Gram : UNIVERSITY

Phones 2570301
2570263
2570450

छत्रपति शाहू जी महाराज विश्वविद्यालय, कानपुर
CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

कल्यानपुर, कानपुर
KALYANPUR, KANPUR

Ref. No. CSJMU/RCamp/ 177/2015

Dated : 20- 02 - 2015

SHORT TERM TENDER FOR SUPPLY AND COMMISSIONING OF Wi-Fi FACILITY

Sealed tenders are invited from OEM and/or their authorized dealer and/or Channel Partner for participation in Open Tender Enquiry (Under Two Bid System) for Supply, Installation, Testing, Commissioning and three years warranty with on site support.

Interested parties may collect the detailed Tender Document from the University cash counter during working hours on payment of Rs. 500/- Non Refundable in cash or may download the Tender Document from the University website www.kanpuruniversity.org and attach a DD of Rs. 500/- in favour of "Finance Officer, CSJM University, Kanpur" from 21/02/2015 to 27/02/2015. The Tender complete in all respects should be dropped up to 01.00 p.m. on 27/02/2015 along with prescribed Earnest Money Deposit & MAF in the tender box placed at Central Store, CSJM University, Kanpur. The tender will be opened on 27/02/2015 at 02:00 p.m. in the presence/absence of the tenderers.

The tender document consists of the following two parts -
01.Part-1: "TERMS & CONDITIONS" & "TECHNICAL BID" of the tender.
02.Part-2: "FINANCIAL BID" of the tender.

The University reserves all the right to accept or reject any or all the tenders without assigning any reason.

Registrar

PART – 1
TECHNICAL BID FOR SUPPLY AND INSTALLATION OF Wi-Fi FACILITY AT CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR

TERMS & CONDITIONS

1. Sealed Tenders are invited from the reputed OEM and/or their authorized dealer and/or Channel Partner for supply, installation, testing, commissioning and three years warranty with on site support at Chhatrapati Shahu Ji Maharaj University Kanpur.
2. OEM and/or their authorized dealer and/or Channel Partner are allowed to take part in the bid for the supply, installation, testing, commissioning and three years warranty with on site support. Bid should be accompanied by proofs that the vendor is OEM and/or their authorized dealer and/or Channel Partner. Authorization letter specific to this tender should be attached with the technical bid in case of authorized dealer and/or Channel Partner.
3. The earnest money deposit of Rs. 50,000/- (Rupees Fifty Thousand) should be enclosed along with the terms & conditions & technical bid duly signed and stamped in the form of Bank Demand Draft/Banker's Cheque of any branch of Nationalized /Schedule Bank in favor of "Finance Officer, Chhatrapati Shahu Ji Maharaj University, Kanpur" in a separate sealed envelope. All tenders submitted without requisite amount of earnest money shall be rejected and their technical and financial bids shall not be opened.
4. The bids submitted by the vendors should be valid for a minimum period of 60 days from the date of the opening of tender and the prices should be valid till execution of purchase agreement.
5. The sealed envelope containing "Terms & Conditions", "Technical Bid" and "Financial Bid" on prescribed tender document of the Chhatrapati Shahu Ji Maharaj University, Kanpur should be dropped in the tender box placed at Central Store, Chhatrapati Shahu Ji Maharaj University, Kanpur on or before 27/02/2015 up to 01:00 p.m. For submission of bids, the two-bid system should be followed for this tender;-The bidder must submit their offer in two separate sealed envelopes. Both the technical bid and financial bid envelopes should be securely sealed and stamped separately and clearly marked as "Envelope No.1 - Technical Bid" and "Envelope No.2 - Financial Bid" respectively. Both the sealed envelopes should be placed in a third larger envelope. All the three envelops should be sealed properly. The main envelope which will contain both the bids i.e. 'Technical Bid' and 'Financial Bid' should be super scribed with the "Tender Notice No." and last date and time of the opening of the tender.
6. In the event of date specified for bids opening being declared a holiday for Tendering Authority's office then the due date for opening of bids shall be the following working day of the earlier scheduled time.
7. CSJM University, Kanpur reserves all the right to accept or reject any or all the tenders without assigning any reason.
8. The supply, installation, testing, commissioning and three years warranty with on site support of Wi-Fi related items shall be made by the vendor within 2-3 weeks from the date of issue of the purchase order by CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR to the vendor. If any loss or damage occurs in transit then it will be the responsibility of the supplier. The entire supply should be made within the time stipulated in the tender/purchase order for installation.
9. Material supplied should be new and of good quality and standard as per the technical specifications mentioned in technical bid document.
10. The vendor will provide operational manuals, OEM documents for items supplied.
11. Prices should be quoted in Indian Rupee (INR) only.

12. Payment for the items to be supplied by the vendor against the purchase order shall be made by CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR as follows:-

    80% of the hardware supplied will be released on receipt and verification of Wi-Fi related hardware and remaining 20% of the total payment will be made after satisfactory installation and commissioning of Wi-Fi facility in the University campus.

13. Payment shall be released on receipt of the original bills in triplicate complete in all respect and original delivery challans of all the items duly signed and stamped by the authorized representative of the user department.
14. Three years Standard warranty on items supplied. Warranty period will start from the date of Successful commissioning of all the items at the site.
15. Vendor should specify the make (only from Motorola, Cisco. Ruckus) and model along with all other technical details and relevant data/ technical brochure.
16. All the documents should be submitted along with the technical bid of the tender.
17 The vendor should be registered with the service tax department of the govt. (submit valid documentary proof for the same e.g. sales tax/vat no./service tax registration number and details of income tax registration / PAN etc. along with the technical bid.
18 Tender will be rejected, if technical specifications offered by the vendor in the technical bid differ from that of Technical compliance sheet of tender.
19 Tender not conforming to any or all the terms and conditions of this tender will be rejected.
20 Incomplete tenders are liable to be rejected.
21 CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR reserves all the rights to increase/decrease the specified quantities of any item(s) given in the tender.
22 All the items being quoted should have minimum technical specifications given in the tender. **Line-by-Line compliance in the technical bid format (Part-1(B)) should bid filled-in properly. Do not leave line-by-compliance column blank"**
23 OEM/Authorized partner Certificate should be attached in Technical Bid for this specific Tender if the Vendor is not direct manufacture of product. If MAF is not attached in Technical Bid then bid will be rejected.
24 OEM should have local after Sales service and support present in Kanpur either self or through authorized dealer/Channel Partner.
25 A bidder is required to propose a single integrated Wi-Fi Solution and all the wireless products (Access point type-1, 2 & the controller) should be from the same OEM.

26 Wireless infrastructure should be conforming to IEEE 802.11n/ac.

27 In order to ensure proven-ness of the offered Wi-Fi solution, the OEM should have presence in India from last 05 years and also have minimum 05 deployments in Education/Research Institute with at least Count of 100 Access Points in single P.O. (Order copies from OEM to be provided).

28 The OEM should have been in operation for a period of at least 05 years as on date, as evidenced by certificate/document to be attached.

29 The vendor's annual turnover should be at least Rs.5 crore (Rs five crore) in each of the last three financial years. Attach documentary evidence for confirmation regarding turnover. The turnover refers to a company and not the composite turnover of its subsidiaries/sister concerns .etc. for 2011-12, 2012-13 and 2013-14.

PART – 1 (B)

BILL OF QUANTITY & TECHNICAL SPECIFICATIONS

S. No.	Description	Quantity (Approx.)
1	Wireless Controller	1
2	Access Point TYPE-1 with POE injector & mounting mechanism	50
3	Access Point TYPE-2 with POE injector & mounting mechanism	12

2.0 Technical Specifications

WLAN Controller Specifications

1. WLAN Controller should have minimum 2 10/100/1000 Ethernet or SFP port.WLAN Controller should support up to 65 AP's from day one and should be scalable up to 75 campus connected access points in a single 1 RU chassis.

2. Controller should support 100+ WLAN's.

3. Compatibility Must Support Wireless Intrusion Prevention feature.

4. High Availability: Must support 1+1 and N+1 redundancy models. Must support redundancy functionality for all the Access points to move from primary to backup Controller.

5. RF Management: Must support an ability to dynamically adjust channel and power settings based on the RF environment. Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference Must support interference detection and avoidance. Must support coverage hole detection and correction.

6. IPv6 features WLAN Controller should support IPv4. IPv6 and Dual stack. WLC should support Guest-access functionality for IPv6 clients

7. Performance: Controller performance must remain the same if encryption is on or off for wireless SSIDs. Security: Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP). 802.1X with multiple Extensible Authentication Protocol (EAP) types and Radius server. Controller should support integrated or External AAA server. System should provide DOS attacks and Intrusion Detection & Prevention and Control for any Rough Access Points. The AP should be able to scan for rogue access points and the controller should be able to locate them on a floor map. The controller should be able to send a notification to the administrator when a rogue AP has been detected.

8. 802.11e and WMM.

9. Wi-Fi Alliance Certification for AP.

10. Must support settingL2, L3 Access Control Lists (ACLs).

11. System should support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.

12. Guest Wireless-Must support built-in web authentication and Captive portal support with external AAA/Gatewa}.

13. Controller should have BYOD features and Guest Access management procedure where user may use internet without entering to Enterprise SSID and should be time restricted.

14. Guest credential delivery should be done via SMS and e-mail, via the controller or by a third party appliance.

15. Should be able to set per-user bandwidth limit on a per user/SSID basis.

16. Must support user load balancing across Access Points.

17. Controller must provide Mesh capability for Mesh supported AP.

18. Must support client roaming across controller on L2 or L3. Solution proposed must support clients roaming across at least 75 campus connected APs.

19. System should provide the faster clients should not starve airtime fairness between these different speed clients -slower clients and faster clients should not adversely affected by slower clients.

Access Point Tvpe-1

1. Access Points proposed must include radios for both 2.4 GHz and 5 GHz.

2. Must have a robust design for durability.

3. Should be able to handle up to 250 Concurrent users.

4. Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams

5. Must support simultaneous 802.11a/b/g/n/ac.

6. Must support data rates up to 300Mbps on 2.4GHz Radio and 867MBps on 5GHz.

7. AP should provide minimum 23dBm transmission power for 2.4Ghz and 21dBm for 5Ghz. (EIRP should limited as per govt regulation for indoor AP's).

8. For better performance on Smart devices like phones and tablets, the access point should support diverse multiple polarization of integrated antennas.

9. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one and two spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

10. Must support AP enforce load-balance between 2.4Ghz and 5Ghz band.

11. Should support receiver's sensitivity of -101dBM or better.

12. Must have Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method. Should also support coverage hole detection and performance optimization.

13. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

14. Should support locally significant certificates on the APs using a Public Key Infrastructure (PKI).

15. Must support IDS/IPS.

16. Access Points must support a distributed encryption/decryption model.

17. Access Points must support encryption on CAPWAP/LWAPP Standard. Monitoring

18. Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.

19. Must support 16 WLANs per AP for SSID deployment flexibility.

20. Must support HTTP/S, telnet and/or SSH login to APs directly for troubleshooting flexibility.

21. Must support Power over Ethernet, local power, and power injectors.

22. 802.11e and WMM

23. WiFi Alliance Certification for AP

24. Must support Reliable Multicast Video to maintain video quality.

25. Must support QoS and Call Admission Control capabilities.

Access Point Type-2

1. Access Points proposed must include radios for both 2.4 GHz and 5 GHz.

2. Must have a robust design for durability

3. AP Must be IP 67 Certified and outdoor rated (datasheet of the Access Point should haveIP- 67 mentioned).
4. Operating temperature: -10 degree to 55 degree
5. Should be able to handle up to 250 Concurrent users.

6. Must support 2X2 multiple-input multiple-output(MIMO).

7. Must support simultaneous 802.11a/b/g/n/ac

8. For better performance on Smart devices like phones and tablets, the access point should support diverse multiple polarization of integrated antennas.

9. Must support data rates up to 300Mbps on 2.4GHz Radio and 867 Mbps on 5GHz.

10. AP should provide minimum 26dBm transmission power for 2.4Ghz and 25dBm for 5Ghz. (EIRP should limited as per govt regulation for indoor AP's).

11. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one and two spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

12. Must support AP enforce load-balance between 2.4 GHz and 5 GHz band.

13. Should support receiver's sensitivity of -100 dBM or better.

14. Must bave Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method. Should also support coverage hole detection and performance optimization.

15. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

16. Should support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).

17. Must support IDS/IPS.

18. Access Points must support a distributed encryption/decryption model.

19. Access Points must support encryption on CAPWAP/LWAPP Standard. Monitoring

20. Mesh support should support QoS for voice over wireless.

21. Must support 16 WLANs per AP for SSID deployment flexibility.

22. Must support HTTP/S, telnet and/or SSH login to APs directly for troubleshooting flexibility.

23. Must support Power over Ethernet 802.3 af.

24. 802.11e and WMM

25. Must support QoS and Call Admission Control capabilities.

Compliance Sheet for Wi-Fi Setup

WLAN Controller -

Sl.	Specifications	Compliance (Yes/No)	Remarks	Item Quoted in commercial bid (Yes, separately/No/Yes, Inbuilt)
1.	WLAN Controller have minimum 2 10/100/1000 Ethernet or SFP port.WLAN Controller should support up to 65 AP's from day one and should be scalable up to 75 campus connected access points in a single 1 RU chassis.			
2.	Controller support 100+ WLAN's.			
3.	Compatibility Support Wireless Intrusion Prevention feature.			
4.	High Availability: support 1+1 and N+1 redundancy models. support redundancy functionality for all the Access points to move from primary to backup Controller.			
5.	RF Management: support an ability to dynamically adjust channel and power settings based on the RF environment. Radio coverage algorithm must allow adjacent APs to operate on different channels, in order to maximize available bandwidth and avoid interference support interference detection and avoidance. Must support coverage hole detection and correction.			
6.	IPv6 features WLAN Controller support IPv4, IPv6 and Dual stack. WLC support Guest-access functionality for IPv6 clients			
7.	Performance: Controller performance must remain the same if encryption is on or off for wireless SSIDs. Security: Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types and Radius server. Controller should support integrated or External AAA server. System should provide DOS attacks and Intrusion Detection & Prevention and Control for any Rough Access Points. The AP should be able to scan for rogue access points and the controller should be able to locate them on a floor map. The controller should be able to send a notification to the administrator when a rogue AP has been detected.			
8.	Wi-Fi Alliance Certification for AP.			
9.	Support setting L2, L3 Access Control Lists (ACLs).			
10.	System support L2 Client Isolation so User cannot access each other's devices. Isolation should have option to apply on AP or SSID's.			
11.	Guest Wireless- support built-in web authentication and Captive portal support with external AAA/Gateway.			
12.	Controller have BYOD features and Guest Access management procedure where user may use internet without entering to Enterprise SSID and should be time restricted.			
13.	Guest credential delivery should be done via SMS and e-mail, via the controller or by a third party appliance.			
14.	Should be able to set per-user bandwidth limit on a per user/SSID basis.			
15.	Support user load balancing across Access Points.			
16.	Controller must provide Mesh capability for Mesh supported AP.			
17.	Support client roaming across controller on L2 or L3. Solution proposed must support clients roaming across at least 75 campus connected APs.			
18.	System should provide the faster clients should not starve airtime fairness between these different speed clients –slower clients and faster clients should not adversely affected by slower clients.			
19.	Support 802.11e WMM			

Note : Any other features may be listed separately in continuation of the compliance sheet.

Access Point Type-1

Sl.	Specifications	Compliance (Yes/No)	Remarks	Item Quoted in commercial bid (Yes, separately /No/Yes, Inbuilt)
1.	Access Points proposed include radios for both 2.4 GHz and 5 GHz.			
2.	Have a robust design for durability.			
3.	Should be able to handle up to 250 Concurrent users.			
4.	Support 2X2 multiple-input multiple-output (MIMO) with two spatial streams			
5.	Support simultaneous 802.11a/b/g/n/ac.			
6.	Support data rates up to 300Mbps on 2.4GHz Radio and 867MBps on 5GHz.			
7.	AP should provide minimum 23dBm transmission power for 2.4Ghz and 21dBm for 5Ghz. (EIRP should limited as per govt regulation for indoor AP's).			
8.	For better performance on Smart devices like phones and tablets, the access point should support diverse multiple polarization of integrated antennas.			
9.	The Wireless AP should have the technology to improve downlink performance to all mobile devices including one and two spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.			
10.	Support AP enforce load-balance between 2.4Ghz and 5Ghz band.			
11.	Should support receiver's sensitivity of -101dBM or better.			
12.	Have Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method. Should also support coverage hole detection and performance optimization.			
13.	Support Proactive Key Caching and/or other methods for Fast Secure Roaming.			
14.	Support locally significant certificates on the APs using a Public Key Infrastructure (PKI).			
15.	Support IDS/IPS.			
16.	Access Points support a distributed encryption/decryption model.			
17.	Access Points support encryption on CAPWAP/LWAPP Standard. Monitoring			
18.	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.			
19.	Support 16 WLANs per AP for SSID deployment flexibility.			
20.	Support HTTP/S, telnet and/or SSH login to APs directly for troubleshooting flexibility.			
21.	Support Power over Ethernet, local power, and power injectors.			
22.	Support 802.11e and WMM			
23.	WiFi Alliance Certification for AP			
24.	Support Reliable Multicast Video to maintain video quality.			
25.	Support QoS and Call Admission Control capabilities.			

Note : Any other features may be listed separately in continuation of the compliance sheet.

Access Point Type-2

Sl.	Specifications	Compliance (Yes/No)	Remarks	Item Quoted in commercial bid (Yes, separately /No/Yes, Inbuilt)
1.	Access Points proposed include radios for both 2.4 GHz and 5 GHz.			
2.	Have a robust design for durability			
3.	AP Must be IP 67 Certified and outdoor rated (datasheet of the Access Point should haveIP- 67 mentioned).			
4.	Operating temperature: -10 degree to 55 degree			
5.	Able to handle up to 250 Concurrent users.			
6.	Support 2X2 multiple-input multiple-output(MIMO).			
7.	Support simultaneous 802.11a/b/g/n/ac			
8.	For better performance on Smart devices like phones and tablets, the access point should support diverse multiple polarization of integrated antennas.			
9.	Support data rates up to 300Mbps on 2.4GHz Radio and 867 Mbps on 5GHz.			
10.	AP should provide minimum 26dBm transmission power for 2.4Ghz and 25dBm for 5Ghz. (EIRP should limited as per govt regulation for indoor AP's).			
11.	The Wireless AP should have the technology to improve downlink performance to all mobile devices including one and two spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.			
12.	Support AP enforce load-balance between 2.4 GHz and 5 GHz band.			
13.	Support receiver's sensitivity of -100 dBM or better.			
14.	Must have Channel selection based on measuring throughput capacity in real time and switching to another channel should the capacity fall below the statistical average of all channels without using background scanning as a method. Should also support coverage hole detection and performance optimization.			
15.	Support Proactive Key Caching and/or other methods for Fast Secure Roaming.			
16.	Support locally-significant certificates on the APs using a Public Key Infrastructure (PKI).			
17.	Support IDS/IPS.			
18.	Access Points support a distributed encryption/decryption model.			
19.	Access Points support encryption on CAPWAP/LWAPP Standard. Monitoring			
20.	Mesh support should support QoS for voice over wireless.			
21.	Support 16 WLANs per AP for SSID deployment flexibility.			
22.	Support HTTP/S, telnet and/or SSH login to APs directly for troubleshooting flexibility.			
23.	Support Power over Ethernet 802.3af.			
24.	Support 802.11e and WMM			
25.	Support QoS and Call Admission Control capabilities.			

Note : Any other features may be listed separately in continuation of the compliance sheet.

FINANCIAL BID PART-2
FOR SUPPLY AND INSTALLATION OF Wi-Fi ITEMS
AT
CSJM University, Kanpur
FINANCIAL BID FORMAT for Wi-Fi Items
(Bidders are requested to offer their price bid in the following format)

S.No.	Item Description	UoM	Qty	Unit Price	Taxes	Total Price inclusive of All Taxes
1	Wireless Controller					
2	Access Point TYPE-1 with POE injector & mounting mechanism					
3	Access Point TYPE-2 with POE injector & mounting mechanism					
4	Installation / Commissioning Charges					
	Total					

Note: As a part of commissioning of the aforesaid items, networking from switch to Access Point (AP), Controller shall be done by vendor with supply of networking cable and related items.

Signature of the bidder with seal