



REQUEST FOR PROPOSAL

FOR

SUPPLY/ PURCHASE, INSTALLATION CONFIGURATION,
COMMISSIONING TESTING AND SUPPORT/ SERVICE FOR
SIEM SOLUTION

STATE LIFE INSURANCE CORPORATION OF PAKISTAN

Name of the Respondent	
Address	
Telephone	
Fax	
Email	

State Life Insurance Corporation of Pakistan

Regional Procurement Department (RPD),

Health & Accidental Insurance (H&AI), Regional Office
3rd Floor, State Life Tower, Jinnah Avenue, Islamabad

Contact No: 051-9216344

1. Table of Contents

1. DEFINITIONS:.....	4
2. INTRODUCTION.....	4
3. VALIDITY OF PROPOSALS.....	5
4. RIGHT TO ACCEPT / REJECT PROPOSAL.....	5
5. FRAUD AND CORRUPTION.....	5
6. CLARIFICATIONS AND AMENDMENTS OF RFP DOCUMENT.....	5
6.1. RFP CLARIFICATIONS.....	5
6.2. AMENDMENTS IN RFP.....	5
7. PROCESS FOR HIRING OF SERVICES.....	6
8. MANDATORY CRITERIA.....	7
9. DISQUALIFICATIONS.....	8
10. REQUEST FOR PROPOSAL.....	8
11. PREPARATION OF PROPOSAL.....	9
12. LIST OF DOCUMENTS SUBMITTED AS PART OF PROPOSAL.....	9
12.1. TECHNICAL PROPOSAL.....	9
12.2. FINANCIAL PROPOSAL.....	10
13. EVALUATION OF PROPOSALS.....	10
14. EVALUATION OF TECHNICAL PROPOSAL.....	11
15. EVALUATION OF FINANCIAL PROPOSAL.....	12
16. DETERMINATION OF MOST ADVANTAGEOUS BIDDER.....	13
17. BID SECURITY DEPOSIT.....	13
17.1. RELEASE OF BID SECURITY.....	13
17.2. CONFISCATION OF BID SECURITY:.....	14
18. BANK GUARANTEE.....	14
18.1. RELEASE OF BANK GUARANTEE:.....	14
18.2. CONFISCATION OF BANK GUARANTEE:.....	14
19. PENALTY.....	15
20. CONFIDENTIALITY.....	15
21. OWNERSHIP OF “DATA/INFORMATION”.....	16
22. DURATION:.....	16
1. BACKGROUND.....	17
2. GOAL.....	17

3. PLACE OF EXECUTION OF ASSIGNMENT	17
4. GENERAL INSTRUCTIONS FOR VENDORS:.....	17
5. EXECUTION TIMELINE:.....	18
6. SCOPE OF WORK:	18
6.1. TECHNICAL SPECIFICATIONS	19
7. PAYMENT SCHEDULE:.....	23
7.1. Payment Schedule for Component A	24
FIN- 1: FINANCIAL PROPOSAL	25
ANNEX-A:	26
Covering Letter	26
Annex-B:.....	28
Proposed Specifications and Recommended Brand.....	28
ANNEX-C:	29
QUOTED PRODUCT DETAILS	29
ANNEX-D	30
BANK GUARANTEE	30
ANNEX-E.....	31
MANDATORY SIEM TRAINING	31
ANNEX-F: DRAFT AGREEMENT.....	34

Section I: Invitation for Proposal

1. State Life Insurance Corporation of Pakistan intends to hire the services of a reputed Service Provider for subject procurement
2. State Life Insurance Corporation (hereinafter referred to as “the Purchaser”) is seeking proposals as per Single Stage Two Envelope Procedure as per PPRA Rules 2004 from Services Providers (hereinafter referred as “the Contractor”) registered with the Sales Tax and Income Tax departments
3. State Life reserves the right to accept or reject any proposal, and to annul the proposal process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected Respondent(s) or any obligation to inform the affected Respondent(s) of the grounds for such decision as per PPRA rules
4. All proposals must be valid for **One Hundred and Twenty (120)** days and any bid shorter than subject bid validity will be declared as conditional and will be declared non-responsive

5. Tender Schedule

A	Bid Submission Timeline Through EPADs	26/02/2026 @ 11:00 AM
B	Bid Opening Timeline	26/02/2026 @11:30 AM
C	Clarification Timeline	23/02/2026 UPTO 05:00 PM

5. Address for submission of Hard Copy of Bid Security amounting to **PKR. 170,000/-** in favor of “**SLIC H&AI PREMIUM COLLECTION ACCOUNT**” in the form of pay order/ demand draft and any other document if needed:

“Office of Regional Procurement Department (RPD), Health and Accidental Insurance (H&AI) Regional Office, 3rd Floor, State Life Tower, Jinnah Avenue, Islamabad”

Contact No: 051-9216344

Email for clarity and information regarding general conditions:

masabslic@gmail.com ; mwaqas.slic09@gmail.com

Email for Technical Clarification:

sys.architect.health@statelife.com.pk; dba.health.isb@statelife.com.pk

Section II: Instruction to Respondents

1. DEFINITIONS:

Unless the context otherwise requires, the following terms whenever used in this RFP and contract have the following meanings:

- a) “Proposals” means the Technical & Financial Proposals submitted by respondents in response to this RFP issued by State Life for “Supply/ Purchase, Installation Configuration, Commissioning Testing and Support/ Service for SIEM Solution” through EPADs.
- b) “State Life” means State Life Insurance Corporation of Pakistan.
- c) “SIEM” means Security Information and Event Management
- d) “Procuring Agency” means State Life Insurance Corporation of Pakistan
- e) “H&AI” Health and Accidental Insurance, Regional Office, Islamabad
- f) “Service Provider/ Bidder/ Vendor” means any entity that furnishes proposal in response to this RFP through EPADs
- g) “Competent Authority” means the CEO State Life
- h) “RFP” means Request for Proposal
- i) “RPC” means Regional Procurement Committee constituted by State Life for evaluation of proposal
- j) “Solution” corresponds to **SIEM Solution** as mentioned in Scope of Work
- k) “Government” means the Government of Pakistan
- l) “PPRA Rules” Public Procurement Rules 2004
- m) “SOW” means Scope of Work
- n) “EPADs” stands for E-Pak Acquisition and Disposal System
- o) “Service/ Support Charges” means the annual lump sum cost of support services that will be provided after complete deployment of SIEM Solution.

2. INTRODUCTION

State Life is undertaking Sehat Sahulat Program for provision of indoor medical services to the population in social sector. State Life has also launched Corporate Health Insurance initiative and different products are being offered both in Public and Private Sector

IT Department is actively engaged in development of different software applications. Further State of the art Data Center has also been set up at H&AI Regional Office, 3rd Floor, State Life Tower, Jinnah Avenue, Islamabad to cater technological requirements of the Corporation

3. VALIDITY OF PROPOSALS

Proposals must be valid for a period of **One Hundred and Twenty (120) days** after the date of its submission prescribed in RFP. A proposal valid for shorter period will be declared as non-responsive. State Life may solicit the Respondents' consent to extend proposal validity (without modification in proposals).

4. RIGHT TO ACCEPT / REJECT PROPOSAL

State Life reserves the right to accept or reject any proposal, and to annul the proposal process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected Respondent(s) or any obligation to inform the affected Respondent(s) of the grounds for such decision as per PPRA rules.

5. FRAUD AND CORRUPTION

State Life requires that respondents hired through this RFP must observe the highest standards of ethics. Further, case any bidder is found indulged in Corrupt and Fraudulent practice as defined under definition section in PPRA Rules then necessary action as per PPRA Rule-19 (A) will be taken

6. CLARIFICATIONS AND AMENDMENTS OF RFP DOCUMENT

6.1. RFP CLARIFICATIONS

During technical evaluation of the proposals, State Life may, at its discretion, ask Respondents for clarifications on their proposals in writing and response thereof must also be in writing. The Respondents are required to respond within the time frame prescribed by State Life.

In case a vendor fails to respond to clarification in stipulated time then vendor will be simply disqualified from further proceedings without any notice

6.2. AMENDMENTS IN RFP

At any time prior to deadline for submission of proposal, State Life may, for any reason, modify the RFP and revised documents will be advertised in the form of addendum in a manner like advertised earlier

7. PROCESS FOR HIRING OF SERVICES

This enquiry is Request for proposal (RFP) intended to result in the hiring of service provider for subject procurement. The responses received pursuant to this RFP will be evaluated as per the criteria specified in this document and the most advantageous bidder will be required to sign an agreement with State Life which would specify the assignment that the selected respondent is expected to perform. Evaluation of the proposals shall be carried out in two steps, first the technical and then the financial.

The technical and financial proposals shall be submitted at the same time on EPADs and any proposal or part of proposal received after the Bid Submission timeline shall be returned unopened and bid won't be considered as part of formal procurement process. No amendment to the technical or financial proposal after submission on EPADs.

First the technical proposals will be opened and evaluated in conformity with the provisions of the RFP. The Evaluation Committee shall not have access to the financial proposals until the technical evaluation is concluded. Financial proposals shall be opened only thereafter.

After completion of evaluation of the technical proposal, State Life shall upload **Technical Evaluation Report** as per **PPRA Rule-35** on EPADs, State Life and PPRA Website

The respondents who are found technically responsive based on technical evaluation would be informed about the date and time of opening of their financial proposals through EPADs and letter, Fax or E-mail as communicated by the respondents in their proposals.

Subject to scrutiny of Financial Proposal, the Final Evaluation Report will be published on EPADs, PPRA and State Life Website and after completion of necessary timeline, an agreement with most advantageous bidder will be signed (Copy of Draft Agreement is enclosed herewith at Annex-F). The said agreement will remain intact during configuration, installation, commissioning and testing of SIEM Solution. After completion of said deliverable a separate Service Level Agreement (SLA) for support services will be executed with most advantageous bidder based upon mutually agreed terms

8. MANDATORY CRITERIA

Eligible Service Provider/Respondent must fulfill following criteria:

- i. All Proposals must be furnished on EPADs and proposal submitted by any mode other than EPADs won't be accepted
- ii. Must have relevant business experience of at least Two (2) years (Here relevant Work Awards, Purchase Orders, Agreement etc must be affixed wherein experience of at least two (2) years is clearly visible)
- iii. A Pre-Bid Session will be held on **19-02-2026 @11:00 AM** and attending said session is must. Only those bidders' proposal will be accepted who will attend Pre-Bid Session. In case a bidder can't attend pre-bid session physically he/she must send a formal request via email for online session at least two (2) days prior to scheduled Pre-Bid session timeline
- iv. Must be registered with Tax Authorities as per prevailing latest tax rules (Only those companies which are validly registered with Government legal entities, sales tax and income tax departments) and on active taxpayer list.
- v. Has not been blacklisted by any of Provincial or Federal Government Department, Agency, Organization or autonomous body or Private Sector Organization anywhere in Pakistan (Submission of undertaking on legal stamp paper of worth Rs.100/- (**One Hundred Rupees Only**/-) duly authorized by Notary Public is mandatory);
The said affidavit must be uploaded on EPADs along with **technical proposal** as scanned copy. Further hard copy of the said affidavit must be furnished along with hard copy of Bid Security well before Bid Submission Timeline at the address appended at Serial No v below
- vi. Bid Security amounting to **PKR 170,000/-** in the form of Pay order/ Bank Draft in favor of "SLIC H&AI PREMIUM COLLECTION ACCOUNT" must be submitted as scanned copy with technical proposal on EPADs and hard copy must reach to the office of undersigned well before Bid Submission Timeline:

"Office of Regional Procurement Department (RPD), Health and Accidental Insurance (H&AI), Regional Office, 3rd Floor, State Life Tower, Jinnah Avenue, Islamabad"
- vii. Vendor must have Local Offices in large cities such Lahore, Karachi, Islamabad (Relevant Proof is needed here)
- viii. Must obtain minimum weightage average score of **50** points in Technical Evaluation

- ix. Submission of details as per Annexures (Annex-A to Annex-E)

NOTE: Compliance with all above clauses is mandatory and in case of non-compliance proposal will be declared as non-responsive.

9. DISQUALIFICATIONS

State Life may at its sole discretion and at any time during the evaluation of proposal, disqualify any Respondent, if the Respondent has:

- i. Submitted the proposal document or any other associated document after the Bid Submission deadline
- ii. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements
- iii. Submitted a proposal that is not accompanied by required documentation as per RFP
- iv. Failed to provide clarifications related thereto, when sought
- v. Submitted a proposal with price adjustment / variation provision
- vi. Required documentation not affixed with Technical and Financial Proposal
- vii. Any violation/missing information as required in Clause-08 above
- viii. Any violation of PPRA Rules-2004

10. REQUEST FOR PROPOSAL

The Respondent is expected to examine all the instructions, guidelines, terms and conditions and formats in the RFP. Failure to furnish all the necessary information as required by the RFP on submission of a proposal not substantially responsive to all the aspects of the RFP, shall be at Respondent's own risk and will be liable for rejection. When Respondents receive the RFP, and if they can meet the requirements of the RFP and the commercial and contractual conditions, they should make arrangements necessary to prepare a responsive proposal

If the Respondents find in the RFP documents - especially in the selection procedure and evaluation criteria – any ambiguity, omission or internal contradiction, or any feature that is unclear or that appears discriminatory or restrictive, they should seek clarification from State Life well in advance through an official email or EPADs. Email for clarification can be sent on email addresses as mentioned in tender notice. However, no relaxation or exemption shall be provided to the respondent on any term or condition of the RFP for reasons of non-receipt of any clarification.

Respondents/Service Providers should ensure that they submit a fully responsive proposal including all the supporting documents requested in the RFP is furnished on EPADs

11. PREPARATION OF PROPOSAL

The Respondent shall comply with the following during preparation of the proposal:

- i. The proposal and all associated correspondence shall be written in English and shall conform to prescribed formats. Any interlineations, erasures or overwriting shall be valid only if they are initialized by the authorized person signing the proposal
- ii. The proposal shall be typed and shall be signed by the Respondent or duly authorized person(s) to bind the Respondent to the contract. The letter of authorization shall be indicated by written power of attorney or authority letter and shall accompany the proposal.
- iii. Proposals received by any means other than EPADs will be declared non-responsive and will be rejected
- iv. All expenses related to participation in this tender document shall be borne by the respondents
- v. Respondents are not permitted to modify, substitute, or withdraw proposals after its submission
- vi. All the pages of the proposals should be signed by the authorized person(s) and should conform strictly to the formats and procedures laid down in this RFP
- vii. All proposals must be furnished as per Single Stage Two Envelop Procedure

12. LIST OF DOCUMENTS SUBMITTED AS PART OF PROPOSAL

12.1. TECHNICAL PROPOSAL

- i. Cover letter on respondent's official letter (format is attached as Annex-A)
- ii. Verifiable information of number of clients served on official letterhead duly signed and stamped
- iii. Complete HR Details on official letterhead duly signed and stamped. SIEM Certification of HR will be an added advantage
- iv. Provide details of similar projects completed with minimum overall value of at least **4.0 million** in last three

- (3) years. Here completed project means a single assignment, project that is completed before Bid Submission Timeline. Verifiable proof such as Work Completion Certificate or any other relevant document must be affixed
- v. All relevant proofs as requested in Mandatory Criteria--
-Clause-8
 - vi. Complete details of quoted solution as per format placed at Annex-C
 - vii. Bank Statement for the period January 01, 2025, to December 31, 2025, which must exhibit sound financial strength
 - viii. Signed and stamped RFP Document

All the above papers should be duly signed by the authorized signatory.

12.2. FINANCIAL PROPOSAL

- i. The financial proposal must be as per format placed at FIN-1 and in case proposal is not as per attached format it will be declared as non-responsive
- ii. All rates will be quoted in Pakistan Rupee (rounded to the rupee amount).
- iii. The quoted cost must be inclusive of supply, configuration and installation cost of SIEM Solution and support cost both quoted separately
- iv. The supply, configuration and installation cost of SIEM Solution will be a fixed cost
- v. Support Cost will be a recurring cost which will be charged on quarterly basis
- vi. Further overall lump sum cost will be considered for evaluation
- vii. In case of any discrepancy/confusion/ difference between the financial proposal quoted in figures and in words, the proposal mentioned in the form of words would be considered as final and would prevail.

13. EVALUATION OF PROPOSALS

State Life will form RPC to evaluate the proposals

- i. During evaluation of technical proposals, the Committee, may, at its discretion, ask the Respondents for clarification of their proposals. However, such clarification would not effectuate any change in the substance of the proposal.

- ii. After the technical evaluation the Technical Evaluation Report will be published as per PPRA Rule-35 on EPADs, PPRA and State Life Website. After uploading of Technical Evaluation Report, technically responsive bidders will be intimated through EPADs and other means of correspondence about opening of Financial Proposal
- iii. Bidders who are not found technically responsive will also be intimated via letter regarding the overall status and they will be required to collect Bid Security furnished without opening their financial proposal
- iv. The committee would undertake the financial evaluation of proposals of bidder/bidders found technically responsive and in case any clarity is required it will be taken in writing and after detailed evaluation, Final Evaluation Report as per PPRA Rules will be published on EPADs, PPRA and State Life Website

14. EVALUATION OF TECHNICAL PROPOSAL

The committee will evaluate the technical proposals based on given qualification parameters. The technical scoring will be done as per following criteria and formula for technical weightage is appended below:

S.No	Evaluation Criteria	Detailed Requirements	FC	NC
1	Advanced Search & Raw Log Access	Real-time & historical search, raw log access, complex queries (time-based, boolean, regex)	2.5	0
2	Agent Management & Telemetry	Centralized agent inventory, health monitoring, remote deployment, agent grouping, asset metadata visibility	5	0
3	Alert & Rule Tuning	Event ID tuning, rule customization, threshold tuning, centralized rule distribution, rule performance dashboards	5	0
4	Data Retention & Backup	Configurable retention per source, automated & manual backups, secure restore mechanism	5	0
5	User Management & Access Control	RBAC, user groups, MFA/2FA integration, audit trail of user/admin actions	5	0
6	Dashboard & Reporting	Custom dashboards, role-based views, compliance reports, CSV/PDF export, scheduled & on-demand reports, geo/MAP visualization	5	0
7	Threat Intelligence & Feeds	Geo-IP enrichment, AbuseIPDB, VirusTotal, MISP, MITRE ATT&CK mapping, IOC scoring, APT context, IOC lookup	5	0
8	Notification & Alerting	Severity-based alerts, in-app, email, mobile alerts, Slack/Telegram or equivalent integration	5	0

9	Compliance Framework Coverage	ISO 27001, NIST, HIPAA, PCI-DSS, SOC 2, GDPR, CIS Benchmarks, UAE NESA, SAMA	5	0
10	Vulnerability Management Integration	Vulnerability ingestion, CVSS v3/v4 scoring, patch reports, SCA dashboards	5	0
11	Integration & Auto Discovery	Agentless integrations (firewall, router, PBX), auto-discovery, SAP ERP logs, SNMP, SMTP	5	0
12	UEBA & Machine Learning	UEBA baselining, ML-based anomaly detection, continuous learning	5	0
13	SOAR Integration / Adaptive Response	Automated playbooks, IF/THEN conditional workflows, SOAR or native automation	5	0
14	Application Performance Monitoring (APM)	Real-time app metrics, transaction tracing, baseline deviation alerts	5	0
15	Threat Hunting Workspace	Visual query builder, threat-specific filters, saved hunts, analyst collaboration	5	0
16	Insider Threat Behavioral Analytics	User behavior baselining, anomaly detection, peer-group analysis	5	0
17	Dynamic Risk Scoring per Asset	Real-time risk scoring, risk decay logic, asset risk tier tagging	5	0
18	Mobile App (Alerts & Dashboards)	Secure mobile dashboards, push notifications for critical alerts	2.5	0
19	Compliance Workflow Automation	Control tracking, automated reminders, audit readiness dashboards, evidence export	5	0
20	Real-Time Threat Feed Enrichment	IOC enrichment at ingestion, threat prioritization, malware/actor auto-tagging	5	0
21	Dynamic Asset Grouping	Metadata-based grouping, real-time updates, scoped alerting & policies	5	0
	Total Technical Score	Maximum Achievable Score	100	

Weightage for technical evaluation is 70% and will be calculated as per following formula:

$$(100 - (((\text{Highest Score} - \text{Marks Secured}) / \text{Highest Score}) * 100)) * 0.7$$

Weightage Average Technical Score will be considered as benchmark for evaluation and will contribute to declaration of most advantageous bidder

15. EVALUATION OF FINANCIAL PROPOSAL

Evaluation of Proposals found to be technically responsive will be carried out as per following procedure:

- A.** Compliance of Financial Proposal with required format i.e. FIN-1 will be checked. In case of non-compliance with the required format, the proposal will be declared as non-responsive
- B.** After ascertaining that proposal is as per format, we will check general computations, tax etc

Subject to above general checking, the financial evaluation will be done as per following formula

Assigning 30% Weightage, the formula is appended below:

$$(100 - ((\text{Quoted Cost in PKR} - \text{Lowest Cost in PKR}) / \text{Lowest Cost in PKR}) * 100) * 0.3$$

Weightage Average Score will contribute to declaration of most advantageous bidder

16. DETERMINATION OF MOST ADVANTAGEOUS BIDDER

Subject to Technical and Financial Evaluation most advantageous bidder will be decided as per following formula:

Most Advantageous Bidder= Weightage Average Technical Score (70% Weightage) + Weightage Average Financial Score (30%)

Bidder who will secure **highest marks** will be the most advantageous bidder

17. BID SECURITY DEPOSIT

Bid Security amounting to **PKR 170,000** must be furnished by the respondent in shape of Demand Draft/Pay order in favor of "SLIC H&AI PREMIUM COLLECTION ACCOUNT" as scanned copy along with technical proposal on EPADs.

Bid Security must also be submitted in hard copy well before Bid Submission Timeline at following address:

"Office of Regional Procurement Department (RPD), Health and Accidental Insurance (H&AI), 3rd Floor, State Life Tower, Jinnah Avenue, Islamabad"

It is entirely bidders' responsibility to ensure timely submission of Bid Security in hard copy without any liability to State Life. If a bidder fails to submit Bid Security before Bid Submission Timeline his/her proposal will be rejected no matter if it is uploaded on EPADs.

17.1. RELEASE OF BID SECURITY

- A.** Bid Security of bidders who aren't most advantageous will be released subject to completion of formal procurement proceedings i.e. conclusion of timeline post final evaluation report uploading on EPADs, PPRA and State Life Website as per PPRA Rules
- B.** Bid Security of Technically Non-Responsive Bidder will be released subject to completion of timeline post uploading of Technical Evaluation Report on PPRA

Website, EPADs and SLIC Website. Vendor will have to furnish a proper request duly signed and stamped addressed to Regional Procurement Department (RPD)

- C.** Bid Security of the most advantageous bidder will be returned after submission of Bank Guarantee as per Clause-18

A formal request must be furnished duly signed and stamped and addressed to Regional Procurement Department (RPD)

17.2. CONFISCATION OF BID SECURITY:

Bid Security will be confiscated in case of following:

- I.** Bid Security of most advantageous bidder will be forfeited in case of failure to submit Bank Guarantee as per Clause-18
- II.** In case bidder denies executing the assignment as per requirements outlined and in accordance with proposal furnished on EPADs. Further we will also resort to second most advantageous bidder and necessary legal action as per PPRA Rule-19 will be initiated

18. BANK GUARANTEE

Most advantageous bidder will be required to furnish Bank Guarantee amounting to **10%** of quoted cost (LUMP SUM) as per format placed at Annex-D within fifteen days of issuance of Work Order with validity of one year from the date of submission of Bank Guarantee. In case of failure to submit Bank Guarantee within stipulated timeline stated above, necessary action as per Clause-17.2 (I) will be initiated along with cancellation of Work Order

18.1. RELEASE OF BANK GUARANTEE:

Bank Guarantee will be released subject to successful completion of One (1) year support period. The said period will commence after complete installation, configuration, commissioning, testing and training of SIEM Solution at our Data Center. In this regard a successful installation certificate will be provided by IT Department.

18.2. CONFISCATION OF BANK GUARANTEE:

Bank Guarantee will be confiscated in case:

- A. Vendor is indulged in any practice as mentioned at Clause-5 of RFP
- B. Vendor doesn't successfully complete One (1) year support period
- C. Vendor is bound to resolve the issue within three (3) working days of initiation. In case of continuous failure to resolve the issue within stipulated timeline we may confiscate the Bank Guarantee
- D. In case of any breach of confidentiality clause (Refer Clause-20 appended below

19. PENALTY

Vendor is expected to remain professional and exercise highest standards of professionalism. In case most advantageous bidder doesn't comply with timeline we will impose penalty amounting to **0.1%** of overall invoiced amount (Refer Payment Schedule) for each day of delay which will be adjusted from respective stage of execution as per Payment Schedule appended in Scope of Work

20. CONFIDENTIALITY

Bidder understands and agrees that all materials and information marked and identified by STATE LIFE as 'Confidential' are valuable assets of STATE LIFE and are to be considered STATE LIFE 's proprietary information and property. Bidder will treat all confidential materials and information provided by STATE LIFE with the highest degree of care and necessary to ensure that unauthorized disclosure does not occur.

Bidder will not use or disclose any materials or information provided by STATE LIFE without STATE LIFE 's prior written approval. Bidder shall not be liable for disclosure or use of any materials or information provided by STATE LIFE or developed by Bidder which is:

- I. possessed by Bidder prior to receipt from STATE LIFE, other than through prior disclosure by STATE LIFE, as documented by Bidder's written records;
- II. published or available to the general public otherwise than through a breach of Confidentiality; or
- III. obtained by Bidder from a third party with a valid right to make such disclosure, provided that said

third party is not under a confidentiality obligation to STATE LIFE; or

IV. Developed independently by the bidder.

In the event that Bidder is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, Bidder shall promptly notify State Life and allow State Life a reasonable time to oppose such process before making disclosure.

Bidder understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause State Life irreparable harm, may leave STATE LIFE with no adequate remedy at law and State Life is entitled to seek to injunctive relief.

Nothing herein shall be construed as granting to either party any right or license under any copyrights, inventions, or patents now or hereafter owned or controlled by the other party.

The requirements of use and confidentiality set forth herein shall survive the expiration, termination or cancellation of this RFP.

21. OWNERSHIP OF “DATA/INFORMATION”

All information processed, stored, or transmitted by Service Provider’s equipment belongs to State Life. By having the responsibility to maintain the equipment, the Service Provider does not acquire implicit access rights to the information or rights to redistribute the information. The Service Provider understands that civil, criminal, or administrative penalties will apply for failure to protect information appropriately.

22. DURATION:

The initial engagement will be for a period of one year during which support will also be provided. After expiry of **one (1)** year term, the engagement can be extended for **two (2)** more years subject to requirement, mutual consent and satisfactory performance.

The extended engagement will generally be on same terms and conditions as per RFP and subsequently agreed terms with the most advantageous bidder in a Service Level Agreement.

Section III: Scope of Work

1. BACKGROUND

State Life Health Insurance is implementing Sehat Sahulat Program coverage to almost entire population all over Pakistan. As part of this program the patients are taking inpatient health services all over Pakistan.

State Life has also launched Corporate Health Insurance Program and different products are being offered to both Public and Private sector.

This Security Information and Event Management (SIEM) solution is intended to establish a centralized, scalable, and resilient security platform for the State Life Insurance Corporation of Pakistan – Health & Accidental Insurance (H&AI). The solution shall enable real-time monitoring, advanced threat detection, alerting, and automated incident response across SLIC's entire IT infrastructure. It will support SLIC in meeting its regulatory, compliance, and cybersecurity obligations, in alignment with both the organization's internal security framework and internationally recognized standards such as ISO/IEC 27001 and NIST SP 800-53.

2. GOAL

To ensure installation, configuration, customization and ongoing maintenance of the SIEM Solution.

3. PLACE OF EXECUTION OF ASSIGNMENT

The subject solution as required is to be installed at Data Center, Health and Accidental Insurance (H&AI) Regional Office, 3rd Floor, State Life Tower, Jinnah Avenue, Islamabad

4. GENERAL INSTRUCTIONS FOR VENDORS:

- A. Vendors must note that said assignment is to be executed on the 3rd Floor, therefore prior visit for better understanding must be conducted
- B. Vendor must quote a single solution with complete details
- C. Vendor must note that if he is found most advantageous, he is required to supply same solution as quoted and no request on this issue will be entertained

- D. Vendor must take extra caution while quoting the required solution and must take all allied factors into consideration
- E. Vendor must ensure strict adherence to all directions as communicated from time to time
- F. Most Advantageous Bidder must furnish complete details of relevant technical staff which will execute the subject assignment on official letterhead within seven days of issuance of Work Order

5. EXECUTION TIMELINE:

The execution timeline for the subject assignment is as follows:

A. Commissioning, Installation and Configuration of Solution at Data Center, Islamabad.

Most advantageous bidder will be required to ensure complete commissioning, installation, configuration and testing within thirty **(30)** days of issuance of Work Order

B. Training of H&AI Regional Office Team

The above-mentioned deliverable must be completed within fifteen days of complete deliverable A

C. Support Service:

Support Service will be required for a period of **One (1)** year from completion of deliverables at Serial No. A and Serial No. B

In case of non-compliance of any above timeline necessary penalty as per Clause-19 of Section-II of RFP will be imposed.

6. SCOPE OF WORK:

This Security Information and Event Management (SIEM) solution is intended to establish a centralized, scalable, and resilient security platform for the State Life Insurance Corporation of Pakistan – Health & Accidental Insurance (H&AI). The solution shall enable real-time monitoring, advanced threat detection, alerting, and automated incident response across SLIC's entire IT infrastructure. It will support SLIC in meeting its regulatory, compliance, and cybersecurity obligations, in alignment with both the organization's internal security framework and internationally recognized standards such as ISO/IEC 27001 and NIST SP 800-53.

The selected vendor shall be responsible for the installation, configuration, integration, customization, and ongoing maintenance of the SIEM solution. All activities must strictly comply with SLIC's data

privacy and information security policies and procedures, as revised from time to time.

The proposed SIEM solution shall have the following features:

1. Centralize Log Management:
2. Real-Time Threat Detection and Monitoring:
3. Compliance Reporting:
4. Incident Management and Response:
5. Integration Capabilities:
6. Dashboard and Visualization:
7. AI Features
8. User and Entity Behavior Analytics (UEBA):
9. High Availability and Scalability:
10. Data Protection and Privacy:
11. Training and Knowledge Transfer:
12. Licensing Model:
13. Deployment Model:
14. Red Team Detection Simulation Support
15. Business Continuity and Disaster Recovery Testing
16. Support Tier Structure and Escalation Workflow
17. Product Innovation and Roadmap Disclosure
18. Version Upgrades and Change Management
19. SIEM Expert Level Training

6.1. TECHNICAL SPECIFICATIONS

1. Architecture Requirements

- **Deployment Models**

The SIEM solution must support on-premises and hybrid deployments, with clear separation of data ingestion, processing, storage, and presentation layers.

- **Scalability**

- Horizontally scalable architecture capable of ingesting logs from thousands of sources without service interruption.
- Scale-out must be supported without re-architecture or license replacement.

- **High Availability (HA)**

Built-in redundancy and automatic failover for all critical components, including:

- Log collectors
- Correlation engine
- Storage
- User Interface / Dashboard

No single point of failure is acceptable.

- **Disaster Recovery (DR)**
 - Native support for backup, restore, failover, and failback.
 - DR implementation across Primary Site (Islamabad) and DR Site (Karachi).
 - DR testing must be demonstrated during UAT, including preservation of logs, alerts, dashboards, and correlation rules.

2. Log Collection and Ingestion

- **Supported Protocols**

Syslog (UDP/TCP/TLS), SNMP, WMI, REST API, Filebeat, Winlogbeat, Fluentd, and equivalent industry-standard collectors.
- **Collection Methods**
- Support both agent-based and agentless log collection.
- Agents must be lightweight and centrally manageable.
- **Supported Log Sources (minimum)**
 - **Operating Systems:** Windows, Linux, macOS, Android, iOS
 - **Network & Security Devices:**
 - Firewalls (Fortinet, Palo Alto, Juniper, Huawei)
 - Routers, switches, IoT devices
 - IDS/IPS, VPN, Web Proxy
 - **Identity & Endpoint:**
 - Active Directory / LDAP
 - Antivirus, EDR, Endpoint Protection
 - **Databases:** Oracle, MySQL, Microsoft SQL Server
 - **Cloud (optional):** AWS and Azure logs
- **Log Integrity & Time Accuracy**
 - Logs must be tamper-proof, protected by hashing or equivalent integrity controls.
 - All ingested logs must preserve original timestamps.
 - SIEM must support NTP synchronization to ensure consistent event correlation across systems.

3. Event Correlation and Analysis

- **Correlation Engine**
 - Advanced rule-based correlation combined with machine-learning-assisted analytics.
 - Correlation must work across multiple data sources and time windows.
- **Threat Intelligence Integration**
 - Integration with commercial and open-source threat intelligence feeds.
 - Support for custom IoC ingestion (IP, hash, domain, URL, email indicators).
 - IoCs must be usable in correlation rules without manual re-coding.

- **UEBA (User & Entity Behavior Analytics)**
 - Baseline normal behavior for users, systems, and service accounts.
 - Detect anomalies such as:
 - Privileged misuse
 - Lateral movement
 - Unusual login patterns
 - Insider threat indicators
- **MITRE ATT&CK Mapping**
 - Pre-configured and customizable detection rules aligned with MITRE ATT&CK tactics and techniques.
 - Alerts must clearly reference mapped ATT&CK techniques for investigation and reporting.

4. Alerting and Incident Handling

- **Alerting Mechanisms**
 - Real-time alerts via:
 - Dashboard
 - Email
 - SMS (or equivalent)
- **Alert Prioritization**
 - Alerts must be prioritized based on:
 - Severity
 - Risk score
 - Asset criticality
- **Incident Handling & Workflow**
 - Support alert acknowledgment, assignment, escalation, and closure.
 - Maintain full incident lifecycle history for audit purposes.
- **SOAR Integration**
 - Integration with SOAR platforms (optional but preferred).
 - At minimum, SIEM must support automated actions such as:
 - Ticket creation
 - Alert enrichment
 - Notification workflows
- **Playbooks**
 - Predefined incident response playbooks for common threats (e.g., brute force, malware, privilege abuse).
 - Playbooks must be customizable by administrators.

5. Dashboard and Reporting

- **Dashboards**
 - Fully customizable dashboards with role-based access for:
 - SOC analysts
 - IT operations

- Management
 - Audit & compliance teams
- **Reports (minimum)**
 - Compliance reports for:
 - ISO 27001
 - CTDISR
 - PCI-DSS
 - HIPAA (where applicable)
 - Executive-level summary reports for senior management and board.
- **Log Retention**
 - Online (hot/warm): Minimum 12 months
 - Archived (cold): Minimum 3 years
 - Retention periods must be configurable per log source.

6. Integration Capabilities

- **Identity Integration**
 - Active Directory / LDAP integration for user and role enrichment.
- **ITSM / Ticketing Integration**
 - Integration with helpdesk or ITSM platforms (e.g., ServiceNow, GLPI).
 - Alerts must be convertible into tickets automatically.
- **APIs**
 - REST APIs for:
 - External integrations
 - Automation
 - Data export

7. Security and Compliance

- **Encryption**
 - In-transit: TLS 1.2 or higher
 - At-rest: AES-256 or equivalent
- **Access Control**
 - Role-Based Access Control (RBAC)
 - Multi-Factor Authentication (MFA) for administrative access
- **Audit Logging**
 - Full audit trail of:
 - User logins
 - Configuration changes
 - Rule modifications
 - Administrative actions
- **Data Privacy**
 - Support for field-level masking of sensitive or personal data.
 - Ensure compliance with internal data protection policies.

8. Performance Requirements

- **EPS Capacity:** Minimum 1000 Events per Second (EPS), scalable to 20,000+ EPS.
- **Search Performance:** Query time under 5 seconds for 30-day log data.
- **Retention:** Hot and warm data access for at least 90 days.

9. Mobile App Access

- **Capability:** Mobile alerting & dashboards — especially for 24x7 SOC teams.

10. Licensing and Support

- **Licensing:** Transparent and scalable licensing tiers.
- **Support Services:**
 - 24x7 support availability.
 - SLA-backed incident response time.
 - Local support team presence (mandatory).
- **Maintenance:**
 - Periodic patching and updates.
 - Health check services (monthly or quarterly).

11. Documentation and Training

- **Complete and up-to-date:**
 - User manuals
 - Administrator manuals
 - Architecture and deployment documentation
- **Training Requirements (Annex-F for full detail)**
 - SIEM architecture and internal data flow
 - Advanced correlation logic and detection engineering
 - Threat hunting and investigation workflows
 - Performance tuning and false-positive reduction
 - Incident response and forensic analysis using SIEM
- **Certification**
 - Vendor must provide training completion certificates.

12. SIEM Hardware

- The Vendor may provide the required hardware.

7. PAYMENT SCHEDULE:

The payment schedule for the subject procurement will basically comprise two components:

- A. Payment Schedule for Installation, Configuration, Commissioning and Testing**

B. Payment Schedule for Support

7.1. PAYMENT SCHEDULE FOR COMPONENT A

The payment schedule for this component is as follows:

Sr. No	Particular	Amount to be Paid	Remarks
01.	Installation Configuration and integration of SIEM Solution.	40% of remaining amount will be paid	Deductions if any as per Clause-19: Section-II will be made
02.	Customized Dashboard and Reporting Modules, Successful testing and resolution of issues.	40% of remaining amount will be paid	Deductions if any will be made as per Clause-19, Section-II will be made
03.	Comprehensive Expert Level Training sessions on the SIEM Solution by the Certified SIEM Experts	20% of remaining amount will be paid	Deductions if any will be made as per Clause-19, Section-II will be made

The above timeline must be followed, and invoices must be done accordingly. No payment out of turn under any circumstances will be made

7.2. PAYMENT SCHEDULE FOR COMPONENT B

In this case payment will be made on quarterly basis, i.e. quarter to comprise of three months' period. Vendor will have to submit invoices after completion of respective quarters. Vendor must submit all relevant documentation and subject to satisfactory report by concerned department payment will be made.

General Conditions for payment are as follows:

- I. All invoices must be in PKR
- II. Invoices must be as per approved rates
- III. Invoice must be furnished along with Bank Details, Tax record and Work Completion Report
- IV. Invoice will be subject to work done satisfactory
- V. Invoice will be subject to deductions if any as per Clause-19
- VI. Invoice will be cleared within Thirty (30) days subject to completion of all codal formalities

FIN- 1: FINANCIAL PROPOSAL

SR No	DESCRIPTION	A QUANTITY	B QUOTED COST IN PKR WITHOUT TAX	QUOTED PRODUCT (COMPLETE MODEL WITH SPECIFICATIONS AND ACCESSORIES)	APPLICABLE TAX IN PKR	C QUOTED COST IN PKR INCL. TAXES	TOTAL FINANCIAL IMPACT IN PKR $D=C*A$
1	Supply, Installation, Commissioning Configuration, Testing and Training of SIEM Solution in PKR (For specifications refer Annex-B)	SINGLE JOB					
2	Support/ Service Charges Annual in PKR	ANNUAL COST					
3	Any Other Accessories (Optional) in PKR	LUMP SUM					
TOTAL FINANCIAL IMPACT IN PKR IN FIGURES							
TOTAL FINANCIAL IMPACT IN PKR IN WORDS							

- I. ALL ENTRIES MUST BE FILLED
- II. CUTTING/OVERWRITING ISN'T ALLOWED
- III. QUOTED COST MUST BE INCLUSIVE OF ALL APPLICABLE TAXES AND OTHER CHARGES IF ANY
- IV. VENDOR MUST ENSURE THAT CALCULATIONS ARE PROPERLY DONE WITHOUT ANY ERROR. IN CASE ANY CALCULATION MISTAKE IS FOUND, PROPOSAL WILL BE REJECTED
- V. FINANCIAL PROPOSAL MUST BE STRICTLY AS PER ABOVE FORMAT
- VI. SOLUTION MUST BE CLEARLY SPECIFIED WITHOUT ANY OR CONDITION OTHERWISE PROPOSAL WILL BE DECLARED AS NON-RESPONSIVE
- VII. SUPPORT/ SERVICE CHARGES AS PER SERIAL NO.02 ABOVE MUST BE QUOTED FOR ONE YEAR (ANNUAL COST)
- VIII. COST AT SERIAL NO.03 ABOVE IS OPTIONAL AND MUST BE QUOTED AS LUMP SUM BASIS. COST AT SERIAL NO.03 IS A FIXED COST
- IX. PROPOSAL MUST BE SIGNED AND STAMPED
- X. TOTAL FINANCIAL IMPACT IN PKR. WILL BE CONSIDERED FOR EVALUATION

ANNEX-A: Covering Letter

(On Respondent's letterhead)

Date: _____

Proposal Reference No. xx/2026

Incharge HR & Admin/ RPD

State Life Insurance Corporation of Pakistan,
Health & Accident Insurance Regional Office, 3rd Floor, State Life Tower,
Jinnah Avenue, Islamabad
Contact No: 051-9216344

SUBJECT: SUPPLY, INSTALLATION CONFIGURATION, COMMISSIONING AND TESTING OF SIEM SOLUTION

Dear Sir,

1. Having examined the RFP, we / I, the undersigned, offer to submit a proposal for the Hiring of Services for activities to be undertaken under RFP, in full conformity with the said RFP.
2. We / I have read the terms and conditions of RFP and confirm that these are acceptable to us. We further declare that additional conditions, variations, deviations, if any, found in our proposal shall not be given effect to.
3. We / I agree to abide by this proposal, consisting of this letter, technical and financial proposal and all attachments, for a period of 120 days from the date fixed for submission of proposal as stipulated in the RFP.
4. Until the formal agreement is prepared and executed between the parties, this proposal, together with your written acceptance of the proposal and your notification of award, shall constitute a binding agreement between us.
5. We / I hereby declare that all the information and statements made in this proposal are true, correct and acceptable. Any misinterpretation contained in it may lead to our disqualification.
6. We / I understand State Life is not bound to accept any proposal it receive.
7. We / I confirm that our authorized representative has signed all pages of this proposal as acceptance of all conditions of RFP. All documents attached along with our proposals have also been signed by our authorized representative as an attestation of their authenticity. The financial proposal has been prepared separately as desired and duly signed.
8. We / I am submitting herewith a demand draft/Pay Order No. _____ dated _____ drawn from ----- in favor of "SLIC H&AI PREMIUM COLLECTION ACCOUNT" as Bid Security Deposit for consideration of our proposals is attached as scanned copy with technical proposal on EPADs and also furnished in hard copy to Regional Procurement Department

9. The letter of authorization by the competent authority is also attached herewith.
10. We / I undertake to engage eligible experts/ skilled workers as per requirements outline in SOW

Dated [date / month / year]

Authorized Signatory (in full and initials):

Name and title of signatory:

Duly authorized to sign this proposal for and on behalf of [Name of Respondent]

Name & Address of Firm

Affix rubber stamp

Email/Fax No.

Income Tax Certificate

Return Submitted

Annex-B: Proposed Specifications and Recommended Brand

Category	Specification
Advanced Search & Raw Log Access	Real-time & historical search, raw log access, complex queries (time-based, boolean, regex)
Agent Management & Telemetry	Centralized agent inventory, health monitoring, remote deployment, agent grouping, asset metadata visibility
Alert & Rule Tuning	Event ID tuning, rule customization, threshold tuning, centralized rule distribution, rule performance dashboards
Data Retention & Backup	Configurable retention per source, automated & manual backups, secure restore mechanism
User Management & Access Control	RBAC, user groups, MFA/2FA integration, audit trail of user/admin actions
Dashboard & Reporting	Custom dashboards, role-based views, compliance reports, CSV/PDF export, scheduled & on-demand reports, geo/MAP visualization
Threat Intelligence & Feeds	Geo-IP enrichment, AbuselPDB, VirusTotal, MISP, MITRE ATT&CK mapping, IOC scoring, APT context, IOC lookup
Notification & Alerting	Severity-based alerts, in-app, email, mobile alerts, Slack/Telegram or equivalent integration
Compliance Framework Coverage	ISO 27001, NIST, HIPAA, PCI-DSS, SOC 2, GDPR, CIS Benchmarks, UAE NESA, SAMA
Vulnerability Management Integration	Vulnerability ingestion, CVSS v3/v4 scoring, patch reports, SCA dashboards
Integration & Auto Discovery	Agentless integrations (firewall, router, PBX), auto-discovery, SAP ERP logs, SNMP, SMTP
UEBA & Machine Learning	UEBA baselining, ML-based anomaly detection, continuous learning
SOAR Integration / Adaptive Response	Automated playbooks, IF/THEN conditional workflows, SOAR or native automation
Application Performance Monitoring (APM)	Real-time app metrics, transaction tracing, baseline deviation alerts
Threat Hunting Workspace	Visual query builder, threat-specific filters, saved hunts, analyst collaboration
Insider Threat Behavioral Analytics	User behavior baselining, anomaly detection, peer-group analysis
Dynamic Risk Scoring per Asset	Real-time risk scoring, risk decay logic, asset risk tier tagging
Mobile App (Alerts & Dashboards)	Secure mobile dashboards, push notifications for critical alerts
Compliance Workflow Automation	Control tracking, automated reminders, audit readiness dashboards, evidence export
Real-Time Threat Feed Enrichment	IOC enrichment at ingestion, threat prioritization, malware/actor auto-tagging
Dynamic Asset Grouping	Metadata-based grouping, real-time updates, scoped alerting & policies

Note:

- i. Above cited specifications are basically a benchmark/ reference point for vendor
- ii. Vendor (s) must meet above requirements and may exceed as well

ANNEX-C: QUOTED PRODUCT DETAILS

Category	Specification
Advanced Search & Raw Log Access	
Agent Management & Telemetry	
Alert & Rule Tuning	
Data Retention & Backup	
User Management & Access Control	
Dashboard & Reporting	
Threat Intelligence & Feeds	
Notification & Alerting	
Compliance Framework Coverage	
Vulnerability Management Integration	
Integration & Auto Discovery	
UEBA & Machine Learning	
SOAR Integration / Adaptive Response	
Application Performance Monitoring (APM)	
Threat Hunting Workspace	
Insider Threat Behavioral Analytics	
Dynamic Risk Scoring per Asset	
Mobile App (Alerts & Dashboards)	
Compliance Workflow Automation	
Real-Time Threat Feed Enrichment	
Dynamic Asset Grouping	

- a. All entries must be filled
- b. No Overwriting/cutting is allowed and if done must be signed properly
- c. The said proforma must be signed and stamped
- d. Must be affixed with Technical Proposal on EPADs
- e. A single solution must be quoted without an OR condition

ANNEX-D

BANK GUARANTEE

**State Life Insurance Corporation of Pakistan,
State Life Building No. 9, Dr. Zia Uddin Road, Karachi,
P A K I S T A N.**

Dear Sir,

Ref: Our Bank Guarantee No. _____ in the sum of
_____ Account _____ Amount of
Contract _____
In consideration of you having entered into contract No. _____
Dated _____
with _____ called Vendor and in consideration of value
received from VENDOR, we hereby agree and undertake as follows:

1. To make unconditional and immediate payment to you as called upon of **10%** of the **total bid amount/ quoted price** in Pak Rupees on your first written demand without further recourse, question, deferment, contestation or reference to VENDOR or any other person, in the event of default, non-performance or non-fulfillment by VENDOR of his obligations liabilities, responsibilities under the said Contract of which you shall be the sole and absolute judge.
2. To accept written intimation from you as conclusive and sufficient evidence of existence of a default or breach as aforesaid on the part of VENDOR and to make payment immediately upon receipt thereof.
3. To keep this Guarantee in full force from the date hereof until completion of project from the date of contract execution.
4. That no grant of time or other indulgence to, amendment in the terms of the contract by Agreement between the parties, or imposition of Agreement with Vendor in respect of the performance of his obligation under and in pursuance of the said Agreement with or without notice to us, shall in any manner discharge or otherwise affect this Guarantee and our liabilities and commitments there under.
5. This Guarantee shall be binding on us and our successor's interest and shall be irrevocable.
6. This Guarantee shall not be affected by any change in the constitution of the Guarantor Bank or the constitution of the Contractor.

Authorized Sign for Issuing Bank

Seal of the Bank

ANNEX-E

MANDATORY SIEM TRAINING

- **A. SIEM Architecture & Internals**
 - Component architecture (collectors, parsers, correlation engine, storage)
 - EPS optimization and ingestion bottlenecks
 - High availability and DR architecture
 - Log parsing, normalization, and enrichment internals
- **B. Advanced Correlation & Detection Engineering**
 - Writing advanced correlation rules (multi-stage, time-based, chained events)
 - MITRE ATT&CK-aligned detection use cases
 - IOC-based and behavior-based detections
 - Rule versioning, lifecycle management, and performance tuning
 - False-positive reduction strategies
- **C. UEBA & Behavioral Analytics**
 - Behavior baseline creation
 - Insider threat detection use cases
 - Peer-group analysis
 - Anomaly confidence scoring
 - UEBA tuning and validation
- **D. Threat Intelligence Integration**
 - Ingesting multiple threat feeds
 - IOC confidence scoring and decay
 - Threat actor / malware family attribution
 - Enrichment workflows at ingestion and alert stages
- **E. Threat Hunting & Investigation**
 - Hypothesis-driven threat hunting
 - Visual and advanced query building
 - Pivoting across user, host, asset, and IOC context
 - Case creation and evidence preservation
 - Live attack simulation analysis (if available)
- **F. Incident Response & SOAR Integration**
 - Alert triage workflows
 - Incident lifecycle management
 - Automated and semi-automated response playbooks
 - Integration with ticketing / ITSM systems
 - Escalation and SLA enforcement
- **G. Compliance & Audit Use**
 - Mapping SIEM detections to ISO 27001, NIST, PCI-DSS
 - Audit-ready reporting

- Evidence extraction for compliance audits
- Log retention and legal hold scenarios
- **H. Performance, Health & Optimization**
 - EPS monitoring and capacity planning
 - Storage optimization
 - Search performance tuning
 - Platform health monitoring and troubleshooting
- **7. Hands-On Requirement (Mandatory)**
 - Minimum 60% of training time must be hands-on
 - Hands-on labs must include:
 - Rule creation and tuning
 - Alert investigation
 - Threat hunting exercises
 - Incident simulations
 - Labs must be conducted on:
 - SLIC environment **or**
 - Vendor-provided sandbox closely resembling SLIC architecture
- **8. Trainer Qualifications (Mandatory)**

Training must be delivered by a certified SIEM expert, meeting all of the following:

 - Vendor-certified Expert / Architect / Advanced Instructor
 - Minimum 5 years hands-on SIEM deployment & SOC experience
 - Experience delivering training to enterprise or government SOCs
 - Trainer CV must be submitted with bid
- **9. Training Materials & Deliverables**

Vendor must provide:

 - Detailed training agenda
 - Soft copy of:
 - Training slides
 - Lab manuals
 - Use-case documentation
 - Sample correlation rules
 - Post-training reference guides
 - Recorded sessions (if permitted by SLIC)
- **10. Training Evaluation & Certification**
 - Post-training knowledge assessment (quiz or practical)
 - Training completion certificates for all participants
 - Certificates must clearly state:
 - “SIEM Expert Level Training”
 - Product name
 - Duration
 - Trainer credentials
- **11. Knowledge Transfer & Sustainability**

Vendor must ensure:

- Full knowledge transfer to reduce vendor dependency
- Documentation of:
 - Custom rules
 - Dashboards
 - Use cases
- Minimum 30 days post-training support for:
 - Query assistance
 - Rule tuning guidance
 - Operational questions

12. Commercial Requirement

- Training cost must be included in the main commercial proposal
- No separate or optional pricing allowed
- Training shall be delivered within 60 days of SIEM go-live

13. Evaluation Impact (Recommended for RFP)

Failure to meet any mandatory training requirement may result in:

- Technical score reduction or
- Bid disqualification

ANNEX-F: DRAFT AGREEMENT

This AGREEMENT (hereinafter called the "Agreement") is made on this **[DATE]** , **2026** at
Karachi

Between

State Life Insurance Corporation of Pakistan, incorporated under the Life Insurance Nationalization Ordinance, 1972, having Principal Office at State Life Building No.9, Dr. Ziauddin Ahmed Road, Karachi (hereafter called the "**State Life**" which expression shall include the successors, legal representatives and permitted assigns) of the one part,

and

M/s [SERVICE PROVIDER] , head office at [ADDRESS]. (hereafter called the "**Service Provider**" which expression shall include the successors, legal representatives and permitted assigns) of the other part. [Procurement Title]

WHEREAS

The State Life has sought proposal from the Service Provider to provide services as defined in the Invitation of Proposal/Bid ((hereinafter called the "Services"); and the Service Provider, having represented to the State Life that they have the required professional skills, and personnel and technical resources, have agreed to provide the Services and submitted the proposal through EPAD

NOW THEREFORE the Parties hereby agree as follows:

1. The following documents attached hereto shall be deemed to form an integral part of this Agreement:
 - a. The Invitation of Proposal/Bid.
 - b. The Letter of Acceptance.
 - c. The complete Form of Proposal/Quotation/Bid submitted by the Service Provider on EPADs

2. The mutual rights and obligations of the State Life and the Service Provider shall be as set forth in the Agreement, in particular:
 - (a) The Service Provider shall carry out the Services in accordance with the provisions of the Agreement; and
 - (b) The State Life shall make payments to the Service Provider in accordance with the provisions of the Agreement.
 - (c) The discretion of acquiring Annual Support for the Developed & Designed Software and Maintenance thereof from the Service Provider shall rest with State Life. No cost/amount shall be paid to Service Provider if the State Life

does not acquire Annual Support from the Service Provider.

3. The Service Provider shall not sub-let the services to any other without prior written consent of the State Life.
4. In the event if the services were not provided as per timeline given in the Proposal/Quotation/Bid submitted by the Service Provider (11 pages in total) the State Life reserve the right to terminate the Agreement and to recover the amount/payment made to the Service Provider.
5. Any dispute if arisen shall amicably be settled.
6. The Service Provider shall indemnify and hold harmless the State Life from and against all liabilities, claims, litigations and demands, on account of fraud, injury, loss or damage in obtaining Domain Registration & Hosting etc.
7. If the Service Provider defaults or neglects to carry out the Services in accordance with the Agreement Documents or fails to perform any provision of the Agreement, the State Life may terminate Service Provider's Services under the Agreement and shall recover the amount so paid to the Service Provider.
8. In no event shall the State Life and Service Provider be responsible or liable for any failure or delay in the performance of its obligations hereunder arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, strikes, work stoppages, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, and interruptions, loss or malfunctions of utilities, communications or computer (software and hardware) services.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be signed in their respective names as of the day, month and year first above written

For and on behalf of State Life

For and on behalf of the service provider

Name:

Name:

Designation:

Designation:

Signature: -----

Signature: -----

WITNESS NO.1

Name:

Designation:

CNIC No:

Signature: -----

WITNESS NO.2

Name:

Designation:

CNIC No:

Signature: -----