SERVICE LEVEL AGREEMENT

AGREEMENT FOR _____

BETWEEN

STATE BANK OF INDIA, _____

AND

_____

Date of Commencement : _____

Date of Expiry :_____

Table of Contents

This agreement ("Agreement") is made at_____ (Place) on this _____day of _____ 20__.

BETWEEN

State Bank of India, constituted under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Madame Cama Road, Nariman Point, Mumbai-21 and its Global IT Centre at Sector-11, CBD Belapur, Navi Mumbai- 400614 through its _____ Department, hereinafter referred to as "**the Bank**" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of First Part:

AND

_____ a private/public limited company/LLP/Firm incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having its registered office at _____ hereinafter referred to as "**Service Provider/ Vendor**", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS

(i) "The Bank" is carrying on business in banking in India and overseas and desirous to avail services for **Techno Legal Agency**

(ii) _____;

(iii) _____; and

(iv) Service Provider is in the business of providing **Techno Legal Services** and has agreed to provide the services as may be required by the Bank mentioned in the Request of Proposal (RFP) No. _____ dated _____issued by the Bank along with its clarifications/ corrigenda, referred hereinafter as a "RFP" and as per the statement of work defined in the **Annexure- A** of this document same shall be part of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for other valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree to the following terms and conditions hereinafter contained:-

1. DEFINITIONS & INTERPRETATION

1.1 Definition

Certain terms used in this Agreement are defined hereunder. Other terms used in this Agreement are defined where they are used and have the meanings there indicated. Unless otherwise specifically defined, those terms, acronyms and phrases in this Agreement that are utilized in the information technology services industry or other pertinent business context shall be interpreted in accordance with their generally understood meaning in such industry or business context, unless the context otherwise requires/mentions, the following definitions shall apply:

1.1.1 **'The Bank'** shall mean the State Bank of India (including domestic branches and foreign offices), Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures:

1.1.2 "**Confidential Information**" shall have the meaning set forth in Clause 16.

1.1.3 **"Bidder"** means an eligible entity/firm submitting the Bid in response to this RFP.

1.1.4 **"Bid"** means the written reply or submission of response to this RFP.

1.1.5 **"Day"** means English calendar day.

1.1.6 **"The Contract"** means the agreement entered into between the Bank and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.1.7 "**Deficiencies"** shall mean defects arising from non-conformity with the mutually agreed specifications and/or failure or non-conformity in the Scope of the Services.

1.1.8 **"Intellectual Property Rights"** shall mean, on a worldwide basis, any and all: (a) rights associated with works of authorship, including copyrights &moral rights; (b) Trade Marks; (c) trade secret rights; (d) patents, designs, algorithms and other industrial property rights; (e) other intellectual and industrial property rights of every kind and nature, however designated, whether arising by operation of law, contract, license or otherwise; and (f) registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

1.1.9 **"Request for Proposal (RFP)"** shall mean RFP NO. _____ dated _____ along with its clarifications/ corrigenda issued by the Bank time to time.

1.1.10 **'Services'** shall mean and include all the services offered by Service Provider under this agreement more particularly described in Statement of Work

1.1.11 **"Service Provider"** is the successful Bidder found eligible as per eligibility criteria set out in this RFP, whose technical Bid and commercial bid has been accepted and who has emerged as the Successful Bidder as per the selection criteria set out in the RFP and to whom notification of award has been given by Bank.

1.2 **"Deliverables / Work Product"** shall mean all work product generated by Service Provider solely or jointly with others in the performance of the Services, including, but not limited to, any and all information, notes, reports, material, drawings, records, diagrams, formulae, processes, technology, firmware, software, know-how, designs, ideas, discoveries, inventions, improvements, copyrights, trademarks and trade secrets.

1.3 **Interpretations:**

1.2.1 Reference to a person includes any individual, firm, body corporate, association (whether incorporated or not) and authority or agency (whether government, semi government or local).

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

1.2.4 The provisions of the contents table, headings, clause numbers, italics, bold print and underlining is for ease of reference only and shall not affect the interpretation of this Agreement.

1.2.5 The Schedules, Annexures and Appendices to this Agreement shall form part of this Agreement.

1.2.6 A reference to any documents or agreements (and, where applicable, any of their respective provisions) means those documents or agreements as amended, supplemented or replaced from time to time provided they are amended, supplemented or replaced in the manner envisaged in the relevant documents or agreements.

1.2.7 A reference to any statute, regulation, rule or other legislative provision includes any amendment to the statutory modification or re-enactment or, legislative provisions substituted for, and any statutory instrument issued under that statute, regulation, rule or other legislative provision.

1.2.8 Any agreement, notice, consent, approval, disclosure or communication under or pursuant to this Agreement is to be in writing.

1.2.9 The terms not defined in this agreement shall be given the same meaning as given to them in the RFP. If no such meaning is given technical words shall be understood in technical sense in accordance with the industrial practices.

1.4 **Commencement, Term & Change in Terms**

1.3.1 This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from _____ (Effective Date).

1.3.2 This Agreement shall be in force for a period of _____ year(s) from Effective Date, unless terminated by the Bank by notice in writing in accordance with the termination clauses of this Agreement.

1.3.3 The Bank shall have the right at its discretion to renew this Agreement in writing, for a further term of _____ years on the mutually agreed terms & conditions.

2. STATEMENT OF WORK

2.1 The scope and nature of the work which Service Provider has to provide to the Bank (Services) is detailed in the Statement of Work in **Annexure-A.**

2.2 Time shall be the essence of this Agreement. The Service Provider shall therefore fully abide by various time limits as prescribed for different assignments and the performance of the Service Provider shall be judged as per the adherence to such quality and time parameters as laid down for the respective work.

2.3 **Risk Management**

The Service Provider shall identify and document the risk in delivering the services. (Service Provider) shall identify the methodology to monitor and prevent the risk, and shall also document the steps taken to manage the impact of the risks.

2.4 **Service Request**

Service Provider shall dispense the services to the bank's satisfaction in a time bound manner as per the TAT defined under SLA.

2.5 **Service Management Technologies**

The Service Provider must use the state-of-the-art technology for monitoring, detection, taking down of Content / Fake sites / Apps / profiles etc. and initiating legal action or for any other activities as required as per the statement of work and also keep it self updated with dynamic environment of Techno Legal space.

2.6 **Service Complaints**

The complaint shall be acknowledged by the Service Provider in 24 Working Hours. In case of re-occurrence of the service complaints, despite repeated escalations the penal provisions may be triggered as per clause in the SLA , as decided by the Bank.

3. COMPLIANCE OF INFORMATION SECURITY (IS) POLICY

3.1 The Service Provider should comply with Bank's Information Security (IS) policy in key concern areas relevant to the Services provided under this Agreement and as notified by the Bank from time to time. The key areas include, but are not limited to, the following:

a) Confidentiality, privacy and security for data and application gained as a result of having access to the Banks internal system, software and other administration should be maintained.

b) Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to the selected agency.

c) Physical and logical separation from other customers of the selected Service Provider.

d) Incident response and reporting procedures.

e) Password Policy of the Bank.

f) Data Encryption/Protection requirement of the Bank.

g) Any other requirement as decided by the Bank in this regard.

4. FEES /COMPENSATION

4.1 **Professional fees**

Service Provider shall be paid fees and charges in the manner detailed in here under, the same shall be subject to deduction of income tax thereon wherever required under the

provisions of the Income Tax Act by the Bank. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations for the time being in force. Nothing in the Agreement shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Agreement.

Sl. No.	**Job List**	**INR (per month)**
1.	Monitoring and identification of malicious, misleading, defamatory, fraudulent, unauthorised or reputation-damaging content, brand guideline violation or brand / logo infringement content related to the bank including fake profiles / handles / channels / pages /websites/Apps/phishing sites/ deep fakes etc on digital and social media channels relevant to the Bank as per SOW	
2.	Taking down of identified content, fake profiles / handles / channels / pages /websites/Apps/phishing sites, deep fakes etc from digital and social media space as per SOW	
3.	Initiation of Legal action including serving Defamation Notices as and when advised by the bank	Actual Cost basis
4.	Representing Bank in Competent Courts for purposes defined in Statement of Work	Actual Cost basis
	TOTAL	

4.2 All duties and taxes (excluding _____ or any other tax imposed by the Government in lieu of same), if any, which may be levied, shall be borne by Service Provider and Bank shall not be liable for the same. All expenses, stamp duty and other charges/ expenses in connection with execution of this Agreement shall be borne by Service Provider. _____ or any other tax imposed by the Government in lieu of same shall be borne by the Bank on actual upon production of original receipt wherever required.

4.3 Service Provider shall provide a clear description quantifying the service element in the invoices generated by them.

4.4 The service provider shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by the service provider shall include all such taxes in the contract price.

4.5 **Payments**

4.5.1 The Bank will pay properly submitted valid invoices within reasonable period but not exceeding 45 (Forty-Five) days after its receipt thereof. All payments shall be made in Indian Rupees.

4.5.2 The Bank may withhold payment of any product/services that it disputes in good faith and may set-off penalty amount or any other amount which Service Provider owes to the Bank against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, the Bank shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidences, if any, within 21 (twenty one) days. Penalty or damages, if any, recoverable from Service Provider shall be recovered by the Bank through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, the Bank shall have right to withhold the payment or set-off penal amount from current invoices.

4.5.3 The Bank has the sole discretion to pay only for the services they undertake and may choose to discontinue services for any one or all jobs listed in the table above, as mutually discussed and agreed between the Parties. However, this clause shall not apply to those Services that have already been rendered by the Service Provider and payments for the same must be duly made by the Bank based on the agreed timelines, terms and conditions detailed under this Agreement (Payments as per SLA to be made in accordance with the utilisation of services as per individual line items listed above).

4.5.4 The Service Provider will submit the invoices complete in all respects, before 5th of every month for necessary payment of the retainership fee. The invoice should be supported with the list of work initiated /complete during the month. There will be no additional remuneration towards the delayed payments.

4.5.5 The Service Provider will submit all supporting documents and bills, where relevant. to avoid double taxation, SBI will directly pay any of the Service Provider's vendors e.g. Legal and technical experts, advocates etc. if required.

4.5.6 A reconciliation sheet pertaining to the bills will be submitted every month as well as supporting documents evidencing work/activities performed during a month.

4.5.7 The Tax component shall be payable as applicable and as per actuals.

5. BANK GUARANTEEN AND PENALTIES

5.1 Service Provider shall furnish performance security in the form of Bank Guarantee for an amount of _____valid for a period of _____ from a Scheduled Commercial Bank other than State Bank of India in a format provided/ approved by the Bank.

5.2 The Bank Guarantee is required to protect the interest of the Bank against the risk of non-performance of Service Provider in respect of successful implementation of the project and/or failing to perform / fulfil its commitments / obligations in respect of providing Services as mentioned in this Agreement; or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

5.3 If at any time during performance of the contract, Service Provider shall encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable, after receipt of Service Provider's notice, the Bank shall evaluate the situation and may at its discretion extend Service Provider's time for performance, in which case the extension shall be ratified by the Parties by amendment of the Agreement.

5.4 Performance of the obligations under the Agreement shall be made by Service Provider in accordance with the time schedule finalized in this Agreement.

5.5 The Service Provider shall be liable to pay penalty as per Clause 27 of RFP in respect of any delay beyond the permitted period in providing the Services and which are solely attributable to the Service Provider. No penalty shall be levied in case of delay(s) in deliverables or performance of the contract for the reasons not attributable to the Service Provider.

5.6 No penalty shall be levied in case of delay(s) in deliverables or performance of the contract for the reasons solely and directly attributable to the Bank. On reaching the maximum of penalties specified the Bank reserves the right to terminate the contract.

6. LIABILITIES/OBLIGATION

6.1 **The Bank's Duties /Responsibility (if any)**

(i) Processing and authorising invoices

6.2 **Service Provider Duties**

(i) Service Delivery responsibilities

(a) To adhere to the service levels documented in this Agreement.

(b) Service Provider shall ensure to filter all phishing / spamming / overflow attacks in order to ensure availability and integrity on continuous basis.

(c) Service Provider shall ensure that Service Provider's personnel and its sub-contractors (if allowed) will abide by all reasonable directives issued by the Bank, including those set forth in the Bank's then-current standards, policies and procedures (to the extent applicable), all on-site rules of behaviour, work schedules, security procedures and other standards, policies and procedures as established by the Bank from time to time.

(d) Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable laws, concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

(e) Service Provider shall report the incidents, including cyber incidents and those resulting in disruption of service and data loss/ leakage immediately

(f) The Service Provider shall execute Data Processing Agreement on the format attached as Appendix-A-1 to this RFP

(g) The service provider shall comply with all applicable laws, regulations, and regulatory directions issued by the Reserve Bank of India (RBI) and other competent authorities in relation to the activities under SOW.

(h) The Service Provider agrees to comply with the obligations arising out of the Digital Personal Data Protection Act, 2023, as and when made effective. Any processing of Personal Data by the Service Providers in the performance of this Agreement shall be in compliance with the above Act thereafter. The Service Provider shall also procure that any sub-contractor *(if allowed)* engaged by it shall act in compliance with the above Act, to the extent applicable. The Service Provider understands and agrees that this agreement may have to be modified in a time bound manner to ensure that the provisions contained herein are in compliance with the above Act.

(i) The service Provider shall identify, document, and maintain a list of skilled resources (key personnel, technical specialist) who provide core services under this Agreement. These persons shall be designated as "Essential Personnel". The service provider shall ensure: (a) back-up arrangements are in place for such

essential personnel. (b) The service provider shall maintain knowledge transfer, cross-training, and succession plans to ensure continuity in case of absence, leave, incapacity, or other unavailability of any essential personnel. In situations of exigency (including but not limited to pandemics, natural disasters, infrastructure disruptions, regulatory restrictions), the service provider shall ensure that a limited number of essential personnel are able to work on -site at locations during exigencies.

(j) The service provider shall not erase, delete, purge, revoke access to, or otherwise make unavailable any data belongings to the bank or its customers, whether stored, processed, or transmitted as part of services, without the Bank's prior written approval. All actions relating to data modification, erasure, or destructions shall be carried out only under written instruction of the Bank and in accordance with (a) the bank's data retention and destruction policies; (b) regulatory directions issued by the Reserve Bank of India (RBI) or any competent authority.

(k) Service provider shall ensure that storage of data only in India as per the extant regulatory requirements

(l) Service Provider agrees to comply with the guidelines contained in the Bank's IT Outsourcing Policy / IT Procurement Policy or any other relevant policy (ies) of the Bank, including any amendment thereto, along with compliance to all the Laws of Land and Statutory/Regulatory rules and regulations in force or as and when enacted during the validity period of the contract.

(m) The service provider shall ensure adherence to Prevention of Money Laundering Act, 2002 and other applicable AML/CFT laws. The service provider shall provide, as and when required by the Bank, copies of AML policy and other related documents.

(ii) Security Responsibility

a. To maintain the confidentiality of the Bank's resources and other intellectual property rights.

7. REPRESENTATIONS & WARRANTIES

7.1 Each of the Parties represents and warrants in relation to itself to the other that:

7.1.1 It has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement and has been fully authorized through applicable corporate process to do so.

7.1.2 The person(s) signing this Agreement on behalf of the Parties have the necessary authority and approval for execution of this document and to bind his/their respective organization for due performance as set out in this Agreement. It has all necessary statutory and regulatory permissions, approvals and permits for the running and operation of its business.

7.1.3 It has full right, title and interest in and to all software, copyrights, trade names, trademarks, service marks, logos symbols and other proprietary marks (collectively 'IPR') (including appropriate limited right of use of those owned by any of its vendors, affiliates or subcontractors) which it provides to the other Party, for use related to the Services to be provided under this Agreement.

7.1.4 It will provide such cooperation as the other Party reasonably requests in order to give full effect to the provisions of this Agreement.

7.1.5 The execution and performance of this Agreement by either of the Parties does not and shall not violate any provision of any of the existing Agreement with any of the party and any other third party.

7.1.6 Service Provider shall assume responsibility under all applicable including, Labour Laws for its employees, and also hold the Bank harmless from any direct and actual loss, expense, damage or personal injury, death and any claim for payment of compensation of its employees, salary, retirement benefits, or any other benefits asserted by an employee of the Service Provider, and/or any claim arising out of alleged infringement of intellectual property rights or other proprietary right of any third party arising out of 'Service Provider's performance of Services hereunder.

7.1.7 Each party represents and warrants that it has all requisite power and authorization to enter into and perform this Agreement and that nothing contained herein or required in the performance hereof conflict or will conflict with or give rise to a breach or default under, or permit any person or entity to terminate, any contract or instrument to which the party is bound.

7.1.8 Service Provider warrants the Bank against any license or IPR violations on its part or on the part of subcontractor, wherever permitted, in use of any technology /software /product for performing services or developing software for the Bank as part of this Agreement.

7.1.9 The Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management

practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods.

7.1.10 The Service Provide) has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services to the Bank.

7.1.11 The Service Provider shall duly intimate to the Bank immediately, the changes, if any in the constitution of the Service Provider.

7.1.12 The Services and products provided by the Service Provider to the Bank do not violate or infringe any patent, copyright, trademarks, trade secrets or other intellectual property rights of any third party.

7.1.13 The Service Provider shall ensure that all persons, employees, workers and other individuals engaged by or sub-contracted by the Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by the Service Provider unless such person is found to be suitable in such verification and the Service Provider shall retain the records of such verification and shall produce the same to the Bank as when requested.

7.2 **Additional Representation and Warranties by Service Provider**

7.2.1 Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods.

7.2.2 Service Provider has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services to the Bank.

7.2.3 Service Provider shall duly intimate to the Bank immediately, the changes, if any in the constitution of Service Provider.

7.2.4 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the services and products provided by Service Provider to the Bank do not violate or infringe any patent, copyright, trademarks, trade secrets or other intellectual property rights of any third party.

7.2.5 Service provider shall ensure that all persons, employees, workers and other individuals engaged by or sub-contracted (if allowed) by Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by Service provider unless such person is found to be suitable in such verification and Service Provider shall retain the records of such verification and shall produce the same to the Bank as and when requested.

7.2.6 Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard.

8. GENERAL INDEMNITY

8.1 Service Provider agrees and hereby keeps the Bank indemnified against all claims, actions, loss, damages,, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which the Bank may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any willful misconduct and gross negligent acts on the part of employees, agents, representatives or sub-contractors (if allowed) of Service Provider; or (iv) any misuse of data /information or deficiency in Services. Service Provider agrees to make good the loss suffered by the Bank.

8.2 Service provider further undertakes to promptly notify the bank in writing any breach of obligation of the agreement by its employees or representatives including confidentiality obligation and in such an event, the Bank will in addition to and without prejudice to any other available remedies be entitled to immediate equitable relief in a Court of competent jurisdiction to protect its interest including injunctive relief.

8.3 The Service provider shall indemnify and keep fully and effectively indemnified the Bank against any fine or penalty levied on the Bank for improper payment of tax for the reasons solely attributable to the Service provider.

8.4 The Service provider hereby undertakes the responsibility to take all possible measures, at no cost, to avoid or rectify any issues which thereby results in non-performance of software within reasonable time. The Bank shall report as far as possible all material defects to the

Service provider) without undue delay. The Service provider also undertakes to co-operate with other service providers thereby ensuring expected performance covered under statement of work.

8.5 Nothing contained in this agreement shall impair the Bank's right to claim damages without any limitation for an amount equal to the loss suffered for non-performance of software.

9. CONTINGENCY PLANS

Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other contingency plans to meet any unexpected obstruction to Service Provider or any employees or sub-contractors (if allowed) of Service Provider in rendering the Services or any part of the same under this Agreement to the Bank. Service Provider at Banks discretion shall co-operate with the Bank in case on any contingency.

10. TRANSITION REQUIREMENT

In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistances to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of Services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing vendor is found to be in breach of this obligation, they shall be liable for paying a penalty, which may be settled from the payment of invoices or bank guarantee for the contracted period. Transition & Knowledge Transfer plan . The Bank may also require the Service Provider to enter into a Transition & Knowledge Transfer Agreement.

11. LIQUIDATED DAMAGES

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this Agreement, the Bank may, without prejudice to its other

remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 1% of total Project cost for delay of each week or part thereof maximum up to 10% of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

12. RELATIONSHIP BETWEEN THE PARTIES

12.1 It is specifically agreed that Service Provider shall act as independent service provider and shall not be deemed to be the Agent of the Bank except in respect of the transactions/services which give rise to Principal - Agent relationship by express agreement between the Parties.

12.2 Neither Service Provider nor its employees, agents, representatives, Sub-Contractors shall hold out or represent as agents of the Bank.

12.3 None of the employees, representatives or agents of Service Provider shall be entitled to claim any absorption or any other claim or benefit against the Bank.

12.4 This Agreement shall not be construed as joint venture. Each Party shall be responsible for all its obligations towards its respective employees. No employee of any of the two Parties shall claim to be employee of other Party.

12.5 All the obligations towards the employee(s) of a Party on account of personal accidents while working in the premises of the other Party shall remain with the respective employer and not on the Party in whose premises the accident occurred unless such accidents occurred due to gross negligent act of the Party in whose premises the accident occurred.

12.6 For redressal of complaints of sexual harassment at workplace, Parties agree to comply with the policy framed by the Bank (including any amendment thereto) in pursuant to the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 including any amendment thereto.

13. SUB CONTRACTING

Sub-Contracting is not permitted. However, Bank may permit sub-contracting on case-to case basis at the sole discretion of the Bank.

14. INTELLECTUAL PROPERTY RIGHTS

14.1 For any technology / software / product used/supplied by Service Provider for performing Services for the Bank as part of this Agreement, Service Provider shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Service Provider.

14.2 Without the Bank's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.

14.3 Subject to below mentioned sub-clause 14.4 and 14.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

14.4 The Bank will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Service Provider shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Bank with respect to the defense and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

14.5 Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an Infringement Claim and Service Provider did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

15. INSPECTION AND AUDIT

15.1 It is agreed by and between the parties that the Bank reserves the right to audit the service Provider, annual or as applicable, by internal/external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to the Bank and Service Provider shall submit such

certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

15.2 Where any Deficiency has been observed during audit of Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, it is agreed upon by Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the Deficiencies. It is also agreed that Service Provider shall provide certification of the auditor to the Bank regarding compliance of the observations made by the auditors covering the respective risk parameters against which such Deficiencies observed.

15.3 Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/ Reserve Bank of India and/or any regulatory authority(ies). The Bank reserves the right to call for and/or retain any relevant information / audit reports on financial and security reviews with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/ data not related to Services under the Agreement (e.g. internal cost breakup etc.).

15.4 Service Provider shall grants unrestricted and effective access to a) data related to the Services; b) the relevant business premises of the Service Provider; subject to appropriate security protocols, for the purpose of effective oversight use by the Bank, their auditors, regulators and other relevant Competent Authorities, as authorised under law.

16. CONFIDENTIALITY

16.1 “Confidential Information” mean all information which is material to the business operations of either party or its affiliated companies, designated as being confidential or which, under the circumstances surrounding disclosure out to be treated as confidential, in

any form including, but not limited to, proprietary information and trade secrets, whether or not protected under any patent, copy right or other intellectual property laws, in any oral, photographic or electronic form, whether contained on computer hard disks or floppy diskettes or otherwise without any limitation whatsoever. Without prejudice to the generality of the foregoing, the Confidential Information shall include all information about the party and its customers, costing and technical data, studies, consultants reports, financial information, computer models and programs, software Code, contracts, drawings, blue prints, specifications, operating techniques, processes, models, diagrams, data sheets, reports and other information with respect to any of the foregoing matters. All and every information received by the parties and marked confidential hereto shall be assumed to be confidential information unless otherwise proved. It is further agreed that the information relating to the Bank and its customers is deemed confidential whether marked confidential or not.

16.2 All information relating to the accounts of the Bank's customers shall be confidential information, whether labeled as such or otherwise.

16.3 All information relating to the infrastructure and Applications (including designs and processes) shall be deemed to be Confidential Information whether labeled as such or not. Service Provider personnel/resources responsible for the project are expected to take care that their representatives, where necessary, have executed a Non-Disclosure Agreement similar to comply with the confidential obligations under this Agreement.

16.4 Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential Information is required by law, legal process or any order of any government authority. Service Provider in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of Banks and the banks per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law; legal process or order of a government authority.

16.5 Each party, including its personnel, shall use the Confidential Information only for the purposes of achieving objectives set out in this Agreement. Use of the Confidential Information for any other purpose shall constitute breach of trust of the same.

16.6 Each party may disclose the Confidential Information to its personnel solely for the purpose of undertaking work directly related to the Agreement. The extent of Confidential Information disclosed shall be strictly limited to what is necessary for those particular personnel to perform his/her duties in connection with the Agreement. Further each Party

shall ensure that each personnel representing the respective party agree to be bound by obligations of confidentiality no less restrictive than the terms of this Agreement.

16.7 The non-disclosure obligations herein contained shall not be applicable only under the following circumstances:

(i) Where Confidential Information comes into the public domain during or after the date of this Agreement otherwise than by disclosure by a receiving party in breach of the terms hereof.

(ii) Where any Confidential Information was disclosed after receiving the written consent of the disclosing party.

(iii) Where receiving party is requested or required by law or by any Court or governmental agency or authority to disclose any of the Confidential Information, then receiving party will provide the other Party with prompt notice of such request or requirement prior to such disclosure.

(iv) Where any Confidential Information was received by the receiving party from a third party which does not have any obligations of confidentiality to the other Party.

(v) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

16.8 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

16.9 Service Provider shall not, without the Bank's prior written consent, make use of any document or information received from the Bank except for purposes of performing the services and obligations under this Agreement.

16.10 Any document received from the Bank shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of Service Provider's performance under the Agreement.

16.11 Upon expiration or termination of the Agreement, all the Bank's proprietary documents, customized programs partially or wholly completed and associated documentation, or the Bank's materials which are directly related to any project under the Agreement shall be delivered to the Bank or at the Bank's written instruction destroyed, and no copies shall be retained by Service provider without the Bank's written consent.

16.12 The foregoing obligations (collectively referred to as "Confidentiality Obligations") set out in this Agreement shall survive the term of this Agreement and for a period of five (5) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

17. OWNERSHIP

17.1 Service Provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all intellectual property rights, copyrights. Any work made under this Agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

18. TERMINATION

18.1 The Bank may, without prejudice to any other remedy for breach of Agreement, by written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:

(i) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement, or any extension thereof granted by the Bank;

(ii) If Service Provider fails to perform any other obligation(s) under the Agreement;

(iii) Violations of any terms and conditions stipulated in the RFP;

(iv) On happening of any termination event mentioned herein above in this Agreement.

Prior to providing a written notice of termination to Service Provider under above mentioned sub-clause (i) to (iii), the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.

18.2 The Bank, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, for its convenience, provided same shall not be invoked by the Bank before completion of half of the total Contract period (including the notice period). In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

18.3 In the event the Bank terminates the Agreement in whole or in part for the breaches attributable to Service Provider, the bank may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to clause 20

Service Provider shall be liable to the Bank for any increase in costs for such similar Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

18.4 The Bank shall have a right to terminate the Agreement immediately by giving a notice in writing to Service Provider in the following eventualities:

(i) If any Receiver/Liquidator is appointed in connection with the business of Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider.

(ii) If Service Provider applies to the Court or passes a resolution for voluntary winding up of or any other creditor / person files a petition for winding up or dissolution of Service Provider.

(iii) If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors or representatives, in the reasonable opinion of the Bank tantamount to fraud or prejudicial to the interest of the Bank or its employees.

(iv) Any document, information, data or statement submitted by Service Provider in response to RFP, based on which Service Provider was considered eligible or successful, is found to be false, incorrect or misleading.

18.5 In the event of the termination of the Agreement Service Provider shall be liable and responsible to return to the Bank all records, documents, data and information including Confidential Information pertains to or relating to the Bank in its possession.

18.6 In the event of termination of the Agreement for material breach, the Bank shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations.

18.7 Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

19. DISPUTE REDRESSAL MACHANISM & GOVERNING LAW

19.1 All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement, if any, or in discharge of any obligation arising out of this Agreement

and the Contract (whether during the progress of work or after completion of such work and whether before or after the termination of the contract, abandonment or breach of the contract), shall be settled amicably. If however, the parties are not able to solve them amicably within 30 (Thirty) days after the dispute occurs, as evidenced through the first written communication from any Party notifying the other regarding the disputes, the same shall be referred to and be subject to the jurisdiction of competent Civil Courts of Mumbai only. The Civil Courts in Mumbai, Maharashtra shall have exclusive jurisdiction in this regard.

19.2 Service Provider shall continue work under the Contract during the dispute resolution proceedings unless otherwise directed by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the competent court is obtained.

19.3 In case of any change in applicable laws that has an effect on the terms of this Agreement, the Parties agree that the Agreement may be reviewed, and if deemed necessary by the Parties, make necessary amendments to the Agreement by mutual agreement in good faith, in case of disagreement obligations mentioned in this clause shall be observed.

20. POWERS TO VARY OR OMIT WORK

20.1 No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the Agreement shall be made by successful bidder except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct successful bidder to make any variation without prejudice to the Agreement. Successful bidder shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of successful Bidder , if carried out, prevent them from fulfilling any of their obligations under the Agreement, they shall notify the Bank, thereof, in writing with reasons for holding such opinion and Bank shall instruct successful bidder to make such other modified variation without prejudice to the Agreement. The finally selected bidder shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If Bank confirms their instructions successful bidder's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in cost occasioned by such variation shall be mutually agreed between the parties. In any case in which successful bidder has received instructions from the Bank as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in

the opinion of finally selected bidder, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

20.2 If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of reduction in payment to be made to finally selected bidder, before successful bidder proceeding with the change.

21. WAIVER OF RIGHTS

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this Agreement will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

22. LIMITATION OF LIABILITY

22.1 The maximum aggregate liability of Service Provider, subject to below mentioned sub-clause 22.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total Project Cost.

22.2 Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

22.3 The limitations set forth in above mentioned sub-Clause 22.1 shall not apply with respect to:

(i) claims that are the subject of indemnification pursuant to Clause 14 (infringement of third party Intellectual Property Right);

(ii) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider;

(iii) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations;

(iv) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.

For the purpose of above mentioned sub-clause 22.3(ii) “Gross Negligence” means any act or failure to act by a party which was in reckless disregard of or gross

indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.

"Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

23. FORCE MAJEURE

23.1 Notwithstanding anything else contained in the Agreement, neither Party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

23.2 For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or sub-contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

23.3 If Force Majeure situation arises, the non-performing Party shall promptly notify to the other Party in writing of such conditions and the cause(s) thereof. Unless otherwise agreed in writing, the non-performing Party shall continue to perform its obligations under the Agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

23.4 If the Force Majeure situation continues beyond 30 (thirty) days, either Party shall have the right to terminate the Agreement by giving a notice to the other Party.Neither Party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

24. NOTICES

24.1 Any notice or any other communication required to be given under this Agreement shall be in writing and may be given by delivering the same by hand or sending the same by prepaid registered mail, postage prepaid, telegram or facsimile to the relevant address set forth below or such other address as each Party may notify in writing to the other Party from time to time. Any such notice given as aforesaid shall be deemed to be served or received at the time upon delivery (if delivered by hand) or upon actual receipt (if given by postage prepaid, telegram or facsimile).

24.2 A notice shall be effective when it is delivered or on the effective date of the notice, whichever is later.

24.3 The addresses for Communications to the Parties are as under.

(a) In the case of the Bank

_____

_____

(b) In case of Service Provider

_____

_____

24.4 In case there is any change in the address of one Party, it shall be promptly communicated in writing to the other Party.

25. PENALTY CLAUSE

Performance of the services made by the Service Provider shall be in accordance with the detection guideline, time schedule, reporting & escalation norms and other terms & conditions as specified in the Contract. Any instances in failure of performing the obligation or defect, solely attributable to any act/omission by the Service Provider, in its performance may result in deduction from the retainership fee of that particular job list (as more particularly defined in Clause 4.1 of the Service Level Agreement), as penalty which a sum equivalent to 1% of the monthly retainership fees for that particular Job list or part thereof, maximum up to l0% of the monthly retainership fee for the particular job list. For avoidance of doubt, it is hereby clarified that this clause does not apply to any third-party payments including but not limited to Legal matters related spends, made by the Service Provider to third parties on behalf of the Bank and no penalty shall be levied on such amount.

The Bank shall, without prejudice to its other remedies under the contract invoke the

Performance Bank Guarantee which the Service Provider has furnished in favour of the Bank. Once the maximum is reached, SBI may consider termination of Contract pursuant to the conditions of contract and amicable discussion with the Service Provider.

ln the event SBI terminates the Contract in whole or in part, SBI may procure, upon such terms and in such manner, as it deems appropriate, services similar to those not delivered by the Service Provider. However, the Service Provider shall continue the performance of the contract to the extent not terminated.

26. GENERAL TERMS & CONDITIONS

26.1 PUBLICITY: Service Provider may make a reference of the services rendered to the Bank covered under this Agreement on Service provider's Web Site or in their sales presentations, promotional materials, business plans or news releases etc., only after prior written approval from the Bank.

26.2 SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

26.3 NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other party, or aid any third person to do so, without the specific written consent of the other party. However nothing in this clause shall affect the Bank's regular recruitments as per its recruitment policy and not targeted to the employees of Service provider.

26.4 SEVERABILITY: The invalidity or unenforceability of any provision of this Agreement shall not in any way effect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

26.5 MODIFICATION: This Agreement may not be modified or amended except in writing signed by duly authorized representatives of each party with express mention thereto of this Agreement.

26.6 ENTIRE AGREEMENT: This Agreement, including all Work orders, Exhibits, Annexures, RFP and other documents or communications incorporated herein, represents the entire agreement for the services of between the parties and supplements all prior negotiations, understandings and agreements, written or oral, relating to the subject matter herein.

26.7 PRIVITY: Neither this Agreement nor any provision hereof is intended to confer upon any person/s other than the Parties to this Agreement any rights or remedies hereunder.

26.8 EFFECTIVE DATE: This Agreement shall be effective from the date mentioned at the beginning of this Agreement.

26.9 DUE AUTHORISATION: Each of the undersigned hereby represents to the other that she/ he is authorized to enter into this Agreement and bind the respective parties to this Agreement.

26.10 COUNTERPART: This Agreement is executed in duplicate and each copy is treated as original for all legal purposes.

26.11 The ownership of all through the Service Provider will at all-time rest with SBI and the agency/copy writer/photographer/producer, etc. will have no proprietary or other rights in respect of the same. This would include full copyright for all time use of the images used in the creative and publicity material.

26.12 The Service Provider will provide all scheduled or explicitly requested data / information / reports etc as would be required and conveyed by the Bank.

26.13 The Service Provider will be responsible for copy right issues concerning usage of images, footage, text material, etc. obtained through various sources. SBI will not be a party to any disputes arising out of copyright violation by the Service Provider, unless the images or creatives are provided by the Bank to the Service Provider.

26.14 The Service Provider will be responsible for obtaining any permission that may be required for undertaking work as detailed in this Agreement and the attached SOW. SBI may assist the Service Provider in this regard, wherever possible.

26.15 The Service Provider will at no time resort to plagiarism. 'SBI' will not be a party Io any dispute arising on account of plagiarism resorted to by the Service Provider, unless the content is provided to the Service Provider by the Bank.

26.16 Fee / commission for sending legal notices / injunction orders / other legal action would be on actual cost basis however, other standard tasks as defined under SOW would be a part of retainership. There will not be any extra fee/commission for this, unless as agreed by the Parties in writing.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date and day first mentioned above.

State Bank of India	**_____Service Provider**
By:	**By:**
Name:	**Name:**
Designation:	**Designation:**
Date:	**Date:**

WITNESS:

1.	1.
2.	2.

ANNEXURE-A STATEMENT OF WORK

This Statement of Work ("SOW") dated the last date of signature below, is made pursuant to and is governed by the Services Level Agreement date: _____, effective from _____ ("SLA") entered between State Bank of India ("Client") and _____ ("Service Provider")

The parties hereby agree as follows:

1. **Effect of SOW**

1.1 Client wishes to obtain and Service Provider has agreed to provide the Services as described in this SOW in accordance with the terms of the SLA.

1.2 Any conflict between the terms and conditions of this SOW and the terms of the SLA shall be dealt with in accordance with the clauses of the SLA, subject to any express written statement in this SOW that states that a part of this SOW prevails over the SLA's Terms and Conditions.

1.3 Unless the context requires otherwise, capitalized terms undefined in this SOW will have the meaning given to them in the SLA.

2. **Services and Deliverables**

Objective of Engagement

Broad list of activities under the scope of work includes but is not limited to the following:

The Service Provider shall undertake the following activities as per the Scope of Work

- Continuously listen, monitor, analyse, and assess all digital and social media content related to the bank across various websites, social media platforms and other digital mediums like WhatsApp and Telegrams Channels and any other emerging platforms on 24 X 7 basis.
- Detect malicious, misleading, defamatory, fraudulent, unauthorised or reputation-damaging content, brand guideline violation or brand / logo infringement content related to the bank and report on 24 X 7 basis.
- Use content intelligence tools to detect such objectionable content in any form of text, video, infographics including AI generated contents and other emerging content forms as well.

- Identify fake profiles / handles / channels / pages / websites / Apps / phishing sites / Ads etc. in a time bound manner on digital and social media channels relevant to the Bank
- Identification of Deep fake / AI Generated videos featuring Bank's Logo/Brand name, Bank's Senior executives
- Identification and taking appropriate action, in coordination with the bank on comments over Social/Digital Media, related to Chairman, MDs and other senior functionaries, adversely affecting Brand image.
- Monitoring of brand rights violation across various platforms.
- Monitoring of violation of intellectual property rights (IPRs) over Digital and Social Media channels
- Initiate platform escalations for takedown actions with respect to content over digital and Social Media channels and various profiles / handles / channels / pages / websites / Apps / phishing sites / Ads etc. as advised by the Bank
- Initiate regular takedown actions related to contents / profiles / handles / channels / pages / websites / Apps / phishing sites / Ads etc. based on Brand assets / guidelines shared
- Initiate specific takedown actions related to reputation damaging contents / profiles / handles / channels / pages / websites / Apps / phishing sites / Ads etc in coordination with bank officials
- Initiate legal proceedings including FIRs, assistance in law enforcement actions, sending defamation notices, filing of defamation suits, initiating civil and criminal proceedings in eligible cases
- Act as the Bank's early-warning, enforcement, and response partner in the digital ecosystem
- Create and update strategies in line with the broad objectives of the bank
- Assisting Bank in initiating legal proceedings / defamation suits and other legal actions

A. Platforms to be Covered

The Service Provider shall monitor **24×7** content across:

- Social media platforms: Facebook, Instagram, X (Twitter), YouTube, LinkedIn, Quora and Pinterest Threads, and snapchat and any other emerging platforms in future as advised by the bank.
- Messaging & community platforms (where legally permissible): Telegram channels, public WhatsApp groups, Reddit
- News portals, websites, landing pages, forums, local media websites

Activity wise detailed Scope of Services

B. Monitoring of Digital and Social Media Platforms

The Service Provider shall monitor various digital and social media platforms advised by the bank on 24*7 basis

The Service Provider shall monitor Digital and Social Media platforms to detect

- Malicious, misleading, defamatory, fraudulent, unauthorised or reputation-damaging content, brand guideline violation or brand / logo infringement content related to the bank and report on 24 X 7 basis.
- Fake profiles / handles / channels / pages /websites/Apps/phishing sites etc. on digital and social media channels relevant to the Bank
- Deep fake / AI Generated videos featuring Bank's Logo/Brand name, Bank's Senior executives
- Misuse of Bank Name/Bank logos/Trademarks, branch visuals, screenshots of apps/websites
- Misleading Ads using Brand Name in time bound manner
- Screen recordings of banking apps/websites used for misinformation
- Intellectual property rights (IPRs) violation across platforms
- Edited or clipped content taken out of context for misuse
- Reused videos with new misleading narratives
- Thumbnails, Tags related to the bank
- Morphed, fake, or misleading images affecting Bank's reputation
- Comments over Digital / Social Media, related to Chairman, MDs and other senior functionaries of the Bank, adversely affecting our Brand image

C. Virality & Reputation Risk Assessment

Apart from regular monitoring , the Service Provider shall also monitor, assess and classify content from the reputational risk perspective as under :-

- Probable threat of reputational damage
- Speed of sharing and engagement growth
- involvement of Influencer or high-reach account such as News Channels and webpages
- Cross-platform propagation
- Regional spread and language amplification
- Probability of mainstream media pickup

Each identified content shall be assessed on below parameters:

- Threat to brand reputation featuring defamatory / derogatory content
- Potential impact on public trust
- Financial risk to users
- Possibility of fraud or panic
- Regulatory and compliance implications
- Political, social, or sensitive contextual risks
- Any other criteria as suggested by the bank from time to time

Such Content shall be categorized in 4 categories as under and will be dealt as per the TAT decided by the bank under SLA

- **Critical Risk**
- **High Risk**
- **Medium Risk**
- **Low Risk**

- The Service Provider should also put in place a mechanism for real time alerts for high-risk and viral content having probability of reputational damage. A separate dashboard for monitoring such events should also be put in place as advised by the Bank as and when required.

D. Content Verification & Fact Analysis

The Service Provider shall in coordination with SBI team:

- Verify factual accuracy of viral claims
- Identify source authenticity
- Trace origin of content where technically feasible
- Determine intent: misinformation, disinformation, satire, fraud, or malicious activity
- Provide actionable intelligence briefs to the Bank

E. Takedown & Platform Enforcement Actions

The Service Provider shall:

- Draft and submit takedown notices to social media platforms
- Engage with platform representatives
- Use fast-track escalation mechanisms for taking down, including, but not limited to under-noted cases
    - Impersonation of brand name/ logo or Senior officials of the Bank
    - Fraudulent schemes
    - Misuse of Bank branding
    - Removal of malicious, misleading, defamatory, fraudulent, unauthorised or reputation-damaging content,
    - Brand guideline violation or brand / logo infringement related content.
    - Fake Profiles / handles / channels / pages / websites / Apps / phishing sites / Ads etc.
- Track takedown status and resolution timelines

The detailed process flow including timelines in this regard will be as per SLA

F. Content Blocking & Account Actions

- Recommend account suspension / blocking
- Identify repeat offenders
- Assist in permanent account removal where applicable

G. Legal Action & Enforcement Support

Legal Drafting & Advisory

The Service Provider shall provide:

- Drafting of:
    - Legal / defamation notices
    - Platform-specific legal complaints
- Advisory to bank on applicable laws including:

- IT Act & IT Rules
- Cybercrime and fraud statutes
- Defamation and intellectual property laws

Law Enforcement & Regulatory Liaison

The Service Provider will assist the designated bank officials in

- Sending Legal / defamation notices
- Support in filing complaints / FIRs wherever required
- Obtaining Injunction orders from Competent Courts on actual cost basis
- Initiating Civil or Criminal proceedings, wherever required
- Assistance in Law Enforcement actions
- Assistance with regulatory reporting
- Evidence preservation and documentation support for legal purposes
- Initiating suitable action, wherever required, as per DPDP Act, 2023

H. Crisis Management Support

- Immediate action during reputational risk crisis
- Identification of coordinated or malicious campaigns
- Support in content neutralization strategy
- Collaboration with Bank's PR, legal, and compliance teams
- Continuous monitoring until crisis closure

I. Reporting & Documentation

Regular Reports

- Daily monitoring summaries
- Weekly risk assessment reports
- Monthly trend and insight reports
- Reputational Risk reports including monitoring dashboards

- Platform-wise enforcement action reports
- Status monitoring and updating Bank about ongoing legal matters
- Any other reports as decided by the bank

Incident Reports

- Detailed incident analysis for major events
- detection, escalation, action, and closure details of such events
- Learnings and preventive recommendations for such events

J. Technology, Tools & Infrastructure

The Service Provider must ensure:

- Content detection and content intelligence systems
- Secure data storage and access controls
- Ensure compliance with data protection and confidentiality norms
- Backup of specified data as desired by the bank at specified frequency
- Mechanism for sharing Backup of data at a specified frequency with the Bank
- Audit-ready logs of all actions taken and share with Bank on need basis

K. Dedicated Team Structure

The Service Provider shall deploy a dedicated team for carrying out the activities mentioned in SOW, comprising of :

- Tech analysts (AI / video intelligence)
- Social media monitoring specialists
- Legal team with capabilities of handling such matters
- Relationship manager (s) / SPOC for the Bank

L. Confidentiality & Compliance

- Strict confidentiality of Bank data and findings
- No disclosure of incidents or actions without Bank approval
- Compliance with RBI, government, and cybersecurity guidelines
- Adherence to Bank's internal security and governance policies

M. Scope Flexibility

The Bank reserves the right to:

- Expand or restrict scope based on requirements as mutually decided by the Bank and the Service Provider
- Engage the Service Provider for additional legal or enforcement tasks as needed

Technical and Legal Capability

The Service Provider must possess Technical and Legal know how to perform the activities as per the Scope of Work. The Service Provider must also constantly upgrade its technical and Legal capabilities to adopt to the dynamic nature of Digital and Social Media.

Social Media Security

The Service Provider will provide alerts of various threats/ dynamic risks as and when it appears on social sites, which may be detected real-time by use of tool/ software or any other technique and initiate appropriate actions to be protected from it. Below are some threats which are just illustrative but not exhaustive.

- Brand and executive impersonations
- Financial frauds, Profanity & Customer attacks
- Scams (Recruitment, Coupons, Lottery, Counterfeit, etc.)
- Piracy and trademark infringement
- Viruses
- Phishing and Social engineering
- Data leakage or posting inappropriate corporate data
- Targeted attacks
- Insider threat
- Social account hijacking

- Spamming
- Any other existing or emerging threats not covered above

APPENDIX-A-1

Data Processing Agreement

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Service Level Agreement") dated _____between:

(i) State Bank of India ("Data Fiduciary")

AND

(ii) M/s. _____ ("Data Processor")

WHEREAS:

(A) State Bank of India (hereafter referred to as "SBI") acts as a Data Fiduciary.

(B) SBI wishes to contract certain Services (provided in **Schedule 1**), which imply the processing of personal data (provided in **Schedule 2**), to the Data Processor.

The Parties seek to ensure compliance with the Digital Personal Data Protection Act 2023 ('the DPDP Act') together with rules, regulations and Offshore Data Protection Regulations and implement the Agreement that complies with the requirements of the current legal framework in relation to data processing and with the applicable Data Privacy Laws.

(C) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation:

1.1 Unless otherwise defined herein, terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" has the meaning given to it as this Data Processing Agreement and all schedules.

1.1.2 "Data Fiduciary" has the meaning given to it in Data Privacy Laws and Offshore Data Protection Regulations.

1.1.3 "Data Privacy Laws" shall mean Digital Personal Data Protection Act 2023, rules and regulations made thereunder, the Information Technology Act, 2000, the Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules

2011 and any other laws, rules and regulations that is or shall become applicable regarding data protection and data processing in India.

1.1.4 “Data Principal” has the meaning given to it in the Data Privacy Laws and Offshore Data Protection Regulations.

1.1.5 “Party” or “Parties” has the meaning given to it as either Data Fiduciary or the Processor.

1.1.6 "Personal Data" has the meaning given to it in the Data Privacy Laws and under the Offshore Data Protection Regulations.

1.1.7 " Data Processor" has the meaning given to it in the Data Privacy Laws and Offshore Data Protection Regulations.

1.1.8 “Offshore Data Protection Regulations” shall mean data protection regulations including EU General Data Protection Regulation and such other regulations as may be applicable for processing of Personal Data in jurisdictions other than India.

1.1.9 “Sub-processor” has the meaning given to it as means any person appointed by or on behalf of Data Processor to process Personal Data of Data Principals in India or across any other jurisdiction on behalf of Data Fiduciary in connection with the Agreement.

1.1.10 "Data Transfer" shall mean

(i) a transfer of Personal Data from Data Fiduciary to a Data Processor; or

(ii) onward transfer of Personal Data from a Data Processor to a Sub-processor, or between two establishments of a Data Processor, to the extent and in the manner as envisaged in this Agreement.

1.1.11 "Services" has the meaning given to it as the services to be performed by the Data Processor described in the Service Level Agreement and as provided in Schedule 1.

1.1.12 “Supervisory Authority” has the meaning given to it in the Data Privacy Laws and Offshore Data Protection Regulations.

1.1.13 “Personal Data Breach” has the meaning given to it in Data Privacy Laws and Offshore Data Protection Regulations.

1.1.14 “Personnel” has the meaning given to it as the personnel of the Data Processor, Sub processors who provide the applicable Services;

2. Processing of Personal Data:

2.1 In the course of providing Services to Data Fiduciary, the Data Processor may process Personal Data on behalf of the Data Fiduciary.

2.2 Data Processor shall:

2.2.1 comply with all applicable Data Privacy Laws in the Processing of Personal Data; and where the data principal is within the jurisdiction of Offshore Data Protection Regulations, comply with

such respective Offshore Data Protection Regulations.

2.2.2 not Process Personal Data other than on the relevant documented instructions of the Data Fiduciary.

3. PROCESSOR OBLIGATIONS:

3.1 Processor and Processor Personnel:

3.1.1 The Data Fiduciary will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data only as set forth in Data Fiduciary's written instructions.

3.1.2 The Data Processor shall never process the Personal Data in a manner inconsistent with the Data Fiduciary's documented instructions. The Data Processor shall immediately inform the Data Fiduciary if, in its opinion, an instruction infringes Data Privacy Laws or other directions issued by sectoral regulators in India or applicable Offshore Data Protection Regulations.

3.1.3 The Data Processor shall take reasonable steps to ensure the reliability of any employee, agent or Sub-processor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Service Level Agreement, and to comply with applicable Data Privacy Laws and Offshore Data Protection Regulations in the context of that individual's duties to the Data Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Necessary Data Privacy training should be provided by the processor to their employees handling Personal Data.

3.1.4 Notwithstanding clause 3.1, if the Data Processor (and its Personnel) is required to process the Personal Data pursuant to the Offshore Data Protection Regulations or to satisfy any other legal obligations, the Data Processor shall notify Data Fiduciary of such requirement before it processes the Personal Data. and in case of processing of Personal Data under this clause it shall not be construed as processing of Personal Data by the Data Processor under this Agreement

3.1.5 The Data Processor shall immediately notify Data Fiduciary if, in Data Processor's opinion, Data Fiduciary's documented data processing instructions breach the Data Privacy Laws or Offshore Data Protection Regulations or sectoral regulators in India.

3.1.6 The purpose of the Data Processor processing Personal Data is the performance of the Services pursuant to the Service Level Agreement.

3.2 The Data Processor shall comply with Offshore Data Protection Regulations while processing data of an individual residing within the jurisdiction of the Offshore Data Protection Regulations. In the event of any liability arising on account of act or conduct of the Data Processor in processing data of a person residing within the jurisdiction of the Offshore Data Protection Regulations, the Data Processor shall be solely responsible for all pecuniary or other consequence on account of such liability.

3.3 Security:

3.3.1 Taking into account the nature, scope, context and purposes of Processing (provided in Schedule 1 & 2) as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk.

3.3.2 In assessing the appropriate level of security, Data Processor shall take into account, in particular, risks related to processing of Personal Data.

3.3.3 The Data Processor shall use appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and protect against accidental loss or destruction of, or damage to, any Personal Data during processing activities. It shall implement and maintain the security safeguards and standards based on the IS policy of State Bank of India as updated and notified to the Data Processor by State Bank of India from time to time. The Data Processor will not decrease the overall level of security safeguards and standards during the term of this Agreement without State Bank of India's prior consent.

3.4 Sub-Processing:

3.4.1 The Data Processor shall not appoint (or disclose any Personal Data to) any Sub- Processors without prior written authorisation from Data Fiduciary. The Data Processor shall provide Data Fiduciary with **[no less than XX days]** prior written (including email) notice before engaging a new Sub processor thereby giving Data Fiduciary an opportunity to object to such changes. If the Data Fiduciary wishes to object to such new Sub processor, then it may terminate the relevant Services without penalty by providing written notice of termination which includes an explanation of the reasons for such objection.

3.4.2 The Data Processor shall include in any contract with its Sub Processors who will process Personal Data on Data Fiduciary's behalf, obligations on such Sub Processors which are no less onerous than those obligations imposed upon the Data Processor in this Agreement relating to Personal Data. The Data Processor shall be liable for the acts and omissions of its Sub Processors to the same extent to which the Data Processor would be liable if performing the services of each Sub Processor directly under the terms of this Agreement.

3.5 Data Principal Rights:

3.5.1 Data Principal whose Personal Data is processed under this Agreement have all rights conferred on them under applicable Data Privacy Laws and Offshore Data Protection Regulations, in relation to their Personal Data (including, but not limited to, rights of access, correction, erasure, grievance, withdrawal of consent, and any other rights). All such requests shall be directed to Data Fiduciary, which is responsible for handling them in accordance with applicable Data Privacy Laws and Offshore Data Protection Regulations.

3.5.2 Taking into account the nature of the Processing, Data Processor shall assist, insofar as this is

possible, for the fulfilment of Data Fiduciary's obligations, as reasonably understood by Data Fiduciary, to respond to requests to exercise Data Principal rights under the Data Privacy Laws and Offshore Data Protection Regulations.

3.5.3 In case Data Principal Requests are received by the Data Processor, then the Data Processor shall:

3.5.3.1 promptly notify Data Fiduciary if it receives a request from a Data Principal and;

3.5.3.2 ensure that it does not respond to that request except on the documented instructions of Data Fiduciary;

3.5.3.3 inform Data Fiduciary of that legal requirement before the Data Processor responds to the request.

3.6 Personal Data Breach:

3.6.1 Data Processor shall notify Data Fiduciary promptly and without undue delay upon becoming aware of any actual or suspected Personal Data Breach, providing Data Fiduciary with sufficient details of the nature, scope, timing and potential impact of the breach to enable Data Fiduciary to fulfil its obligations under applicable Data Privacy Laws and Offshore Data Protection Regulations

3.6.2 Data Processor shall cooperate fully with Data Fiduciary and take all reasonable steps as may be directed by Data Fiduciary to investigate, mitigate, contain and remediate the Personal Data Breach, including providing Data Fiduciary with regular updates on the status and results of any such measures.

3.7 Data Protection Impact Assessment and Prior Consultation:

3.7.1 Data Processor shall provide all reasonable assistance to Data Fiduciary in carrying out any data protection impact assessments (DPIA) and any prior consultation with Supervisory Authorities or other competent data privacy authorities that Data Fiduciary reasonably deems necessary under applicable Data Privacy Laws in respect of the Processing of Personal Data.

3.7.2 Such assistance shall include descriptions of the Processing operations, and the categories of Personal Data involved; the purposes of the Processing; details of any technical and organizational measures implemented to safeguard Personal Data; and any other information that Data Fiduciary reasonably requests to complete the DPIA or consultation process.

3.8 Deletion or return of Personal Data:

3.8.1 Subject to this section 3.8 Processor shall, promptly and in any event within < **XX** > business days of the date of cessation of any Services under this Agreement either upon termination or expiry of the term of this Agreement (the "Cessation Date"), either delete, destroy or return all Personal

Data including copies of such Personal Data.

The Data Processor shall notify all Sub -Processors of the cessation and shall ensure that all such Sub Processor shall either delete, destroy or return the Personal Data (including copies of such Personal Data) to the Data Processor at the discretion of the Data Processor

3.8.2 Data Processor shall provide written certification to Data Fiduciary that it has fully complied with this section 3.8 within < **XX** > business days of the Cessation Date.

3.8.3 For enabling the detection of unauthorized access, its investigation, remediation and to prevent recurrence while allowing continued processing in the event of a compromise, retention of such logs and personal data shall be done for a period of one year, unless compliance with any law for the time being in force requires otherwise.

3.9 Audit Rights:

The Data Processor and the sub processors, if any, shall make available to Data Fiduciary and any or their representatives the information necessary to demonstrate its compliance with this Agreement and allow for and contribute to audits and inspections by allowing Data Fiduciary, a Supervisory Authority or their representatives to conduct an audit or inspection of that part of the Data Processor's business which is relevant to the Services [on at least an annual basis (or more frequently when mandated by a relevant Supervisory Authority or to comply with the Data Privacy Laws and] on reasonable notice, in relation to the Processing of Personal Data by the Processor.

3.10 Data Transfer:

3.10.1 Except as otherwise provided herein, the Data Processor shall not disclose Personal Data received here under to a third party or transfer it to another country without the Data Fiduciary's authorization. Except as otherwise provided herein, the Data Processor shall immediately notify the Data Fiduciary of any (planned) permanent or temporary transfers of Personal Data to a country outside of India and shall only perform such a transfer after obtaining authorization from the Data Fiduciary, which may be refused at its own discretion.

3.10.2 To the extent that the Data Fiduciary or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Fiduciary and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully acceptable.

3.11 Records:

The Data Processor shall maintain written records of its data processing activities pursuant to providing the Services to Data Fiduciary in accordance with Data Privacy Laws and Offshore Data

Protection Regulations.

3.12 Notify:

The Data Processor shall immediately and fully notify Data Fiduciary in writing of any communications the Data Processor (or any of its Sub-processors) receives from third parties in connection with the processing of the Personal Data, including (without limitation) data principal request or other requests, notices or other communications from individuals, or their representatives, and/or any other supervisory authority or data protection authority or any other regulator (including a financial regulator) or court.

3.13 Indemnity:

Data Processor shall defend, indemnify, and hold harmless Data Fiduciary, its directors, officers, employees, agents, affiliates, and representatives from and against any and all claims, actions, proceedings, fines, penalties, liabilities, damages, losses, costs, expenses, prejudice, and injury (whether pecuniary or non-pecuniary), reputational or otherwise, incurred from Data Fiduciary, arising out of or in connection with:

A. any Personal Data Breach (irrespective of the jurisdiction of the breach) resulting from Processor's negligence, including any such breach caused or contributed to by the Processor or its personnel;

B. any unauthorized, wrongful, or unlawful Processing, access, disclosure, loss, or destruction of Personal Data;

C. any failure by Processor to comply with Data Fiduciary's written instructions regarding Personal Data; and

D. any third-party claims (including those by customers, data principals, or regulators) resulting from any act, omission, or default of the Processor or its personnel.

3.14. Representation and Warranties:

The Data Processor represents and warrants that it will comply with all applicable Data Privacy Laws and Offshore Data Protection Regulations relating to the protection, disclosure, processing and use of Personal Data.

3.15. The Parties agree that in order to give effect / further effect to the provisions of the Data Privacy Laws and Offshore Data Protection Regulations and any amendment therein, this Agreement shall be amended, and the Parties shall execute and be bound by all such amendments as shall be necessary for the purpose of the arrangement as envisaged by this Agreement.

4. SBI'S OBLIGATIONS:

SBI shall:

4.1 in its use of the Services, process the Personal Data in accordance with the requirements of the Data Privacy Laws and Offshore Data Protection Regulations.

4.2 use its reasonable endeavours to promptly notify the Data Processor if it becomes aware of any breaches or of other irregularities with the requirements of the Data Privacy Laws in respect of the Personal Data processed by the Data Processor.

5. General Terms:

5.1. Duration and Termination:

This Agreement shall come into effect on the date execution and shall be valid for the period of [**XX**] years but shall be liable to be termination by either party by serving Notice to the other party of not less than [**XX**] days. Provided however, the Data Fiduciary shall be entitled to forthwith (without prior) notice, terminate this Agreement if, the Data Processor, to the sole determination of the Data Processor, commits any act that amounts to Personal Data Breach.

Notwithstanding the termination of this Agreement the provisions of clause 3.13 (Indemnity), clause 5.2 (Confidentiality) shall continue to be valid and binding upon the Data Processor.

5.2 Confidentiality:

Without prejudice to any existing contractual arrangements between the Parties, the Data Processor shall treat all Personal Data as strictly confidential and it shall inform all its employees, agents and/or approved sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data. The Data Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality

5.3 Notices:

All notices and communications given under this Agreement must be in writing and will be

delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

5.4 Governing Law and Jurisdiction:

5.4.1 This Agreement is governed by the laws of INDIA.

5.4.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of MUMBAI.

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Service Level Agreement with effect from the date first set out below.

For SBI

Signature _____

Name _____

Title _____

Date Signed _____

For Processor M/s

Signature _____

Name _____

Title _____

Date Signed _____

SCHEDULE 1

1.1 Services

<<

Insert a description of the Services provided by the Data Processor (under the Service level Agreement, where relevant)

>>.

SCHEDULE 2

Personal Data Processing

Details of Processing Activities (detailed list of activities carried about by the processor)	Category of Personal Data (Categories of Data Principal whose personal data is processed)	Category of Data Principal	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing	Duration of Retention of Personal Data of Data Principal

SCHEDULE 3

Technical and Organisational Data Protection Measures

1. The Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of SBI, it maintains security measures to a standard appropriate to:

1.1. the nature of the Personal Data; and

1.2. Safeguard from the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data.

2. In particular, the Processor shall:

2.1. have in place, and comply with, a security policy which:

2.1.1. defines security needs based on a risk assessment.

2.1.2. allocates responsibility for implementing the policy to a specific individual (such as the Processor's Data Protection Officer) or personnel and is provided to SBI on or before the commencement of this Agreement.

2.1.3. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice.

2.1.4. prevent unauthorised access to the Personal Data.

2.1.5. protect the Personal Data using pseudonymisation and encryption.

2.1.6. ensure the confidentiality, integrity and availability of the systems and services in regard to the processing of Personal Data.

2.1.7. ensure the fast availability of and access to Personal Data in the event of a physical or technical incident.

2.1.8. have in place a procedure for periodically reviewing and evaluating the effectiveness of the technical and organisational measures taken to ensure the safety of the processing of Personal Data.

2.1.9. ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled.

2.1.10. have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption).

2.1.11. password protect all computers and other devices on which Personal Data is stored, ensuring

that all passwords are secure, and that passwords are not shared under any circumstances.

2.1.12. not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times.

2.1.13. take reasonable steps to ensure the reliability of personnel who have access to the Personal Data.

2.1.14. have in place methods for detecting and dealing with breaches of security

(including loss, damage, or destruction of Personal Data) including:

2.1.14.1. having a proper procedure in place for investigating and remedying breaches of the GDPR; and

2.1.14.2. notifying SBI as soon as any such security breach occurs.

2.1.14.3. Access logs and related Personal Data shall be retained for a period of one year for enabling the detection of unauthorized access, its investigation, remediation and to prevent recurrence while allowing continued processing, unless compliance with any law for the time being in force requires otherwise.

2.1.15. have a secure procedure for backing up all Personal Data and storing back-ups separately from originals; and

2.1.16. adopt such organisational, operational, and technological processes and procedures as are required to comply with the SBI's Information Security Policy as appropriate.

At the time of signing this Agreement, the Processor has the following technical and organizational measures in place: (To be vetted by SBI)

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
1	Whether the Processor has Information security policy in place with periodic reviews?			
2	Whether the Processor have operational processes with periodic review, including but not limited to:	a. Business Continuity Management		
		b. Backup management		
		c. Desktop/system/server/network device hardening with baseline controls		
		d. Patch Management		
		e. Port Management Media Movement		
		f. Log Management		
		g. Personnel Security		
		h. Physical Security		
		i. Internal security assessment processes		
3	Whether a proper documented Change Management process has been instituted by the Processor?			
4	Whether the Processor has a documented policy and process of Incident management /response?			
5	Whether the Processor's environment is suitably protected from external threats by way of:	a. Firewall		
		b. WAF		
		c. IDS/IPS		
		d. AD		
		e. AV		
		f. NAC		
		g. DLP		
		h. Any other technology		
6	Whether rules are implemented on Firewalls of the Processor environment as per an approved process?			
7	Whether firewall rule position is regularly monitored for presence of any vulnerable open port or any-any rule?			

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
8	Whether proper log generation, storage, management and analysis happens for the Processor application?			
9	Is the Processor maintaining all logs for forensic readiness related to:	a. Web		
		b. Application		
		c. DB		
		d. Configuration		
		e. User access		
10	Whether the Processor maintains logs for privileged access to their critical systems?			
11	Whether privilege access to the Processor environment is permitted from internet?			
12	Whether the Processor has captive SOC or Managed Service SOC for monitoring their systems and operations?			
13	Whether the Processor environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall, where any access from an external entity is permitted through DMZ only?			
14	Whether Processor has deployed secure environments for their applications for:	a. Production		
		b. Disaster recovery		
		c. Testing environments		
15	Whether the Processor follows the best practices of creation of separate network zones (VLAN Segments) for:	a. Web		
		b. App		
		c. DB		
		d. Critical applications		
		e. Non-Critical applications		
		f. UAT		
16	Whether the Processor configures access to officials based on a documented and approved Role Conflict Matrix?			
17	Whether Internet access is permitted on:	a. Internal servers		
		b. Database servers		
		c. Any other servers		

S. No	Controls to be implemented	Compliance (Yes / No)	If under implementation, give date by which implementation will be done
18	Whether the Processor has deployed a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations?		
19	Whether CERT-IN Empaneled ISSPs are engaged by the third party for ensuring security posture of their application?		
20	Whether quarterly vulnerability assessment and penetration testing is being done by the Processor for their infrastructure?		
21	Whether suitable Security Certifications (ISO, PCI-DSS etc.) of the security posture at vendor environment are in place?		
22	Whether the Processor has deployed any open source or free software in their environment?		
	If yes, whether security review has been done for such software?		
23	Whether the data shared with the Processor is owned by SBI (SBI = Information Owner)?		
24	Whether the data shared with the Processor is of sensitive nature?		
25	Whether the requirement and the data fields to be stored by the Processor is approved by Information Owner?		
26	Where shared, whether the bare minimum data only is being shared? (Please document the NEED for sharing every data field)		
27	Whether the data to be shared with Processor will be encrypted as per industry best standards with robust key management?		
28	Whether the Processor is required to store the data owned by State Bank?		
29	Whether any data which is permitted to be stored by the Processor will be completely erased after processing by the Processor at their end?		
30	Whether the data shared with the Processor is stored with encryption (Data at rest encryption)?		
31	Whether the data storage technology (Servers /Public Cloud/ Tapes etc.) has been appropriately reviewed by IT AO?		
32	Whether the Processor is required to share SBI specific data to any other party for any purpose?		
33	Whether a system of obtaining approval by the Processor from the IT Application Owner is put in place before carrying out any changes?		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
34	Whether Processor is permitted to take any crucial decisions on behalf of SBI without written approval from IT Application Owner?			
	If not, are such instances being monitored? IT Application Owner to describe the system of monitoring such instances.			
35	Whether Application Owner has verified that the Processor has implemented efficient and sufficient preventive controls to protect SBI's interests against any damage under section 43 of IT Act?			
36	Whether the selection criteria for awarding the work to Processor vendor is based on the quality of service?			
37	Whether the SLA/agreement between SBI and the Processor contains these clauses:	a. Right to Audit to SBI with scope defined		
		b. Adherence by the vendor to SBI Information Security requirements including regular reviews, change management, port management, patch management, backup management, access management, log management etc.		
		c. Right to recall data by SBI.		
		d. Regulatory and Statutory compliance at vendor site. Special emphasis on section 43A of IT Act 2000 apart from others.		
		e. Availability of Compensation clause in case of any data breach or incident resulting into any type of loss to SBI, due to vendor negligence.		
		f. No Sharing of data with any third party without explicit written permission from competent Information		

S. No	Controls to be implemented		Compliance (Yes / No)	If under implementation, give date by which implementation will be done
		Owner of the Bank including the Law Enforcement Agencies.		

ANNEXURE-B

TAT SHEET

TAT Sheet (All activities related to the following)

1. Monitoring/Identification of Content
2. Taking Down of Contents including those advised by the bank
3. Initiating Legal action including injunction orders
4. Internal reporting to Bank
5. Any other activities as per the Statement of work mutually agreed by the bank and the Service Provider

ANNEXURE-C

Team Structure and Escalation (to be provided by the vendor)