REQUEST FOR PROPOSAL (RFP)

FOR

Security Information and Event Management (SIEM)

FOR

UBI Services Limited
504-506, 5th Floor, Centrum, S. G. Barve Road, Wagle Estate,
MIDC, Thane (W), Pin code – 400604.

BID FOR SUPPLY OF SIEM SOLUTIONS

Sr No.	Particulars	Page No.
1	Background	3
2	Requirements	3
3	Scope of Work	3
4	Eligibility Criteria (Technical & Commercial)	4-5
5	Bid Details in Brief	6
6	Empanelment Period and Terms	7
7	Bid Evaluation Criteria	8-9
8	Cloud SIEM Solutions (Managed Services) - Annexure A	10-12

1. BACKGROUND: -

UBI Services Limited (“UBISL” or “The Company”) is a wholly owned subsidiary of Union Bank of India (UBI) engaged in various activities that range from distribution of Retail Loan products & manpower solutions to the Parent Bank. The Company is a Corporate Selling Agent of Parent Bank and into distribution of various retail and other loan products mainly of Home Loan, Car Loan, Education Loan, and MSME Loan etc. The Company is also providing manpower solutions to various department / process of parent Banks like Centralized Vendor Payment Cell (CVPC), Core Banking Solutions (CBS) Helpdesk, Credit Compliance & Monitoring Cell (CMCC), etc.

2. REQUIREMENT:

UBI Services Limited (“UBISL” or “The Company”) invites quotations from suppliers (“Suppliers or Bidder”) from open market from Mumbai, Navi Mumbai and Thane Locations. Interested suppliers who deal in SIEM Solutions (Items as per **Annexure A**) related materials or work and meeting the eligibility criteria shall respond to these bid documents. Suppliers shall be selected based on technical scrutiny followed by Financial Bid.

3. SCOPE OF WORK:

The selected Bidder shall supply SIEM Solutions based on below Requirement as mentioned.

Monitoring Device Types	Qty
Windows Servers	4
Microsoft Hyper-V Server	7
MySQL Database	1
Microsoft Azure Instances	1
Managed Switches	2

Firewall	2
Network IPS/IDS	1
Network VPN / SSL VPN	1
Email Servers (Exchange, Send mail, BES, IMAP, etc)	2
Antivirus / DLP Server *	2
DLP/EDR/XDR	1
Wi-Fi Devices	4
NAS Storage	3
WAF	2
MDM	1
Laptop / Desktop	250

4. ELIGIBILITY CRITERIA:

Only those Bidders who fulfill the following criteria are eligible to respond to the RFP document. Offers received from the bidders who do not fulfill following criteria are considered as ineligible bidder.

(a) TECHNICAL BID:

S No.	Eligibility Criteria	Documents Required
1	Bidder must be legally registered entity i.e. Registered Firm / Limited Liability Partnership / Registered Domestic Company	Registration certificate issued by Registrar of Firms / Ministry of Corporate Affairs etc. Also Shop & Establishment License issued by local authority.
2	Valid / Active Shop & Establishment, PAN and GST registration numbers	Self-certified S&E Certificate, PAN and GST copies
3	Annual Turnover of Rs. 1.5 Cr. for the last three financial years i.e. FY 2021-22, 2022-23 & 2023-24.	Audited Financial Statements for the last three years (if not audited then Financial Statement certified by Chartered

		Accountant along with Income Tax Return filed for respective year)
4	Work Experience: - The bidder / supplier should have a minimum of Two year of experience in supply of SIEM Solutions to any organization like Banks, Govt. Organizations, PSU, Pvt. Ltd. Organization etc.	Copies of purchase orders from the organizations shall be submitted.
5	The bidder / suppliers should not have been blacklisted by any Company in the past or services terminated due to poor performance	An undertaking stating that the Company / Firm have not been blacklisted should be submitted.

(b) COMMERCIAL BID: -

- The Bidder should submit the bid which will contain a item (as referred in Annexure A).
- The Bidder should give MRP and Quoted / Offered Price of each product.

5. BID DETAILS IN BRIEF:

S No.	Description	Details
1	Bid / RFP No. & Date	UBISL/RFP/IT/2025/003 Dated July 04, 2025
2	Brief Description of the RFP	SIEM Solution supply as mentioned in Annexure A
3	Address for Communication	**IT Manager** **UBI Services Limited** **Registered / Head Office: Unit No. 504-506, 5th Floor, Centrum, Wagle Estate, Opp. Raila Devi Lake, Near Satkar Hotel, Thane West, Maharashtra, Pin – 400 604.** **Phone No.: 022 – 6930 3001, 8880141068** **Email: -** **tenders@ubisl.co.in**
4	Date of Issue	**July 08, 2025**
5	Pre-Bid Meeting	**July 14, 2025**
6	Last Date of submission of Bids	**July 22, 2025, 6:00 PM**
7	Date and time of opening Technical Bids.	**July 24, 2025**
8	Date of Evaluation of Technical bids and opening financial bids.	**July 29, 2025**

The bid documents should be delivered / submitted in sealed envelopes and scribed as "**BID for SIEM Solutions Supply To UBISL**" to address mentioned above before last date of submission of bids. **The Bidder should compile two separate envelopes, one**

for technical bid (Documents and technical information) another for Financial Bid which will contain a standard quantity, MRP and Quoted / Offered Price etc.

The bidder can send their tender documents in soft copy via email to tenders@ubisl.co.in but documents should be password protected and password can be shared to Manager IT at the time of opening of bid documents which shall be communicated separately.

- The Bid / Offer should be complete in all respects and contain all information asked for in this document
- The Company or UBISL may, at its discretion, extend this deadline for submission of bids by amending the RFP Document
- The Bid should be signed by the authorized signatory of the bidder. A Power of attorney or letter of authority to that effect shall be submitted by the bidder along with bid submission.
- All supporting documents / annexures should be duly signed and stamped by authorized signatories.
- The submitted bids should be valid for 90 days from the last date of submission of bid.

6. EMPANELMENT PERIOD AND TERMS:

The empanelment period will be valid for a period of one years (12 months) from the date of issue of an empanelment letter or purchase order. The review of the empaneled vendor may be conducted annually to review the quality of products delivered, timelines and negotiation in products prices. Based on performance, the company may consider extending the term, subject to mutually agreed upon terms and conditions. The Company may terminate the services of empaneled vendors at its discretion based on review and shall have the right to cancel this panel of vendors at any time during the empanelment period.

The Company is in process of empanelment of vendor / supplier for procurement of SIEM Solutions for a period of one year. The Company will shortlist three vendors / suppliers based on the following criteria.

- Technically qualified vendors (Top 3)
- Lowest quoted Cost / discount offered (L1, L2, & L3)
- implementation period

The Company will empanel the three vendors based on above criteria. At the time of purchase of SIEM Solutions company will invite the quotations from three empaneled vendors. The company will place the order to lowest quoted vendor for the particular lot. The Company will not invite or request for quote from non-empaneled vendors.

7. BID EVALUATION CRITERIA:

Bidder must qualify the technical eligibility criteria and should submit the required documentary proofs as indicated above. Bids which fail to qualify for any of the following criteria will be rejected. To evaluate the technical and commercial bid, the procurement committee constituted by the Company shall examine the documents furnished by the Bidder in the Technical Bid and Presentation to be given by the bidder. Only those bids which satisfy the Eligibility Criteria will be eligible for negotiation of quoted price.

Sr No.	Bidder Credentials	Max. Marks	Supporting Documents
1	Annual turnover more than Rs.1.50 Cr. in the last three financial years	20	Audited / Certified Financial Statement for last three years
2	Minimum Two year of experience in SIEM Implementation to Corporates/ Banks/ PSU / Govt.	20	Copies of purchase orders from the organizations shall be submitted.

Sr No.	Bidder Credentials	Max. Marks	Supporting Documents
	Organizations.		
3	Bidder should not be blacklisted by any corporate / bank for poor performance.	20	Undertaking by Bidder
4	Provide Draft Timelines for Implementation and previous implementation schedule and UAT Report	40	1. Tentative timeline for implementation from the date of PO. 2. On letter head or other relevant documents required at least last two company's where implemented with timelines.
	TOTAL	**100**	

Annexure A

Scope of Work – Cloud SIEM Solutions (Managed Services)

1. Project Planning and Preparation

- Requirement Gathering of the required services, objectives, and scope.
- Resource Allocation: Allocate necessary resources including hardware, and software.
- Timeline Development: Develop a project timeline with milestones and deadlines.
- Risk Assessment: Identify potential risks and develop mitigation strategies.

2. Infrastructure Assessment

- Network Topology Review: Analyze the existing network infrastructure to identify integration points for SIEM.
- System Inventory: Compile an inventory of all systems, applications, and devices to be monitored.
- Compatibility Check: Ensure compatibility of SIEM Security with existing hardware and software.

3. Solution Design

- Architecture Design: Design the SIEM Security architecture, including the placement of collectors, event handlers, and central management consoles.
- Data Flow Design: Define how data will flow from various sources into the SIEM system.
- Policy and Rule Development: Develop security policies, correlation rules, and alerting mechanisms to be implemented in SIEM application Security.
- Integration Plan: Plan integration with existing security tools, logging systems, and network devices.

4. Installation and Configuration

- Hardware/Virtual Machine Setup: Prepare and configure hardware or virtual machines for SIEM application security components.
- Software Installation: Install SIEM application security components including collectors, event handlers, and management consoles.

- Network Configuration: Configure network settings to ensure proper communication between SIEM application security components and data sources.
- Data Source Integration: Integrate various data sources such as firewalls, routers, servers, and applications with SIEM application Security.

5. Configuration and Tuning

- Policy Configuration: Implement and fine-tune security policies, correlation rules, and alert thresholds.
- Dashboard Setup: Configure dashboards for real-time and proactive alerting, monitoring and reporting.
- User Management: Set up user roles and permissions within SIEM Security.
- Log Management: Configure log retention, storage, and archival policies.

6. Integration

- SIEM Integration: Integrate SIEM application Security with other SIEM systems if required.
- Integration with other tools like cloud Zoho CRM, HRMS, Tally etc. for the monitoring of services and the threats.
- Branch monitoring – Router, Laptops and desktops
- Third-Party Tools: Integrate with other third-party security tools and platforms, such as antivirus, IDS/IPS, DLP, SD WAN and vulnerability management systems.
- Cloud Integration: Integrate with cloud services and platforms wherever necessary.

7. Testing

- Functionality Testing: Test all components to ensure they are functioning correctly.
- Security Testing: Conduct security testing to ensure data integrity and security within SIEM application Security.
- Performance Testing: Verify that the solution handles data input from all sources without performance degradation.

8. Training and Documentation

- Staff Training: Provide training to IT staff and security teams on using and managing SIEM application security.
- User Training: Educate end-users on best practices for reporting and responding to security alerts.

- Documentation: Provide comprehensive documentation, including installation guides, user manuals, and troubleshooting tips.

9. Deployment

- Pilot Deployment: Begin with a pilot deployment to a small group of systems to test the configuration and adjust as necessary.
- Full Deployment: Gradually expand the deployment to include all systems and devices in scope.
- Monitoring and Adjustment: Continuously monitor the deployment, gather feedback, and make necessary adjustments.

10. Post-Deployment Support

- Ongoing Monitoring: Set up continuous monitoring for security events and performance issues.
- Incident Response: Establish procedures for responding to security incidents detected by SIEM application and resolve it.
- Regular Updates: Ensure SIEM application Security is kept up-to-date with the latest patches and updates.
- Review and Optimization: Periodically review the solution’s effectiveness and optimize settings and policies as needed.

Key Points Needs to Take care:

1. Active Directory / LDAP Logs
2. SIEM Platform Logs (Self-monitoring)
3. Critical Application Logs (HRMS, CRM, etc.)
4. Database Access and Query Logs
5. VPN / Remote Access Logs
6. Network Access Control (NAC) Logs
7. Cloud Workload Protection Platform (CWPP) Logs
8. Mobile Device Management (MDM) Logs
9. Web Proxy / Secure Web Gateway (SWG) Logs
10. SIEM Correlation Rules / Use Case Library