereinafter referred as 'PFSPL' or 'Company') a Microfinance Institution "MFI" and is registered with the Reserve Bank of India as Non-Banking Financial Company - Micro Finance Institution "NBFC-MFI" under Section 45 IA having its registered office in Ahmedabad (Gujarat).

This Policy on Outsourcing of Information Technology (IT) Services is framed in accordance with the *Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025* issued vide RBI/DOR/2025-26/363 dated November 28, 2025.

2. Objective of the Policy

The IT Outsourcing Policy provides management directive to govern & manage technology outsourcing arrangements for Pahal Financial Services Private Limited through appropriate control measures across the entire life cycle of outsourcing engagements. PFSPL shall evaluate the risks and increase benefits of technology outsourcing by:

Defining governance framework for evaluation and onboarding of technology outsourcing partner:

- Establish a risk management framework to identify and manage risks associated with technology outsourcing.
- Enabling the team to develop & deploy the right set of controls for better management of outsourcing services.

3. Definitions & Interpretations

- '**IT services'** means IT services / IT enabled services / IT activities.
- '**Material Outsourcing of IT Services'** are those which:
  i. if disrupted or compromised shall have the potential to significantly impact the NBFC's business operations; or
  ii. may have material impact on the NBFC's customers in the event of any unauthorised access, loss, or theft of customer information.
- **Service Provider'** means provider of IT services including entities related to the NBFC, or those which belong to the same group or conglomerate to which the NBFC belongs.

List of vendors and entities that shall not be considered as 'Service Providers'

i. vendors providing business services using IT (e.g., BCs).
ii. Payment System Operators (PSOs) authorised by RBI under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India.

iii. partnership based FinTech firms such as those providing co-branded applications, products, and services (would be considered under outsourcing of financial services in Chapter III).

iv. FinTech firms providing services for data retrieval, and data validation and verification such as, financial statement analysis, GST returns analysis, fetching of vehicle information, digital document execution, data entry and call centre services.

v. telecom service providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of data; and

vi. security or audit consultants appointed for certification, audit or VA / PT related to IT infra, IT services, or Information Security services in their role as independent third-party auditor, consultant, lead implementer.

- **'Sub-contractor'** refers to those providing material / significant IT services to the service provider and is specific to the material / significant IT services arrangement that the NBFC has entered into with the service provider.

4. Applicability

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

5. Materiality and Non-Materiality of Outsourcing

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

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

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

Non materiality of outsourcing arrangement can be defined as any of the services which do not fall under the ambit of the respective points defining materiality above, for e.g. resource based outsourced personnel, application development etc.

6. Authorisation, Accountability, and Oversight

PFSPL shall ensure that:

- all relevant laws, regulations, rules, guidelines and conditions of approval, licensing or registration shall be considered when performing due diligence in relation to outsourcing.
- outsourcing, whether the service provider is located in India or outside, does not impede RBI in carrying out its supervisory functions and objectives, or diminish the ability of a company to fulfil its obligations to the regulator / supervisor.
- outsourcing, whether the service provider is located in India or outside, does not impede or interfere with the ability of a company to effectively oversee and manage its activities, and fulfil its obligations.
- outsourcing would not result in the compromise or weakening of a company's internal control, business conduct, or reputation.
- the service provider employs the same high standard of care in performing the services as would be employed by the company, if the activities were conducted within the company and not outsourced; and
- the service provider, if not a group company of PFSPL , 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 having the same meaning as assigned under Companies Act, 2013 and the Rules framed thereunder, as amended from time to time.

7. IT Outsourcing Governance Framework

The framework ensures effective oversight, accountability, and adherence to regulatory requirements, fostering a robust governance structure that supports PFSPL's strategic objectives and risk management efforts.

A. Role of the Board (IT Strategy Committee)

The IT Strategy Committee of the Board (ITSC) functions as the primary technology governance entity within PFSPL, aiding the Board of Directors in the formulation and execution of effective IT strategies. This committee shall be entrusted with the oversight responsibility on governance of IT outsourcing contracts.

In addition to responsibilities covered in IT policy, IT Strategy committee shall be responsible for:

- Overseeing and approving all IT outsourcing arrangements based on risks and materiality.
- Putting in place a framework for approval of IT outsourcing activities depending on risk and materiality.
- Setting up suitable administrative framework of Senior Management.
- Review all material IT outsourcing arrangements at least annually, covering performance, risks, concentration, incidents, exit readiness, and regulatory compliance.

B. Role of Senior Management (IT Steering Committee)

The IT Steering Committee, composed of Senior Management representatives from business units, will serve an instrumental role in supporting the IT Strategy Committee of the Board as well as Board in executing the IT Outsourcing Policy and ensuring compliance to regulatory guidelines.

In addition to responsibilities covered in IT policy, IT Steering committee shall be responsible for:

- 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 NBFC approved by the Board and its implementation.
- 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.
- Identifying IT outsourcing risks as they arise, monitoring, mitigating, managing and reporting of such risks to the Board or a Committee of the Board in a timely manner.
- Ensuring that suitable business continuity plans based on realistic and probable disruptive scenarios, including exit of any service provider, are in place and tested periodically.
- Ensuring (a) effective oversight over the service provider (and its subcontractors) for data confidentiality and (b) appropriate redressal of customer grievances in a timely manner
- 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 or a Committee of the Board; and
- Creating essential capacity with required skillsets within the company for proper oversight of outsourced services.

C. Role of IT Function

The responsibilities of the IT Function include

- Assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the NBFC
- Ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, auditors, and supervisors
- Effectively monitoring and supervising the outsourced IT activity to ensure that the service provider meets the laid down performance standards and provides uninterrupted services, reporting to the Senior Management, co ordinating periodic due diligence, and highlighting concerns, if any; and
- 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.

[Role of IT Head, CISO has been clearly defined in IT IS Policy]

8. Risk Management for Outsourcing Policy

A. Need for an Outsourcing Policy

The company shall evaluate the need for outsourcing of IT services based on a comprehensive assessment of attendant benefits, risks, and availability of commensurate processes to manage those risk. It shall consider

- the need for outsourcing based on materiality / criticality of activity to be outsourced
- expectations and outcomes from outsourcing
- success factors and cost-benefit analysis; and
- the model for outsourcing.

The company shall ensure that cyber incidents are reported to it by the service provider without undue delay, so that an incident is reported by the company to the RBI within six hours of detection by the service provider.

The Company shall ensure that any cyber security incident, data breach, system compromise, or operational incident detected by the service provider or its subcontractors is reported immediately to PFSPL, enabling:

- Reporting to CERT-In within six (6) hours of detection; and
- Reporting to the RBI without undue delay, as per regulatory directions.

This obligation shall be contractually binding.

B. Risks posed to the Company by Outsourcing all or part of its Activities and Evaluation of Risk:

The key risks in outsourcing that need to be evaluated are: -

a. Reputation Risk – Poor service from the service provider, its customer interaction not being consistent with the overall standards of the Company.
b. Compliance Risk – Privacy, consumer and prudential laws not adequately complied with.
c. Operational Risk – Arising due to technology failure, fraud, error, inadequate financial capacity to fulfil obligations and/or provide remedies.
d. Legal Risk – includes but is not limited to exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as private settlements due to omissions and commissions of the service provider.
e. Country Risk – Due to political, social or legal climate creating added risk.
f. Contractual Risk – arising from whether or not the Company has the ability to enforce the contract.
g. Concentration and Systemic Risk – Due to lack of control of individual Company over a service provider, more so when overall banking industry has considerable exposure to one service provider.
h. Third-Party Risk: Risks from sub-contractors or other third parties involved in the outsourced services shall be assessed, and appropriate controls shall be put in place to manage these risks.
i. Dependency Risk: Over-reliance on a single service provider can increase business vulnerability. Diversification of service providers or contingency arrangements shall be considered to minimize dependency.
j. Data Security and Privacy Risk: Outsourced IT services may expose sensitive data to third parties. Adequate measures, such as encryption and strict data protection protocols, shall be in place to safeguard information.

C. Risk Assessment and Due Diligence

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

D. Risk Management and Compliance

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

E. Contractual Framework

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

F. Confidentiality and Security of Information

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

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

9. Outsourcing Process

A. Service Provider Evaluation

The directions regarding service provider evaluation as applicable to outsourcing of financial services shall apply ***(Refer Policy on Outsourcing of Financial Services)*** , mutatis mutandis, to outsourcing of IT services, with the following additional considerations:

i. technology, infrastructural stability, data backup arrangements, and disaster recovery plan;
ii. conflict of interest, if any;
iii. capability to identify, and segregate NBFC's data;
iv. capability to comply with the regulatory and legal requirements of the outsourcing arrangement;
v. information / cyber security risk assessment;
vi. ensuring that appropriate controls, assurance requirements, and possible contractual arrangements are in place to ensure data protection and NBFC's access to the data which is processed, managed or stored by the service provider;
vii. ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and
viii. ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection, and confidentiality.

The company shall adopt a risk-based approach in conducting such due diligence activities.

B. Outsourcing Agreement

- The company shall ensure that its rights and obligations and those of each service provider are clearly defined and set out in a legally binding written agreement.
- The provisions of the agreement shall appropriately reckon the criticality of the outsourced task to the business of the NBFC, the associated risks and the strategies for mitigating or managing them.
- The terms and conditions governing the contract shall be meticulously defined and vetted by PFSPL's legal counsel to ascertain their legal effect and enforceability.

The agreement shall, at a minimum, include the following aspects, as applicable to the scope of Outsourcing of IT Services:

a) Comprehensive details regarding the activity being outsourced, including appropriate service and performance standards, applicable to both the primary service provider and any subcontractors.
b) Provisions ensuring effective access by PFSPL to all relevant data, books, records, information, logs, alerts, and business premises pertinent to the outsourced activity maintained by the service provider.
c) Regular monitoring and assessment protocols for the service provider by PFSPL to facilitate continuous risk management and enable immediate corrective actions when necessary.

d) Specification of material adverse events including but not limited to data breaches, denial of service, service unavailability and incidents that shall be reported to PSFPL, allowing for prompt risk mitigation measures and compliance with statutory and regulatory guidelines. The incident reporting should be in line with CERT-IN and RBI.
e) Assurance of compliance with the provisions of the Information Technology Act, 2000, and other applicable legal requirements and standards to safeguard customer data.
f) Clear definitions of deliverables, including Service Level Agreements (SLAs) formalizing performance criteria to measure service quality and quantity.
g) Clauses stipulating that data storage, as applicable to the concerned PSFPL, must occur exclusively within India in accordance with extant regulatory requirements.
h) Obligations for the service provider to furnish details regarding the data related to PSFPL and its customers that are captured, processed, and stored.
i) Specification of the types of data/information that the service provider (vendor) is permitted to share with PFSPL's customers and/or any other parties.
j) Clearly defined resolution processes, events of default, indemnities, remedies, and recourse available to the respective parties.
k) Development of contingency plans to ensure business continuity, including testing requirements.
l) PSFPL's right to conduct audits of the service provider (including its subcontractors) by its internal or external auditors or by agents appointed on its behalf. PFSPL shall also retain the right to obtain copies of any audit or review reports related to the services performed for PSFPL.
m) PSFPL's right to seek information from the service provider regarding any third parties engaged within the supply chain.
n) Recognition of the authority of regulators, including the RBI, to perform inspections of the service provider and any of its subcontractors. Clauses shall allow the RBI or its authorized representatives to access PSFPL 's IT infrastructure, applications, data, documents, and other pertinent information handled by the service provider and/or its subcontractors concerning the outsourcing arrangement.
o) Inclusion of clauses that hold the service provider contractually liable for the performance and risk management practices of its subcontractors.
p) Obligations imposed on the service provider to adhere to directions issued by the RBI related to the outsourced activities, reflected through specific contractual terms and conditions.
q) Clauses requiring prior approval or consent from PSFPL for the use of subcontractors by the service provider for any part of the outsourced activity.
r) Clearly defined termination rights for PSFPL, including the ability to transfer the IT outsourcing arrangement to another service provider, if necessary or desirable.
s) The service provider's obligation to cooperate with relevant authorities in the event of the NBFC's insolvency or resolution.
t) Provisions to classify skilled resources of the service provider who provide core services as "essential personnel," ensuring that a limited number of staff, along with back-up arrangements, are available to operate critical functions on-site during exigencies (including pandemic situations).

u) Clauses requiring suitable back-to-back arrangements between service providers and original equipment manufacturers (OEMs).
v) Clauses necessitating the establishment of non-disclosure agreements concerning any information retained by the service provider.

C. Inventory of Outsourced Services

The company shall create an inventory of IT services outsourced to service providers (including key entities involved in their supply chains). Further, the NBFC shall map its dependency on third parties and periodically evaluate the information received from the service providers.

D. [For Business Continuity Plan & Disaster Recovery Plan Refer IT IS Policy]

E. Exit Strategy

- PSFPL's shall incorporate a well-defined exit strategy for all outsourced IT activities and IT-enabled services, ensuring seamless business continuity during and after the termination of services. This exit strategy shall address various exit scenarios, specifying the minimum time required for the orderly transition or cessation of services.
- The PFSPL shall ensure that the agreement with the service provider has necessary clauses on the safe removal/destruction of data, hardware, and all records (digital and physical), as applicable. The service provider shall be legally bound to ensure the integrity and confidentiality of PFSPL's data throughout the transition process.
- The service provider shall be legally obliged to cooperate fully with both the PFSPL 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.
- Data privacy and security are critical. The Exit Mechanism shall consider provision for:
    - The Service Provider shall transfer all data belonging to the PFSPL, including any customer information.
    - An acceptable method for the Service Provider to destroy and remove the PFSPL's proprietary information; and
    - The Service Provider shall destroy and remove sensitive information from all media. The Service Provider shall ensure no information is disclosed to other individuals or other entities.
- The PFSPL shall require the service provider to preserve documents as required by law and take suitable steps to ensure that PFSPL'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.
- PFSPL shall ensure that the exit strategy is tested periodically to validate its effectiveness in maintaining business continuity during unforeseen events.
- PFSPL ensures the necessary steps to be taken to retain operational control and safeguard critical IT services during the transition.

Roles and responsibilities during the transition

- The respective technology units shall also ensure alternative arrangements like switching to another service provider or internalizing the service.

- The respective business unit teams shall monitor the exit strategy during actual transition to ensure safe disposal or destruction of data, hardware, and records by the service provider.
- The respective technology team shall ensure operational readiness for service continuity, procedures for secure data transfer, and arrangements for new services if a new provider is engaged.
- The compliance team shall undertake a legal review to ensure all regulatory and contractual obligations are met.

F. Termination

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.

10. Specific Outsourcing Arrangements

A. Cloud Computing Services Management

PFSPL has established a separate "**Cloud Adoption Policy**". This policy provides detailed procedures and standards specific to cloud service engagements, ensuring alignment with PFSPL's business requirements, legal obligations, and regulatory expectations.

B. Security Operations Centre

Cyber SoC covering critical applications, shall be put in place taking into account, proactive monitoring and management capabilities with sophisticated tools for detection, response, backed by data for sound analytics.

Designated team is responsible for reviewing the SOC alerts on a daily basis and the outcome of the SOC exercise shall be presented to the Senior Management at an appropriate frequency.

11. Monitoring and Control of Outsourced Activities

i. The Company shall have in place a management structure to monitor and control its outsourced activities and shall ensure that outsourcing agreements with its service provider contain provisions to address the same.

ii. The Company shall maintain a central record of all material outsourcing of financial services for review by its Board and Senior Management. The records shall be updated promptly, and half yearly reviews shall be placed before the Board or Risk Management Committee.

iii. Regular audits, by either the internal auditors or external auditors of an NBFC shall assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the NBFC's compliance with its risk management framework, and the requirements of these Directions.

iv. The Company, at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing obligations. Such due diligence reviews, which shall be based on all available information about the service provider, shall highlight any deterioration or breach in performance standards,

confidentiality, and security, and in operational resilience or business continuity preparedness.

12. Redressal of Grievances related to Outsourced Services

The Nodal officer of the company will act as Grievance Redressal officer for the purpose of outsourced services. The designated officer shall ensure that genuine grievances of the Customers are forwarded to concerned department and redressed promptly without any delay. The grievance redressal procedure of the Company and the time frame fixed for responding to the complaints shall be placed on the Company's website.

13. Review

The policy shall be reviewed at regular intervals, or earlier if considered necessary by the Management or the Board of Directors, or in the event of any change in applicable regulatory requirements.

Annexure- A

Due Diligence Checklist

Sr. No.	Details	
A	Date	
B	Form Applicable for: Financial outsourcing	
C	Name and designation of the person authorized for compliance with due diligence:	
E	Vendor Details 1. Name as per registration proof: 2. Registration number, Date and validity of registration 3. PAN number 4. Educational qualifications of applicant 5. Date of birth of applicant 6. Father's name of applicant 7. Legal constitution (Proprietorship/ Ind/ Company/ etc..) 8. Ultimate beneficial ownership details (shareholding exceeds 10%): share holder names and contact	

	no. 9. Name of the Parent Company, if any: 10. Registered Address: 11. Communication Address: 12. Name of the contact person: 13. Email ID: 14. Contact No: 15. Website, if any:	

F	**Service Description:**
	1. Description of the service offered:
	2. Applications/ Systems used by the vendor for providing the services, If Applicable:
	3. Details of the progress reports provided by the vendor:
	4. Mode of dataflow (offline/online/through API integration):
	5. Pricing model of the vendor (Flat per return fee or tired pricing with volume discount):
G	**Experience of the Vendor:**
	1. Experience of the vendor in providing current services:
	2. Details of geographical area covered under the services provided by the vendor, if applicable (Pan India/ Region/ State/ City):
H	**Selection of the Vendor:**
	1. Number of the vendors considered before selecting the current vendor. Please attach service evaluation reports of multiple vendors.
	2. The criteria used by the organization to determine a suitable vendor (i.e. Price, Reputation, Location, Quality of Service, etc.)

I	**Background check of Vendor and employee of Vendor:**
	1. What is the current process in place by the vendor for background verification of its employees? Please provide the policy document for background check of employees.
	Document Submitted? ☐ Yes ☐ No
	2. Has any reference checks or Industry referece obtained before selecting the vendor? If yes, Please provide the reference details and feedback
	Document Submitted? ☐ Yes ☐ No
	3. Has any physical verification visit has been carried out at the business location of the proposed vendor? If yes provide the FI Report
	Document Submitted? ☐ Yes ☐ No
J	**Operational Due-Deligence:**
	1. Details of scope of the work. Pleaes provide the sow.
	Document Submitted? ☐ Yes ☐ No
	2. SLA defined/ included in the agreement to ensure the company's expectations are defined? Please provide the list of the SLAs. Can these SLA clauses help in arriving at KPIs to fulfil the company's expectations in mitigation of the operational risk? Please provide the list of the KPIs.
	Document Submitted? ☐ Yes ☐ No
	3. What are the cost involved in bringing the outsourcing service to inhouse along with the resource and time needed in case of exigencies? Please provide detailed cost Benefit analysis.
	Document Submitted? ☐ Yes ☐ No
	4. Is the vendor dominant vendor/ sole vendor when it comes to city?
	☐Yes ☐ No
	5. Is the vendor dominant vendor/ sole vendor when it comes to State?
	☐Yes ☐No
	6. Is the vendor an outsourcing agent for mulitple financial institutions? What safeguarde are put in place by the vendor to avoid commingling of customer information, records and assets?
	7. Can the vendor isolate and clearly identify the customer information, records and assets to protect the confidentiality of the information?
	☐Yes ☐ No
	8. How does vendor ensure inhouse data of the organization and customer are secured? Is any training given to emplyees of vendor regarding the data security? Please provide the Data Security Policy of the vendor.

	Document Submitted? ☐ Yes ☐ No
	9. What mechanism is in place to ensure reporting of all security breaches and controls of the service provider to organization?
	10. What is the machnisam for raising complaints with the vendor? Please provide the Escaltion Matrix.
	Document Submitted? ☐ Yes ☐ No
K	**Financial Health check of the Vendor**
	1. Provide the Financial statement of the vendor for the past 3 years
	2. W.e.f 01-0402022, as per section 206AA of the income-tax ACT, 1961, if PAN is not linked to Aadhar number, it is treated as invalid, and TDS will be deducted @20% for individuals. Is PAN linked with Aadhar? Document Submitted? ☐ Yes ☐ No
L	**Compliance:**
	1. Please provide list of the regulatory licenses held by the vendor, pertaining to the services being availed.
	Document Submitted? ☐ Yes ☐ No
	2. Would the vendor's service require authorization, approval or other direct action with the government authority for the due execution and perfomance? If so, Pleaes state the requirements.
	3. Please provide the shareholding of the vendor
	Document Submitted? ☐ Yes ☐ No
	4. Does vendor have internal audit or similar mechanism to assess the perfomance?
	☐ Yes ☐ No
	5. Does vendor have BCP policy in place? If so, Please provide the BCP policy of the vendor. What is the frequency of BCP/DR testing and location of DR Sites.
	Document Submitted? ☐ Yes ☐ No
	What mechanism is in place to periodicly monitor the testing of BCP and recovery plan of the service vendor? Is there a need to conduct joint testing and recovery with the service provider?
	6. Does the vendor or its partners, partner, subsidiary or associate entity or any other entity in which vendor or its partner has significant influence or control or whose trademark/brand is used by vendor provide any kind of service to PFSPL?

	☐Yes ☐ No
	7. Does either vendor or its partners, parents, subsidary or associate entity or any other entity is politically exposed? If any please disclose complete details
	☐Yes ☐ No
	8. Does the service provider have adequate manpower to provide the services agreed upon
	☐Yes ☐No
	9. Does the service provided company is owned or controlled by PFSPL's any director, or key managerial personnnel, or approver of the outsourcing arrangement or any of their relatives?
	☐Yes ☐No
	10. Does the vendor have required infrastructure such as CCTV, fire alarm, fire extinguishers etc. to safeguard documents or other assetsd of PFSPL?
	☐Yes ☐No
	- Added in financial information above
M	**For Outsourcing to Tech Enabled Vendors**
	Material outsourcing to tech enabled vendors require additional compliance to the below criteria.Tech enable vendors are vendors from whom we avail services which require integration with our in-house IT systems or wherein we use the interface of these vendors to fulfill our requirements.
	1. Does vendor have BCP policy in place? If so, please provide the BCP policy of the vendor. What is the frequency of BCP/DR testing and location of DR Sites.
	Document Submitted? ☐ Yes ☐ No
	2. What mechanism is in place to periodically monitor the testing of BCP and recovery plan of the service vendor? Is there a need to conduct joint testing and recovery with the service provider?
	3. What mechanism is in place to check the reliability of safeguard put in place by vendor to protect the data of the organization? Is Vulnerability Assessment and Penetration Testing carried out by the vendor? What is the frequency of such tests? Please provide the latest Vulnerability Assessment and Penetration Testing report of the vendor.
	Document Submitted? ☐ Yes ☐ No
	4. What mechanism is in place to store the data of the organization? Please provide the Record Retention policy of the Vendor.

	Document Submitted? ☐ Yes ☐ No
N	**Offshore Outsourcing**
	1. If the outsourced vendor is in foreign country, What are the country, social and political risks related to vendor and the outsourcing activiy?
	2. Is adequate monitoring mechanisam is in place to monitor the Govt policies, political, social, economic, and legal conditions in the foregin country where service provider is loacted both at the initial risk assessement and on a continuous basis? Please provide the mechanism used for the ongoing monitoring and the frequency of the monitoring
	Document Submitted? ☐ Yes ☐ No

For LSPs:	
1	Does your app collect data on a need-to-need basis and ask for borrower's consent before collecting it? Please share the evidence supporting the response
	☐Yes ☐ No
2	Do you have audit trails of data/consent collection if in case those need to be audited? Please share the evidence Audit trails of data collection
	☐Yes ☐No
3	Can you confirm if application does not access other mobile resources like camera, call logs, contact list etc or it is only a one time access for on-boarding?
	☐Yes ☐No
4	If yes then do does application ask for explicit consent to use of specific Data for specific purposes? Pls share the evidence from the app/website
	☐Yes ☐ No
5	Does you application provide revoke consent granted previously to collect the data in the app and delete/forget the data in the app?Pls share the evidence supporting the response
	☐Yes ☐ No
6	Do you have Comprehensive data privacy policy? Does it comply with associated laws, regulations and RBI guidelines?
	☐Yes ☐No
7	To access personal information from borrowers do you have publicly disclosed comprehensive policy on website/application? Pls share evidence of public privacy policy disclosed on app/Website
	☐Yes ☐ No
8	Does your application talk about purpose of obtaining borrower's consent at each stage while collecting data? Pls share evidence from app/Website
	☐Yes ☐ No
9	Do you use third party who collects borrower's data for you? Do you mention details of third party in privacy policy? Do you take explict consent before sharing data personal infromation with third party? Evidence of consent for sharing data with third party
	☐Yes ☐ No

10	Does your app/Website talks about type of data to be held. Data retention time, restriction on the use of data. Data destruction protocol, handling of security breach? This should be disclosed on website and Apps all the time. Evidence on Disclosure from App/Website
	☐Yes ☐No
11	No bio-metric should be collected/stored? Can you confirm if that is not happaning with your app/website?
	☐Yes ☐No
12	Does your app/website have links available for Pahal's website from where borrower can get further infromation about loan product, the lender, particulars of customer care, privacy policies etc. Evidence from Website/App
	☐Yes ☐No
13	Please confirm if data is getting stored in servers located in india while ensuring compliance with statutory and regulatory requirement. Evidence of data storage happens in India
	☐Yes ☐No
14	Do you perform security assessments on your applications to check proper authentication, input validation, clear access rules, measures to insure protection of sensitive data etc. Evidence of App Security assessment done on app/website covering mentioned points
	☐Yes ☐ No
15	Do you keep audit log of every action that users perform with their IP address and device information? Evidence on Log collection
	☐Yes ☐No
16	Do you have monitoring set up for transactions being done through digital lending apps/websites? Evidence of transaction monitoring done through app/website
	☐Yes ☐ No
17	Does your app/website provide multi-step approval logic for critical activites perfomed in your app/website. Evidence of multistep approval from app/website for critical activites
	☐Yes ☐ No

IT Requisition List (As applicable)

Sr No	Artefacts
1	Account Lockout Policy
2	ISO Certifications
3	Password Policy
4	Access Control Policy
5	Physical Access policy
6	DLP Policy
7	Privilege Access Management Policy
8	Asset Management Policy

9	Asset Inventory
10	Information Classification Policy
11	IT Disaster Recovery/ Business Continuity Plan/Procedures
12	BCP/ DR Drill Reports
13	DR Site details
14	Backup and Recovery Policy
15	Data Retention Policy
16	Change Management Policy and Procedure
17	Process for handling emergency changes
18	Patch Management Policy and Procedures
19	Server & Endpoint Hardening Document & report
20	DL SAR Report
21	Acceptable Usage Policy
22	Incident Response Plan
23	Incident Management Policy
24	Logging and Monitoring Policy and Procedures
25	Information Security Policy
26	Risk Management Policy
27	Code of Conduct
28	Risk Register
29	Anti Malware/Anti-Virus Policy
30	Fraud Policy
31	Data Handling Policy and Procedures
32	Media disposal Policy
33	Network Architecture Diagram (HLD and LLD)
34	Encryption Decryption Policy
35	Logs Review Report

36	Application Security Testing Report
37	VA/PT Reports
38	Mock Fire Drill Report
39	HR Policy
41	NDA Signed with Employees

Recommended for onboarding:

SL No.	Confirmation by PFSL:	Yes/ No
1	Has the service provider Background been assessed as per the checklist?	
2	Have you checked and verified the documents	

Completed By:	
Signature of Functional Head:	
Date of Submission:	