



SBI PENSION FUNDS (P) LTD.

Request for Quotation

**Privilege Identity Management (PIM)
Privilege Access Management (PAM)**

SBI Pension Funds Private Limited

Ref NO. SBIPFPL/IT/RFP-002/2021-22

Request For Quotation

For Implementation and Support of Privilege Identity Solution/Privilege Access Management.

| ACTIVITY SCHEDULE | | |
|--------------------------|---|---|
| Sr No | Activity | Details |
| 1. | RFP Number | SBIPFPL/IT/RFP-002/2021-22 |
| 2. | Bid Document Availability including changes/amendments, if any to be issued | downloaded from Company's website https://www.sbipensionfunds.com/ |
| 3. | Call for Quotation | 24 June, 2021 |
| 4. | Any Query / Clarification | Queries on email |
| 4. | Online Bid submission | 27 June 2021, 2021- 16:00 Hrs |
| 5. | Technical/Commercial Bid Opening | 28 June, 2021- 10:00 Hrs |
| 6 | Technical Bid Evaluation and Presentation of shortlisted Service Providers | Mutually Decided |
| 7. | Opening of Commercial Bids | 28 June, 2021- 10:00 Hrs |
| 8. | Method of Selection | The method of selection is Quality and Price Base Selection. The weights given to the Technical capability and Commercial Proposals. |
| 9. | Reverse Auction | Not Applicable |
| 10 | SBIPFPL- Contact Details | Mr. Rajesh K Mishra (CISO) M –7488925030 ciso@sbipensionfunds.com Mr. Prateek Pal (Assistant Manager - IS) M-9987276324systems@sbipensionfunds.com |

1. Introduction

1.1 Background of Company

SBIPFPL is committed to improve its security posture and achieves this objective by updating its processes and technology periodically. Driven by this commitment, SBIPFPL is inviting quotation from Original Equipment Manufacturer (OEM) or Service Providers (SP) to implement Privilege Identity Management (**PIM**) / Privilege Access Management (**PAM**) solution to improve security posture and enhance SBIPFPL's capabilities to monitor, respond and mitigate threats against IT infrastructure of SBIPFPL.

SBIPFPL intends to engage a Service Provider (SP) /OEM who has a sustainable and proven business model, recognized accreditation, established customer-base, distinguishable solution accelerators and enablers, high-performance personnel, while maintaining the ability to support its requirements.

SP's/OEM's are advised to study the document carefully. Submission of proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

The SP/OEM shall bear all Prices associated with the preparation and submission of the proposal, including Price of presentation for the purposes of clarification of the proposal, if so desired by SBIPFPL. SBIPFPL will in no case be responsible or liable for those Prices, regardless of the conduct or outcome of the selection process.

1.2 Disclaimer:

- 1.2.1. The information contained in this document or information provided subsequently to Bidder(s) whether verbally or in documentary form/email by or on behalf of SBIPFPL (Company), is subject to the terms and conditions set out in this document.
- 1.2.2. This is not an offer but an invitation to receive responses from the eligible Bidders. No contractual obligation whatsoever shall arise from the quotation process unless and until a formal contract is signed and executed by duly authorized official(s) of SBIPFPL with the selected Bidder.
- 1.2.3. The purpose of this document of call for quotation is to provide the Bidder(s) with information to assist preparation of their proposals. This document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this document and where necessary obtain independent advices/clarifications. Company may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information if required.
- 1.2.4. SBIPFPL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, Price or expense which may arise from or be incurred or suffered on account of anything contained in this document or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the document and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

- 1.2.5. SBIPFPL also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this document.
- 1.2.6. The issue of this document does not imply that the SBIPFPL is bound to select a Bidder or to appoint the Selected Bidder or Concessionaire for the Project and the Company reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.
- 1.2.7. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder's risk and may result in rejection of the Bid.
- 1.2.8. Proposed solution must be as per the detailed Technical Specifications and the Vendor should adhere to Scope of Work mentioned in this document.
- 1.2.9. The Purchase Order may be placed in part or full by SBIPFPL, the quantity or number of equipment/license to be purchased as mentioned in this document is only indicative. No guarantee or assurance is being provided hereby as to the exact quantity of equipment to be purchased or the minimum order quantity. SBIPFPL, however, reserves the right to procure extra quantity/license during the bid validity period of the offer and till 3 year from the date of project sign-off. However, the quality of services (QOS) will be reviewed annually, and contract may be terminated if the QOS will not be improved reasonably. The price of such procurement will be calculated on pro-rata basis of the balance period.

1.3. Definitions

Throughout this document, unless inconsistent with the subject matter or context:

- 1.3.1. Vendor/ Service Provider/ System Integrator – PIM/PAM Vendors.
- 1.3.2. **Supplier/Contractor/Vendor** – Selected Vendor for this project only.
- 1.3.3. **Company/ Purchaser/** SBIPFPL - Reference to the "SBIPFPL", "Company" and "Purchaser" shall be determined in context and may mean without limitation "SBIPFPL".
- 1.3.4. **Proposal/ Bid** – the Vendor's written reply or submission in response to this document
- 1.3.5. **Tender** – the request for quotation (this document) is entirely, inclusive of any Addenda that may be issued by SBIPFPL.
- 1.3.6. **Solution/ Services/ Work/ System** – "Solution" or "Services" or "Work" or "System" all services, scope of work and deliverable to be provided by a Vendor as described in the document
- 1.3.7. **Product** – "Product" means PIM/PAM
- 1.3.8. **Server / Network / Website** – As specified within the technical requirement section of this request for quotation document.

2. RFP Process

The technical and commercial proposal with the relevant information/documents/acceptance of all terms and conditions as described in this document will be submitted online.

If the tender document is sent to us in hard copy, bidder should take all responsibility of loss /delay. Bid received after due date will not be accepted under any circumstances. An additional copy of the bid needs to be submitted (password protected) to ciso@sbipensionfunds.com

They cannot make their online submission after the time stipulated above and no extension of time will normally be permitted for submission of bids.

Background and Purpose of the Project

The Company has deployed applications across its network for various usage. These applications along with database are being managed internally or through VPN by Company's own /Outsourced team. The administrator/Super user password is also maintained and changes as per Company's guidelines. Company is also following change management process for any change in server/application/database. At present the password policy across all servers is not uniform and is being applied as per the administrator managing the server. Further, changes which require root/admin access, is being given to different users and the changes being performed by admin users are not being logged. The purpose of is to procure a solution **Privileged Identity Management (PIM)/ Privilege Access Management (PAM)/ Privilege User Management (PUM) Tool** for automated monitoring of all User activities across Company devices which would function as a Centralized authentication and authorization system with best security practices along with role based access control for all servers. The tool will monitor the user activity in case any change is being done by super user/user and will store the super user logs for verifying the activities being carried out by them. It would ensure better user management across various servers by applying restrictions on user profile as per role which can be changed on immediate basis.

Scope of Work

The solution will be installed at the Data Center with High Availability (HA) mode. The policies if applied should get replicated immediately across all PIM servers and should have a feature to roll back the applied policy for group admins. The solution should have capability of integrating all devices irrespective of their Hardware/OS/application/Database in Bank environment. Further, in case of any upgradation of current Hardware/OS/application/Database in Company, the same should be integrated with PIM Solution within one month. No extra cost will be paid to vendor for any customization. Vendor should provide and implement all feature upgrades or version upgrades during contract period without any cost. There should be Maker Checker feature available in case any configuration/policy change is being done by any user. Vendor should provide support to plug out any vulnerability found in the PIM solution as and when identified by Bank, as well as by the OEM. Patches made available by the OEM should be applied immediately. All vulnerabilities should be closed immediately or within 15 days of reporting the same to vendor. The successful bidder, in coordination with the OEM must make a detailed study of Company infrastructure and requirements relating to the solution, prepare a detailed plan document/road map mentioning all the pre-requisites, timeframe of milestones/achievements within the Completion Period leading to the full operationalization of the solution. The vendor will provide a detailed Business Requirement Document (BRD), Solution design and Project Plan. The implementation would start only after sign-off of the documents submitted by vendor/Go-ahead from the Company. During the requirement analysis phase, if the bidder expresses inability to integrate any system considered critical by Bank or the PIM solution does not support any requirement, Company may reject the process at its sole discretion without assigning any reason and without incurring any liability towards the vendor.

Technical Specifications

| SR | | Complied with (Y/N) | Remark if Any |
|----|--|---------------------|---------------|
| A | <p>Authentication Models</p> <ul style="list-style-type: none"> ➤ There should be a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc. ➤ The solution should be agentless i.e. does not require to install any agent on target devices ➤ The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection ➤ The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server. ➤ The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server ➤ The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism ➤ The solution should also provide local authentication and all the security features as per best standards. ➤ The solution should provide flexibility user/device wise for local authentication or enterprise authentication ➤ The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors. ➤ The solution should provide multi-domain feature whereby the entire operations can be carried out within a tenant or line of business. ➤ The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs ➤ The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple data center may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations | | |

B

Password Management

- The solution shall perform password change options which is parameter driven
- The solution should set password options every x days, months, years and compliance options via the use of a policy
- Ability to create exception policies for selected systems, applications and devices
- The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.
- The solution enables an administrator to change a target account password to a random value based on a manual trigger or automatic schedule.
- Allow single baseline policy across all systems, applications and devices (e.g. one single update to enforce baseline policy)
- The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')
- Ability to generate 'One-time' passwords as an optional workflow
- Ability to send notifications via email or other delivery methods triggered by any type of activity
- Ability to send notification via email to the user requesting the password that checkout is complete
- Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period
- All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys
- The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities
- The solution should have the ability to reconcile passwords manually, upon demand
- The solution should automatically verify , notify and report all passwords which are not in sync with PIM
- The solution should have the ability to automatically "checkout" after a specific time and "check-in" within a specified time
- The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.
- The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.

- | | | | |
|--|--|--|--|
| | <ul style="list-style-type: none">➤ The solution should be able to control re-prints with adequate authorization➤ Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)➤ The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests. | | |
|--|--|--|--|

| | | | |
|---|--|--|--|
| C | <p>Access Management</p> <ul style="list-style-type: none"> ➤ The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end user ➤ The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM ➤ The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end user. ➤ The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/), front-end database utilities on any combination of target account, group or target system and end-user ➤ The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc. ➤ The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user ➤ The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user ➤ The solution can restrict user-specific entitlements of administrators individually or by group or role ➤ The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical. ➤ The solution can restrict target-account-specific entitlements of end users individually or by group or role. ➤ The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired. ➤ The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time. ➤ System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH | | |
|---|--|--|--|

D

Privileged Session Management and Log Management

- The solution should be able to support an session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments
- The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+
- The solution should be able to log/search text commands for all sessions of database even through the third party utilities
- The solution should be able to log/search based on text commands for all sessions
- The solutions should support option for enabling session based recording for all sessions on any combination of target account, group or target system and end-user.
- All logs created by the solution should be tamper proof and should have legal hold
- The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group
- The tool can restrict access to different reports by administrator, group or role.
- The tool generates reports in at least the following formats: HTML, CSV and PDF
- System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts
- The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats (non-editable and encrypted) preferably in any proprietary format.
- The session recording should be SMART to help jump to the right session through the text logs
- Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.
- The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary
- The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording (Optional). All other commands will be included.
- The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution

| | | | |
|--|--|--|--|
| | <ul style="list-style-type: none">➤ The proposed solution shall allow configuration at platform level to allow selective recording of specific device (Optional).➤ The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).➤ The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.➤ The proposed system shall support full colour and resolution video recording.➤ The proposed system shall support video session compression with no impact on video quality. | | |
|--|--|--|--|

| | | | |
|--|--|--|--|
| | <p>PIM Security</p> <ul style="list-style-type: none"> ➤ All communication between system components, including components residing on the same server should be encrypted. ➤ All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway) ➤ The Administrator user cannot see the data (passwords) that are controlled by the solution. ➤ Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.). ➤ Solution should be TLS1.2 and SHA-2 Compliant and can validate FIPS 140 -2 cryptography for data encryption. ➤ The solution should secure Solution should secure master data records, entitlement, policy data and other credentials in a non-modifiable storage device/process. | | |
| | <p>PIM Administration</p> <ul style="list-style-type: none"> ➤ There must be central administration web based console for administration, user and device management and having of feature to auto on-board them. ➤ The tool uses Active Directory/LDAP as an identity store for administrators and end users. ➤ The tool enables an administrator to define groups (or similar container objects) of administrators and end users. ➤ The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one super group. ➤ The tool enables an administrator to define a hierarchy of roles without limit. ➤ Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address. ➤ Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly ➤ Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.). ➤ All administrative task should be done LOB wise i.e. Line of Business Wise | | |
| | <p>Architecture</p> <ul style="list-style-type: none"> ➤ Support of multi-tier architecture where the database and application level is separated. | | |

| | | | |
|--|---|--|--|
| | <ul style="list-style-type: none"> ➤ Scalable Architecture (Horizontally /Vertically) and not limited to restricted hardware/Software count. (Specified correctly if there is such limit) ➤ Solution should work at the network layer instead through a jump server. This will have achieve large number of sessions. ➤ Solution can support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations. ➤ Solution shall have options for backup or integration with existing backup solutions ➤ Solution can handle loss of connectivity to the centralized password management solution automatically. ➤ There should not be any requirement of change in existing network topology to control privilege session and can support distributed network architecture where different network segment can be controlled centrally. ➤ Solution should support client based and browser based administrations. ➤ Solution should preferably be an agentless and include password management and session recording features. ➤ Solution must support parallel execution of password reset for multiple concurrent request. ➤ Solution should support failover form single active instance to stand by instance without loss of any data. ➤ Solution should support virtual server instance for management and installation if required. ➤ Solution can support multiple instance with load balancer if required in future. ➤ System should support for implemented in high availability mode ➤ Solution should have capability to have direct connection with target device using secured gateway channel without compromising risky ports. ➤ System has ability to integrate with enterprise authentication systems like ADS, LDAP, windows SSO, RADIUS etc. ➤ Systems has ability to integrate BI-METRIC Solution, Hardware/Software Tokens, Ticketing system, HSM (Hardware Security Module), Automation Software if any. | | |
| | <p>SIEM Integration</p> <ul style="list-style-type: none"> - Solution should be able to integrate with leading SIEM Solutions and or other performance monitoring applications to eliminate password hardcoding feature. | | |
| | <p>Password Management</p> <ul style="list-style-type: none"> - Solution should manage to protect and preferably eliminate privileged credentials in application, scripts or configuration files. | | |

| | | | |
|--|--|--|--|
| | <p>Discovery of Privilege Account</p> <ul style="list-style-type: none"> - Solution should authenticate and trust the application requesting privilege password. - Solution should be capable to discover privilege accounts on target system, manage user governance and can reconcile it. It can identify non built-in-local (backdoor) admin or equivalent account. - Solution should identify public/private SSH key, orphan key, and can ascertain its status. | | |
| | <p>Notification of Alerts</p> <p>Solution should be able to generate alert through SMS/Email</p> <ul style="list-style-type: none"> - For any critical PIM Events and able to send message - For any change in Admin rights or configuration file - On Other critical events based on customization | | |
| | <p>Dash-Board/Reports</p> <p>Solution should provide</p> <ul style="list-style-type: none"> - Real time view of the activities of Administrators - Reports based on defined frequency, on-demand - Scheduled Reports like User Activity/Privileged account list/ activity logs - System Administrator changes performed by PIM Admin - Reports of password lockouts/checkout on system/password change report/Password status - Other customised reports - Other Audit Reports based by IT auditors requirement - Ability to replay actual session recording for any forensic analysis as and when required. - Dashboard for viewing critical events and password polices. | | |

Count of License Requirement (As on date)

| | Description | Count | Unit Cost | Total Cost |
|--------------------|--------------------|-----------|-----------|------------|
| Server | Data Base | 4 | | |
| | DB Server | 4 | | |
| | App server | 4 | | |
| | Web server | 1 | | |
| | Total | 13 | | |
| Admin Users | Admin Users | 12 | | |

Format of commercial Quotation

| S.No. | Items | Unit Cost (a) / Bundle License Cost | Multiplicati on Factor (b) | Total Cost (c=a*b) (exclusive of all taxes) |
|--------------|--|-------------------------------------|----------------------------|---|
| A | License Cost for IP | | | |
| B | License Cost for User | | | |
| C | Implementation Cost (including Integration if any) | | | |
| D | AMC of solution per year applicable after expiry of warranty) (range Minimum 10%- Maximum 20% of (A+B) | | | |
| Total | A+B+C+D | | | |

Payment Terms:

| Sl. No. | Details |
|---------|--|
| 1. | Payment would be done on upon receipt of invoice from vendor. AMC charges will be payable as and when due. |

Other Terms & Conditions:

Quotation should strictly confirm to the specifications. Any incomplete or ambiguous terms/ conditions/ quotes or non-conformance to the specification will disqualify the offer.

SBIPFPL reserves the right to accept in part or in full or reject or cancel the entire quotation without assigning any reason there for at any stage.

Any terms and conditions otherwise documented from the Vendors are not acceptable to the SBIPFPL. SBIPFPL reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

Not with standing approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition. Payment shall be regulated on the actual work done at the accepted rates and payment schedule.

The rates finalized discovered will be valid for 36 months and the vendor is bound to execute the orders placed at rates during the duration of the contract.

The validity period may be extended at the discretion of SBIPFPL which will be binding on the vendors. The prices should be **exclusive of all taxes**, the vendor should arrange for obtaining of permits wherever applicable.

During the validity period of quotes, any upward change in the exchange rate/excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SBIPFPL, notwithstanding what has been stated in the quotation or in the Purchase Order.

The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the product for which the Vendor has quoted.

The tools used for PIM/PAM by the vendor should be licensed one.

Cloud based solution / tools and the channel being used, should be clearly stated.

Vendor shall conduct monthly meetings with SBIPFPL and develop use cases of solution. Vendor shall ensure that use cases are updated regularly to keep it relevant to emerging threats.

It would be binding upon the vendor to always maintain security of SBIPFPL systems.

SBIPFPL may change the evaluation criteria at its own discretion after receipt of bids from competent bidder. SBIPFPL also reserves the rights to remove components from Commercial bid for evaluation purpose and for releasing the work order for partial scope.

SBIPFPL will notify in writing by way of issuance of purchase order through letter or email that its Bid has been accepted. The selected Bidder must acknowledge by return email/letter in token of acceptance.

Penalties for Delayed Implementation - Implementation should be started immediately from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SBIPFPL will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

The Bidders will have to submit the **Service Level Agreement** and **Non-disclosure Agreement** as per **standard format** prescribed by company together with acceptance of all terms and conditions of this document, duly signed by the authorized signatory.

Copy of board resolution and power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the acceptance letter, contract and NDA should be submitted.

Confidentiality

This document contains information confidential and proprietary to SBIPFPL. Additionally, the Bidder will be exposed by virtue of the contracted activities to internal business information of SBIPFPL, the Associates, Subsidiaries and/or business partners. The Bidders agree and undertakes that they shall keep confidential all matters relating to this RFP and will not make any disclosure to any person who is under the obligation under this document, any information, data, and know-how, documents, secrets, dealings, transactions or the terms or this RFP (the "Confidential Information"). Disclosure of receipt of this document or any part of the aforementioned information to parties not directly involved in providing the services requested could be treated as breach of confidentiality obligations and SBIPFPL would be free to initiate any action deemed appropriate.

The restrictions on disclosure of confidential information shall not apply to any matter which is already available in the public domain; or any disclosures made under law.

No news release, public announcement, or any other reference to this document or any program there under shall be made without written consent from SBIPFPL. Reproduction, without prior written consent of SBIPFPL, by photographic, electronic, or other means is strictly prohibited.

Non-Disclosure Agreement

The shortlisted bidder will be required to sign a Non-Disclosure Agreement with SBIPFPL. The Bidder shall treat all documents, information, data, and communication of and with SBIPFPL as privileged and confidential and shall be bound by the terms and conditions of the Non-Disclosure Agreement.

Governing Law and Jurisdiction

All disputes and controversies arising out and related bid documents shall be subject to the exclusive jurisdiction of the **Courts in Mumbai** and the parties agree to submit themselves to the jurisdiction of such court and the governing law shall be the laws of India.

Arbitration

All disputes and differences of any kind whatsoever shall be settled by Arbitration in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory amendment thereof. The

dispute shall be referred to the sole arbitrator who shall be appointed by SBIPFPL. The venue of Arbitration proceedings shall be at Mumbai. The Arbitration proceedings shall be conducted in English Language. The award of the Arbitration shall be final and binding on both the Parties and shall be delivered in Mumbai in the English language. The fees of the Arbitrator and the cost of the Arbitration proceedings shall be equally borne by both the Parties.

Indemnification

The Bidder shall, at its own cost and expenses, defend and indemnify SBIPFPL against all losses, judgements, statutory and regulatory penalties, fines, damages, third-party claims on account of the any misrepresentation, infringement of intellectual property rights, frauds, and breach of terms of this violation by the Bidder of any or all national/international trade laws, norms, standards, procedures etc.

The Bidder shall expeditiously meet any such claims and shall have full rights to defend itself there from. If SBIPFPL is required to pay compensation to a third party on account of the Bidder or association with the Bidder, then the Bidder shall be fully responsible for the same, including all expenses and court and legal fees.

Force Majeure

In case of delay in implementation of the Project on account of conditions which are beyond the control of the shortlisted bidder such as war, floods, earthquakes, strikes, lockouts, epidemics, pandemic, riots, fire or Governmental regulations superimposed after the date of order/ contract, the Parties shall be permitted to terminate the contract / bid document, if such delay extends for a period beyond 15 days. SBIPFPL shall not be liable to make any payments in this case.

Termination

SBIPFPL reserves the right to abandon the current tender process and restart the bidding process at any point of time without assigning any reason whatsoever. SBIPFPL can cancel the award granted to the elected Bidder at any point of time and restart the bid process completely or select another Bidder. The Elected Bidders understands and agrees that SBIPFPL shall not be obligated in any manner whatsoever and is free to stop / modify the bidding process at any stage without any liability.

Data Protection

The Bidders authorizes the release from time to time to SBIPFPL (and any of its Subsidiaries or Affiliates) all personal or professional data that is necessary or desirable for the administration of the "Relevant Information". Without limiting the above, the bidders permit SBIPFPL to collect, process, register and transfer to and from mentioned entities all Relevant Information. The Relevant Information will only be used in accordance with applicable law.

Intellectual Property

SBIPFPL shall have sole exclusive ownership to all its Intellectual property including and not limited to its trademarks, logos etc. This document shall in no way be considered as a transfer or assignment of the respective rights over any intellectual property owned, developed or being developed by SBIPFPL.

Commitments of BIDDERS

The BIDDER commits himself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit himself to the following: -

The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

The BIDDER further undertakes that they have not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract.

BIDDERS shall disclose the name and address of agents and the representatives and Indian BIDDERS shall disclose their foreign principals or associates if any.

BIDDERS shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract (if applicable).

The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

The BIDDER shall not instigate or cause to instigate any third party/ person to commit any of the actions mentioned above.

If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of submitting the quotation. The term 'relative' for this purpose

would be as defined in Section 6 of the Companies Act 1956. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reasons.

Annexure-

Inventory List

List of devices / servers (Total 20 device list Approximate)

| Sr. No. | Model | IOS / OS Version | Qty |
|---------|--------------------------|---|-----|
| 1. | Network Devices | Firewall, Routers, Switches, | 7 |
| 2. | AD server | AD | 1 |
| 3. | Servers | Ubuntu(1), Redhat (3) ,Windows server (4) | 8 |
| 4. | Database | Oracle , Mysql | 2 |
| 5. | Other Applications on VM | DLP, EDR | 1 |

Device details include DR setup.

*Kindly also mention cost for additional license if device added subsequently.

Bidder's Organization Profile

(To be printed on Bidder's Letter Head and included with the Technical Bid and Quotation Envelope)

Date: _____

To:

The Head, Information Security

SBI Pension Funds Private Limited,

No 32, 3rd Floor, Maker Chamber-III

Nariman Point, Mumbai-400021

Dear Sir,

Ref: **SBIPFPL/IT/RFP/001** dated: DD.MM.YYYY

Details of the Bidder:

| S/N | Particulars | Bidders Comment |
|-----|---|--|
| 1 | Name of Bidders Company | |
| 2 | Registered Office Address | |
| 3 | Date of Incorporation | |
| 4 | Contact Person Phone and Email | |
| 5 | Director, MD & CEO Name and contacts | |
| 6 | Total Employee count PAN India | |
| 7 | Brief description of the Bidder including details of its main line of Business | |
| 8 | Company /firms website URL | |
| 9 | Of the Authorized Signatory of the Bidder (i.e. Name, Designation, address, contact no., email) | |
| 10 | Income Tax. No. (GST/PAN/GIR). Please enclosed photocopy of latest income tax clearance certificate | |
| 11 | Bidders support office presence at Mumbai, Hyderabad, Chennai, New Delhi, Kolkata) | If not available, how bidder will support remote locations |
| 12 | Total No. of clients in India for the bidder for similar implementation PIM/PAM Solution | |
| 14 | No. of Years of experience, Bidder has in System Integration and providing managed services | |
| 15 | Number of technicians available in for proposed solution and its components | |
| 16 | The Organization certificated with process ISO 9001/20000,27001/ITIL etc. (if any) | |
| 17 | Capability to support 24/7 | |

Non-Disclosure Agreement (NDA) Format

(to be printed on Bidder's Letter Head and included with the Technical Bid Envelope)

THIS AGREEMENT ("**the Agreement**") is made on this ____ day of _____, 2021.

BETWEEN

SBI Penson Funds Private Limited an Indian company duly incorporated under the Companies Act, 1956, having its registered office at No 32, 3rd Floor , Maker Chamber -III , Nariman Point Mumbai - 400021 (hereinafter for the purposes of this agreement, referred to as "**SBIPFPL**")/ "**Disclosing**

Party”), which expression shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors and permitted assigns;

AND

_____ LIMITED, a company incorporated Registered under the Companies Act, 1956 and having its registered office at

_____ in(hereinafter referred to as the “Receiving Party”), which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns)

WHEREAS:

1. SBIPFPL is an authorized Pension Fund Manager for Pension fund products and is registered with PFRDA (Pension funds Regulatory Development Authority).
2. **The Receiving Party** is engaged in the business of _____.
3. **SBIPFPL** and **the Receiving Party** are in the process of discussion and negotiation wherein **SBPFPL** will provide its Information related to Systems, Device, Applications, logs, etc. (“Information”) to the **Receiving Party** and may during discussion, negotiation and/or performance of the said Services, disclose, provide, or make available to **the Receiving Party** certain Confidential Information as defined herein below; and
4. **SBIPFPL** desires to restrict use and disclosure of such Confidential Information as set out herein below.

NOW THEREFORE in consideration of the mutual promises and covenants contained in this Agreement, and the mutual disclosure of Confidential Information to each other, the Parties hereto agree as follows:

1. Confidential Information and Confidential Materials

- (a) “Confidential Information” means non-public information that **SBIPFPL** designates as being confidential or which under the Confidential Information circumstances surrounding disclosure ought to be treated as confidential. “Confidential Information” includes, without limitation, information relating to released or unreleased SBIPFPL ’s services or products, the marketing or

promotion of any **SBIPFPL** Product, **SBIPFPL** 's business policy, Confidential Information or practices, and information received from others that **SBIPFPL** is obligated to treat as confidential. Confidential Information disclosed to the Receiving Party by any parent or agent of **SBIPFPL**, or by any subsidiary of parent of **SBIPFPL**, is covered by this Agreement.

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without the Receiving Party's breach of any obligation owed to **SBIPFPL**; (ii) became known to the Receiving Party prior to **SBIPFPL**'s disclosure of such information to the Receiving Party; (iii) became known to the Receiving Party from a source other than the breach of an obligation of confidentiality owed to **SBIPFPL**; (iv) is independently developed by the Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing Confidential Information, including without limitation, written or printed documents and computer disks or tapes, whether machine or user readable, the Software being licensed including any manual and documents relating to the Software, its Source Code, etc.

2. Restrictions

(a) Except as provided below, the Receiving Party shall not disclose any Confidential Information to third parties. However, the Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order, provided the Receiving Party shall give **SBIPFPL** reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. This restriction on disclosure of Confidential Information shall apply to all the Confidential Information disclosed before entering the service agreement and shall continue to have effect during the subsistence of the Service Agreement. It shall also survive the termination of such agreement for provision of the services, as set out in the recitals hereinabove.

(b) The Receiving Party shall take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, to keep confidential the Confidential Information. The Receiving Party may disclose Confidential Information or Confidential Material only to the Receiving Party's employees or consultants on a need-to-know basis. The Receiving Party will have executed or shall execute appropriate written agreements with its employees and consultants sufficient to enable it to comply with all the provisions of this Agreement

(c) Confidential Information and Confidential Materials may be disclosed, reproduced, summarized or distributed only in pursuance of the Receiving Party's business relationship with **SBIPFPL**, and only as otherwise provided hereunder. The Receiving Party agrees to segregate all such Confidential Materials from the confidential materials of others in order to prevent commingling.

(d) Publications: the Receiving Party shall not make any news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the **SBIPFPL**.

3. Rights and Remedies

- (a) The Receiving Party shall notify SBIPFPL immediately upon discovery of any unauthorized use or disclosure of Confidential Information and/or Confidential materials, or any other breach of this Agreement by the Receiving Party, and will co-operate with **SBIPFPL** in every reasonable way to help SBIPFPL to regain possession of the Confidential Information and/or Confidential Materials and prevent its further unauthorized use.
- (b) The Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at SBIPFPL's request, or at **SBIPFPL**'s option, certify destruction of the same.
- (c) The Receiving Party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information or Confidential Materials and that **SBIPFPL** shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

4. Miscellaneous

- (a) All Confidential Information and Confidential Materials are and shall remain the property of **SBIPFPL** or any affiliate thereof. By disclosing information to the Receiving Party, SBIPFPL and/or its affiliate(s) do not grant any express or implied right to the Receiving Party to or under any patents, copyrights, trademarks, or trade secret information.
- (b) Any software, product, service and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.
- (c) Terms of confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire products without use of other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by persons who have had access to the Confidential Information, including the ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.
- (d) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both Parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of **SBIPFPL**, its agents, or employees, but only by an instrument in writing signed by an authorized officer of **SBIPFPL**. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.
- (e) This Agreement shall be governed by and construed in accordance with the laws of India and shall be subject to the exclusive jurisdiction of the courts of Mumbai.
- (f) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the Parties, their successors and assigns.

- (g) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.
- (h) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.
- (i) In the event this Agreement (including any schedules, exhibits or attachments hereto) is signed in both the English language and in any another language, any conflict or inconsistency between the different language versions shall be resolved solely by reference to the English language version.

5. Arbitration

All the disputes in connection with this Agreement, the construction of any provision of this agreement or the rights, duties or liabilities of the parties hereto under this Agreement shall be amicably settled. However, in the event of any such disputes are not settled amicably between the Parties, reference shall be to three arbitrators. Each party shall appoint its Arbitrator and the two respective Arbitrators appointed by each party shall appoint a presiding Arbitrator to adjudicate the dispute, difference, claim, etc. between the parties. A Party wishing to refer a dispute to arbitration shall appoint its arbitrator and send notice of such appointment in writing to the other party requiring the other party to appoint its own arbitrator within 30 calendar days of that notice and stating that it will appoint its arbitrator as sole arbitrator unless the other party appoints its own arbitrator and gives notice that it has done so within the 30 days specified above. If the other party does not appoint its own arbitrator and give notice that it has done so within the 30 days specified, the Party referring a dispute to the arbitration may, without the requirement of any further prior notice to the other party, appoint its arbitrator as sole arbitrator and shall advise the other party accordingly. The award of such sole arbitrator shall be binding on both parties as if he had been appointed by agreement.

The arbitration will be held **in Mumbai, India** and will be conducted in the English language.

IN WITNESS WHERE OF, THE PARTIES HERE TO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED AS
OF THE DAY AND YEAR FIRST ABOVE WRITTEN

SIGNED AND DELIVERED)

For SBICAP Securities Limited)

)

in the presence of:)

)

1.)
 2.)
 SIGNED AND DELIVERED)
 For _____ Limited)
 in the presence of:)
 1.)
 2.)

 **

Key components Service Level Agreement (SLA)

- 24*7*365 dashboard availability to be ensured.
- Uptime should be >95%
- For every breach of **Service levels**, SBIPFPL may claim a penalty of 1 % of agreement value (calculated on daily basis) for every hour of breach of time. However, the aggregate of all such penalties shall not exceed 25 % of the overall charges paid by SBIPFPL for the said quarterly charges.
- Automatic generation of Daily report /Monthly report of analysis as recommended. Monthly report Information must be shared as stated above of getting validated information about the potential security threats/vulnerabilities new global security threats/zero day attacks in circulation to the designated SBIPFPL official and suggest suitable countermeasures to safeguard against such evolving threats/attacks along with the analysis. The advisories should be provided to customise SBIPFPL Infrastructure.
- **VALIDITY OF AGREEMENT:** The Agreement/ SLA will be valid for the period **of three years**. The Company reserves the right to terminate the Agreement as per the terms of RFP/ Agreement.