The Maharashtra State Co-operative Bank Ltd., Mumbai

(Incorporating the Vidarbha Co-operative Bank Ltd.)

Corrigendum No. 1 of Tender document advertised on 23-09-2019 for Selection of Vendor for Supply, Installation, Configuration, Implementation and Servicing of Firewalls For Data Center.

Following changes be noted in the tender document:

Page No	**Point No**	**Technical Specifications as per Tender Document**	**Change in the tender document**
3	1-Tender Highlights	Last Date of Submission- 15-10-2019 up to 3.00 p.m.	Last Date of Submission- 23-10-2019 up to 3.00 p.m.
3	1-Tender Highlights	Date of Technical Bid Opening - 15-10-2019 at 3.30 p.m.	Date of Technical Bid Opening - 23-10-2019 at 3.30 p.m.
4	4.1 .B	The vendor should have a minimum of 10 (Ten) years' experience in the field of Firewall Supply, Installation, Migration, Implementation and Support Business. (Must attach company incorporation certificate).	The vendor should have a minimum of 10 (Ten) years' experience in the field of IT and 6 (Six) years' experience in Firewall and Cyber Security appliances. (Must attach company incorporation certificate).
4	4.1.C	Must have installed minimum 25 Firewalls.	Must have installed minimum 10 Firewalls in last 6 years
4	4.1.E	Vendor should have supplied DC Firewalls to at least 3 Banks/PSU/NBFC with Value over Rs. 2 Cr.	Vendor should have supplied 3 Enterprise Firewalls in last 3 years valueing arround Rs 1.5 Crores total of which minimum 1 bank customer is must and 2 can be sold to Banks/PSU/NBFC/BFSI / Big Corporate.
4	4.1.G	Vendor should have a fully functional service/support centre in Mumbai with minimum 20 qualified Technical Support Staff to provide quality service support.	Vendor should have a fully functional service/support centre in Mumbai with minimum 10 qualified Technical Support Staff to provide quality service support.
4	4.1.I	Vendor should have an experience of similar project (Data Center firewall) 3 projects worth Rs.2 Crore p.a. for which documentary evidence must be submitted.	Vendor should have an experience of similar project (Data Center firewall, Security Appliance) 3 projects worth Rs.1.5 Crore for which documentary evidence must be submitted.
4	4.1.L	Vendor should have ISO Certification 9001,27001 and CMMI Level 5	Vendor should have ISO Certification 9001,27001
5	4.1.O	Please provide the names of the client banks with proof for supply of DC Firewall. The Bank may consider other customers also	Please provide the names of the client banks with proof for supply of DC Firewall. The Bank may consider other

		but preference and weightage will be given to BSFI segment	customers also but preference and weightage will be given to BSFI segment. Masked customer PO will be considered
5	4.1.P	The vendor should have extensive knowledge and experience (minimum of Ten (10) years) in the field of supply, installation and configuration, migration of High-end Firewalls used in large applications at DC and DR sites.	The vendor should have extensive knowledge and experience (minimum of Six (6) years) in the field of supply, installation and configuration, migration of High-end Firewalls used in large applications at DC and DR sites.
6	4.2.D.f & 4.2.D.g	Detailed Delivery Schedule for supply of Firewall. Tentative briefing about the team to be deployed: number, qualifications etc.	Detailed Delivery Schedule for supply of Firewall. Tentative briefing about the team to be deployed: number, qualifications etc. Can be provided after getting PO or confirmation.
18	7. 2	Vendors support to Bank during the project cycle of 5 years for Supply, Installation, and Configuration, Interfacing, Implementation and Servicing of Firewalls. It is totally OEM's responsibility to install firewalls.	Vendors support to Bank during the project cycle of 5 years for Supply, Installation, and Configuration, Interfacing, Implementation and Servicing of Firewalls. It is totally OEM's / Bidders responsibility to install firewalls.
21	8.G	Vendor must repair any equipment that is reported to be down within next 24 Hrs. from the time of reporting. In case vendor fails to meet the above standards of maintenance, there will be a penalty as specified in the table as under:	Vendor must repair / replace any equipment that is reported to be down within next 24 Hrs. from the time of reporting. In case vendor fails to meet the above standards of maintenance, there will be a penalty as specified in the table as under:
23	2.1.E	Customer Feedback : Feedback certificates from a client being served for DC/DR with minimum 5 firewalls	Customer Feedback : Feedback certificates from a client being served for DC/DR with minimum 3 firewalls
28	Annexure-B, 1.Perimeter Firewall. 10	Firewall should not introduce more than 10 microsecond latency. Vendor's claim must be available in publicly available documents like datasheet, admin guide etc	Firewall should not introduce more than 10 microsecond latency. Vendor's claim must be available in publicly available documents like datasheet, admin guide etc. Documentary evidence is must if public document is not available.
29	Annexure-B, 1.Perimeter Firewall. Intrusion Preventive System. 1.	The IPS capability of proposed OEM should have received NSS labs' "Recommendation" rating of NGIPS 2018 test report	The IPS capability of proposed OEM should have received NSS labs' "Recommendation" rating of NGIPS 2018 test report This clause is for IPS capability not NGFW So NGIPS report is mentioned. You can consider latest NGIPS report.
30	Annexure-B, 1.Perimeter	OEM must have received "Recommendation" rating in NSS labs Breach Prevention System test of 2018	OEM must have received "Recommendation" rating in NSS labs Breach Prevention System test. Latest

	Firewall, Anti-virus and Anti-bot. 6.		BPS test will be considered.
30	Annexure-B, 1.Perimeter Firewall, Anti-virus and Anti-bot. 10.	The proposed solution should analyse advanced malware against a cross-matrix of different operating systems (at least Windows 8 and Windows 10) and various versions of pre-defined applications across at least 4 on-premise virtual machines and expandable to 8 machines in future if requires	The proposed solution should analyse advanced malware against a cross-matrix of different operating systems (at least Windows 8 and Windows 10) and various versions of pre-defined applications across at least 4 on-premise virtual machines and expandable to 8 machines in future if requires. We have asked for on-premise sandboxing solution only. Vendor can propose hardware based sandboxing solution or virtual based sandboxing solution.

Note: **Corrigendum -1 shall be the part of RFP document. Vendors are required to duly sign the Corrigendum -1 by the authorized signatories and enclose the same with Technical offer while submitting bid document.**

Date: 10th October 2019
Place: Mumbai.