Request for Proposal (RFP)

For Selection of Service Provider For

ANTI-PHISHING & ANTI-ROGUE SERVICES

For

The Akola Janata Commercial Co-operative Bank Ltd., Akola
(Multistate Scheduled Bank)

Head Office,
"Janvaibhav",
Old Cotton Market,
Akola – 444001

Tender Reference No. : AJCCB/IT/2021-22/Cyber Security

Date : 16.09.2021

The information provided by the bidders in response to this Request For Proposal (RFP) will become the property of The Akola Janata Commercial Co-operative Bank Ltd., Akola and will not be returned. The Bank reserves the right to amend, rescind or reissue this RFP and such amendments will be binding upon the Bidders. The Bank also reserves its right to accept or reject any or all responses to this RFP without assigning any reason whatsoever. This document is prepared by The Akola Janata Commercial Co-operative Bank Ltd.,Akola for Selection of Cyber Security Service Provider. It should not be reused or copied or used either partially or fully in any form.

1. Invitation for tender offers

The Akola Janata Commercial Co-operative Bank Limited, Akola invites sealed tender offers from eligible, reputed developers and/or their authorized dealers for providing external cyber security services as per requirements elaborated. Through this tender, bank is searching for a reliable cyber security service provider meeting the requirements as per Reserve Bank of India circular DoS.CO/CSITE/BC.4083/31.01.052/2019-20 dated 31.12.2019. The requirement is subscription based and focused on following points from this circular though not limited to:

Section	**Sub-Section**	**Requirement**
Anti-Phishing	8.1	Subscribe to Anti-phishing/anti-rogue application services from external service providers for identifying and taking down phishing websites/rogue applications.
Data Leak Prevention Strategy	9.1	Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.
Baseline Cyber Security and Resilience Requirements - Level	vi.	Put in place an effective mechanism to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. UCBs shall also report all unusual cyber security incidents to CERT-In and IB-CART.
Incident Response and Management	11.1	Put in place an effective Incident Response programme. UCBs must have a mechanism/ resources to take appropriate action in case of any cyber security incident. They must have written incident response procedures including the roles of staff / outsourced staff handling such incidents.
Vendor/Outsourcing Risk Management	viii.	Required to necessarily enter into agreement with the service provider that, among other things, provides for right to audit by the UCB. The outsourcing agreements should include clauses to recognise the right of the Reserve Bank to cause an inspection to be made of a service provider of the UCB and allow the Reserve Bank of India or persons authorised by it to access the bank's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a reasonable time.
Authentication Framework for Customers	7.1	UCBs should have adequate checks and balance to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine/authorised applications and that authentication methodology is robust, secure and centralised.

A complete set of tender document may be downloaded from our website www.akolajanatabank.com.

The details are given below:

Tender Reference	**AJCCB/IT/2021-22/Cyber Security**
Date of commencement of availability of tender document	**16.09.2021**
Last Date and Time for receipts of tender offers	**30.09.2021**
Tender Fees	**Rs.1000/- in the form of demand draft to be drawn in the name of bank**
Address of Communication	**Chief Executive Officer The Akola Janata Commercial Co-operative Bank Limited, Akola. " Janvaibhav" Old Cotton Market, P. B. No. 90, Akola 444001**
Email address	**cbs.ajccb@gmail.com**
Contact Telephone Numbers	**0724-2430012, 2430639, 2430241**
Bids to be given to	**Chief Executive Officer, The Akola Janata Commercial Co-operative Bank Limited, Akola.**

Technical Specifications, Terms and Conditions, the formats and pro-forma for submitting the tender offer are described in this tender document and its Annexure.

Chief Executive Officer
The Akola Janata Commercial Co-operative Bank Limited, Akola.

Instructions to Bidders

1. Bid Submission

Bid should be submitted to the following in single sealed envelope at the Bank's address given below on or before the schedule given above. The envelope should be securely sealed and stamped.

Chief Executive Officer
The Akola Janata Commercial Co-op. Bank Ltd.
"Janvaibhav" ,
Old Cotton Market, Akola.
Akola- 444001 (M.S.)
E-Mail: cbs.ajccb@gmail.com

The envelope must be super scribed with the following information –

- Tender Number
- Due Date
- Name of Bidder
- Name of the Authorized Person
- E-mail ID of the authorized person to contact.
- Mobile Number
- Correspondence Address

All schedules, Formats and Annexure should be stamped and signed by an authorized official of the bidder company.

2. Qualification Criteria

Reputed service providers , who have experience in providing cyber security services and who meet the following Eligibility criteria only need to apply:-

a) The service provider submitting the offers should be a Registered Company or Firm having an Average Annual Turnover of Rs. 25 Lakh in the last three consecutive financial years.
b) The Company/Firm should have made Net Profits in at least two financial years in last 3 Years.
c) Bidders must submit a Tender specific Manufacturer Authorization Form (MAF) that they have been authorized to quote on behalf on the manufacturers. Else bidder has to submit a declaration that they or original developer of the services product.
d) Bidder should be providing services to at least one BFSI customer.

3. Offer validity Period

The offer should hold good for a period of 6 months from the closing date of the tender. Bank may place number of orders during the minimum period of 6 months. The prices and services offered should be valid for the minimum period of 6 months.

4. Opening of Offers

Offers received within the prescribed closing date and time will be opened by the authorities of the Bank.

5. Preliminary Scrutiny

The Bank may, at its discretion, waive any minor non-conformity or any minor irregularity in the offer. This waiver shall be binding on all the service providers and the Bank reserves the right to exercise such waivers.

6. No Commitment to Accept Lowest

The Akola Janata Commercial Co-op. Bank Ltd., is under no obligation to accept the lowest Offer received in response to this tender and reserves the right to split the order or reject any or all the offers including incomplete offers without assigning any reason whatsoever.

7. Submission of Technical Details

It is mandatory to provide the technical details in the exact format **(Annexure C)** given in this tender. The relevant product information, brand and version offered, printed product brochure, technical specification sheets etc. should be submitted along with the offer. Technical compliance sheet das per **Annexure C** must to be included.

8. Format for Offer

The suggested format for submission of technical offer is as follows:

1. Index
2. Covering letter. This should be as per Annexure A.
3. Details of the service provider, as per Annexure B.
4. Technical Offer with Specifications as given in Annexure C, complete with all the columns filled in.
5. Manufacturer's Authorization Form (MAF) for the product quoted or self declaration whatever applicable.
6. Service provider's Financial Details and other supporting documents, as asked in the tender document.
7. Commercial Offer as per Annexure D.
8. Details of track record and customer references as per Annexure E.
9. Terms and Conditions Deviations Compliance as per Annexure F.
10. Tender Fees demand draft of Rs.1000/- drawn in favor of The Akola Janata Commercial Cooperative Bank Ltd., Akola payable at Akola.
11. Technical brochure / document of the product/services offered.

9. Location of Supplies

At the addresses given below.

SNo.	Location	Location Address	District
1	Head Office	THE AKOLA JANATA COMM. CO-OP BANK LTD. AKOLA, 'Janvaibhav', Old Cotton Market, Akola 444 001	Akola

10. Costs

The offer must be in fixed price basis for annual service charges in Indian Rupees only and shall be excluding GST and shall include the following:

1. Training to IT staff
2. Comprehensive support for various cyber security related issues
3. Support required for forensic audit if required
4. Support and reports required during IS Audit / Statutory Audit / RBI Inspection / VAPT / any other inspection
5. Any reports required on regular basis including all types of logs

11. Fixed Price
The Commercial Offer shall be on a fixed price basis, exclusive of GST. No price increase due to any factor will be permitted.

12. Negotiation
It is absolutely essential for the service providers to quote the lowest price at the time of making the offer in their own interest. Bank, however, reserve the right to enter into any price negotiations.

Terms and Conditions of the Tender

1. Technical Inspection and Performance Evaluation
The Akola Janata Commercial Co-operative Bank Limited, Akola reserves its right to carry out a technical inspection and performance evaluation (bench-marking) of all the services quoted. Bank may ask for proof of concept (POC) as a part of evaluation process during bid processing.

2. Payment Terms
The Akola Janata Commercial Co-op. Bank Ltd will make payment as follows:

- Out of yearly charges, 50% payment for services executed will be made after completion of 6 months
- Balance 50% payment will be made after next 6 months

3. Order Cancellation
The Akola Janata Commercial Co-op. Bank Ltd reserves its right to cancel the order in the event of one or more of the following situations:

Delay in delivery beyond 15 days from the date of issuance of services order.

Bank reserves the right to take appropriate action and make good any or all losses incurred during the process from the service provider.

4.Billing
The billing should be done locally for respective locations inclusive of all taxes giving break up thereof. GST as applicable, will be paid extra as per the existing rates.

5. Force Majeure Clause:
The service provider shall not be liable for liquidated damages or termination for default, if and to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of force Majeure. For purposes of this Clause, "Force Majeure" means an event beyond the control of the service provider and not involving the

service provider's fault or negligence and not foreseeable. Such events may include, but are not limited to, Acts of God or of public enemy, acts of Government of India in their sovereign capacity, acts of war, acts of The Akola Janata Commercial Co-operative Bank Limited, Akola in fires, floods and freight embargoes. If a Force Majeure situation arises, the service provider shall promptly notify The Akola Janata Commercial Co-operative Bank Limited, Akola in writing of such conditions and the cause thereof within twenty calendar days. Unless otherwise directed by The Akola Janata Commercial Co-operative Bank Limited, Akola in writing, the service provider shall continue to perform it's obligations under the Contract as far as it is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, The Akola Janata Commercial Co-operative Bank Limited, Akola and the service provider shall hold consultations with each other in an endeavor to find a solution to the problem.

6.Governing Law & Jurisdiction

All disputes under the Jurisdiction will be of the Courts in **AKOLA, Maharashtra only.**

ANNEXURE A - Tender Offer Cover Letter

Date:
Tender Reference No.:

To:
Chief Executive Officer,
The Akola Janata Commercial Co-op. Bank Ltd,
"Janvaibhav", Old Cotton Market,
Akola - 444001

Dear Sir,

Having examined the tender documents including all annexure the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide cyber security services in conformity with the said tender documents in accordance with the schedule of prices attached in the commercial offer and made part of this tender.

If our tender offer is accepted, we undertake to complete delivery within 15 days from the date of services order.

We agree to abide by this tender offer and all the terms & conditions till 6 months from the closing date of tender and our offer shall remain binding upon us and may be accepted by the Bank any time before the expiration of that period.

This tender offer, together with the Bank's written acceptance thereof and the Bank's notification of award, shall constitute a binding contract between us. We shall sign requisite SLA within 15 days of receipt of order.

We hereby, once again, confirm our acceptance to all the terms and conditions of your tender.

We understand that the Bank is not bound to accept the lowest or any offer the Bank may receive.

Dated this _____ day of _____2021

Signature: _____

Designation : _____

Authorized to sign the tender

ANNEXURE B – Service Provider Details

Sr. No	Particulars	Details
1	Name of Company	
2	Mailing Address	
3	Telephone and Fax numbers	
4	Constitution of the Company	
5	Name and designation of the person authorized to make commitments to the "The Akola Janata Commercial Co-operative Bank Ltd."	
6	Email Address	
7	Year of commencement of Business	
8	Turn over of the company (not of group) for the year 2018-2019 2019-2020 2020-2021	
9	Profit of the company (not of group) for the year 2018-2019 2019-2020 2020-2021	
10	GSTIN	
11	PAN	

ANNEXURE C : Technical Requirement with Compliance

Present domains of bank

a) akolajanatabank.com ..
b) akolajanatabank.in ..
c) akolajanatabank.co.in ..
d) akolajanatabank.net.in ..
e) akolajanatabank.org.in ..
f) akolajanatabank.net
g) akolajanatabank.org
h) netbanking.akolajanatabank.com
i) netbanking.akolajanatabank.co.in

Our mobile app named PayJan available on Google Playstore.

Part I – Broad Technical Compliance

SNo	Features – Part I	Compliance (Yes/No)
1.	**Brand and Anti phishing Protection**	
	Anti-Phishing	
	Anti-Trojan AntiPharming	
	Brand Protection	
	Anti-rogue	
	Unlimited Take-downs of Phishing websites	
	Unlimited Take-downs of Rogue Applications	
2.	**Data Leakage detection (Dark Web Monitoring)**	
	Customer Data	
	Employee Data	
	Private / Sensitive Documents	

Part II – Detailed Technical Compliance

SNo	Features – Part II	Compliance (Yes/No)
A	**General Features**	
1	Services must be a tool based automated solution with e-mail Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	
2	24*7*365 real time monitoring and support for all the services covered for:	
3	Anti-Phishing	
4	Anti-Malware	

5	Anti-Web Defacement	
6	Solution support scanning to a depth of multiple pages	
7	Solution support checking all website links against well-known global black list.	
8	A dash board should be provided to the Bank with information on all incidents of phishing and its various stages of resolution	
9	Solution provides online interface to the Bank to see previous online reports of all the websites under monitoring	
10	Solution should be able to identify potential phishing websites hosting similar content resembling the official web-site.	
11	Solution should provide for identification of any sensitive documents/information pertaining to the customer available on the internet and Dark Web.	
12	Solution should be able to identify potential brand infringements and affiliations risk	
13	Solution provides for identification of fake recruitment schemes claiming affiliation with the bank.	
14	Solution should have ability to identify and alert customer, on the related data posted for sale on the dark web by use of intelligence tools integrating with convergent technologies to inspect threats /data related to customer existing in deep/ dark web.	
15	Solution should have ability to detect potential infringements and malicious websites by use of contemporary technologies like threat intelligence etc.	
B	**Anti-Malware and Anti Website Defacement**	
1	The services is required to be provided with comprehensive scanning of URLs/Websites and provide report in various possible ways	
2	Monthly and other ad-hoc reports to be provided as per the bank request.	
3	Website domain tracking analysis to detect phishing sites.	
4	Blocking of the phishing sites in web browsers.	
5	The Solution provide mechanism to detect and protect internal users from targeted phishing attacks. Solution provide agent that will protect employee from phishing, credential harvesting attack	
6	The solution provides employee behavior analysis with regards to phishing campaign. Provide mechanism to bank to see which are top 10 employee involved in phishing-based attack.	
7	Solution provide mechanism to whitelist bank internal and other safe site.	
8	Taking down of phishing sites anywhere in the world either on Vendor's own reach or through partnerships.	
9	The vendor should have the ability to identify defacement of Bank website and corresponding WebPages through a combination of automated scans and manual analysis.	
C	**Early Phishing Detection:**	
1	Wide coverage of web, social media and email sources to detect newly configured phishing attacks.	
2	24x7x365 real monitoring for phishing attacks.	
3	Implementation of real time detection mechanisms and alerts.	
4	Monitoring similar Typosquatted and Cybersquatted domain	
5	Monitoring spam traps to detect phishing mails	
6	Should have mechanism to mail to Bank on the basis of severity of incident.	
7	Domain and social media for Impersonation Monitoring:	
8	Analysis of social networks such as Facebook, Twitter, Linkedin etc. and domain registrations to find fake social profiles, malicious mentions and similar domains that impersonate Bank.	
9	Rogue Mobile Application Protection:	
10	Detect and remove unauthorized applications imitating your official app from third-party app stores. Help Bank to reduce the risk of customers inadvertently downloading imposter apps.	
11	Monitor any fraudulent mobile applications targeting Bank's customers to	

	capture their credentials for fraudulent transactions.	
12	Taking down of fraudulent mobile apps in the world targeting Bank Customers.	
13	Dark Web/Deep Web Scanning for sensitive information pertaining to Bank:	
14	The Vendor has to provide threat monitoring solution that penetrates the restricted cybercrime zone known as the Dark Web looking for compromised sensitive data to proactively mitigate impact after breaches.	
15	Monitor Cyber Crime Forums on clear web as well as dark web/deep web.	
16	Monitor Networks known to be sources of attacks and low points of collection of compromised data.	
17	Deployed honey pots or network or sensors to collect data on threat.	
18	The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand.	
19	The vendor needs to monitor sensitive data such as but not limited to Personal Identifiable Information (PII) such as Customer/Employee data, Compromised banking credential/account monitoring, Credit card I Debit card BIN range monitoring of the bank, leaked source code, technical informational data used to target corporate systems, Vulnerability/ exploit monitoring and correlation with respect to the bank infrastructure	
D	**Brand Protection, Monitoring and Compliance enablement**	
1	24x365 proactive monitoring of World Wide Web etc. for Phishing, Brand Abuse and any other threat or exploitation of vulnerabilities which lead to compromising of credentials of the customers unknowingly directed against the customers of the Bank.	
2	The solution provider should be able to Initiate the responses as per Bank‘s request	
3	The service provider is required to perform takedown services subject to identified threat and subsequently bank's approval	
4	Access to Dashboard view of the risks and threats identified through the Anti-Phishing and threat intelligence services	
5	Monitoring of all major mobile application marketplaces for counterfeit, copycat apps, or apps infringing trademarks, linking to pirated content, attempting phishing attacks or distributing malware	
6	Prompt submission of enforcement notices and for the removal of rogue or infringing applications	
7	Bidder must have capability for monitoring of similar sounding domain name registrations and alerting the Bank if this is detected	
8	Detection and advisories of the attacks anywhere in the world within the minimum possible time.	
9	Continuous scanning of all the websites/apps of the Bank to detect any type of blacklisted links, suspicious activities etc. Reporting to Bank the exact nature and location of the infection for speedy removal of the infection / abnormality.	
10	Proactive Monitoring of major Mobile App stores and blocking/Shutting down of Malicious App/Trojan used against the bank.	
11	Reporting to Bank in line with regulatory requirements about all the attacks and providing detailed information through email & online dashboard	
12	Monthly and other ad hoc reports to be provided as per the requirement and format provided by the bank	

13	Additional Login IDs for bank need to be created which will be utilized for activities like logging of incidents, ascertaining status of current/closed incident, generating reports of the reported incidents etc as per requirement of the bank.	
14	Service provider should provide feasibility for entering the details of websites/apps of the bank which need to be whitelisted so that these sites are not taken down	
15	Taking all necessary security aspects into account to ensure the confidentiality and integrity of the data related to above service.	
16	Ability to monitor incidents related to brand abuse	
17	Ability to monitor all kind of incidents given below:	
18	Phishing	
19	Pharming	
20	Trojan	
21	Brand Abuse	
22	Domains (Old/New) similar to the Bank	
23	Rogue Mobile Apps	
24	Ability to close any incident within the earliest possible time, take proper counter measures wherever required, ensuring continuous monitoring for repeated incidents.	
25	Provision of Dashboard that should have all the following features:	
26	Display of high- and low-level reports, Trends	
27	Regular update of incidents	
28	Intelligence alerts	
29	Monthly report	
30	Regular alerts on critical vulnerabilities and exploitable vulnerability	
31	Authenticated and unauthenticated Penetration Testing	
32	Threat Intelligence	
33	The portal should deliver a real-time view of all the components of Bank's digital threat protection.	
34	The vendors should provide an all-encompassing dashboard illustrates threat data, including volume by source and category, and takedown status.	
35	Users should be able to set up email alerts, create online or printed reports, request takedowns.	
36	Providing incident reports on phishing attacks and fraudulent apps involving threat analysis and threat categorization.	

ANNEXURE D – Commercial Offer

(To be submitted as per this format only)

Sr. No.	Services Short Name (Specify Product Name through which services would be provided)	Annual Subscription Cost in INR	GST Extra in %
1	Cyber Security Services – External		

Signature of Bidder:_____

Place:

Name:

Date:

Business Address:

Annexure E - Details of Track Record & Reference Customers

Name of the Client	**Details of Cyber Security Services**	**Contact person** • **Name** • **Tel. No.**

- Bidder is supposed to give entire list of customers particularly from BFSI segment.

Annexure F - Terms & Conditions Deviation Compliance Statement

The following are the particulars of only deviations from the requirements of the tender specifications:

Term No	Short Description of the Terms & Conditions	Detailed explanation about deviation, if not complied

- If no deviation, put NIL

**********End of RFP**********