



भारतीय प्रौद्योगिकी संस्थान तिरुपति  
**Indian Institute of Technology Tirupati**  
Renigunta Road, Settipalli Post, Tirupati – 517506  
Telephone: 0877- 2503572, Email: [purchase@iittp.ac.in](mailto:purchase@iittp.ac.in)

**Tender No. IITT/CC/2022-23/17**

**Date: 31-May-2022**

**NOTICE INVITING TENDER FOR SUPPLY, INSTALLATION, TESTING AND  
COMMISSIONING OF WIRELESS ACTIVE COMPONENTS**

**(E-PROCUREMENT MODE ONLY)**

**CORRIGENDUM-I**

<b>S.No</b>	<b>TENDER CLAUSE NO.</b>	<b>In place of</b>	<b>To be read as</b>
1	Network functional requirements (Pg. No. 2, S.No.1), and corresponding item in Tech. Compliance	The users and devices should be given access to only specific resources and denied access to others based on their unified login credentials from central LDAP, the necessary hardware/software for deployment of LDAP to be part of the overall solution.	This point is removed, as IITT shall provide LDAP/Radius and associated NAC. However, the APs need to support standard network access protocols such 802.1X.
2	Network functional requirements (Pg. No. 2, S.No. 4), and corresponding item in Tech. Compliance	All devices to have Common Criteria Certification such as EAL/NDPP	Wireless controller/Wireless gateways to have Common Criteria Certification such as EAL/NDPP
3	Network functional requirements (Pg. No. 2, S.No. 5), and corresponding item in Tech. Compliance.	All WiFi devices to be WiFi6 certified by WiFi alliance	All WiFi APs to be WiFi6 certified by WiFi alliance
4	Network functional requirements (Pg. No. 2, S.No. 6), and corresponding item in Tech. Compliance	All WiFi device to support BT5/Zigbee support from Day 1	All WiFi device to support BT5/BT4/Zigbee support from Day1
5	Network functional requirements. “New point added” (Pg. No. 2, S.No. 12), and corresponding item in Tech. Compliance		The power levels of APs to comply with local regulatory norms. Bidder to mention the compliance regulatory norms as remarks, and attach the document with related points highlighted.
6	Commissioning Requirements (Wireless) (Pg. No. 3, S.No. 4), and	Successful bidder should submit a separate HLD/LLD document WiFi which is validated by OEM.	OEM to prepare and share the HLD & LLD document covering the best practices and provide configuration templates for handholding of remaining

	corresponding item in Tech. Compliance		devices to be implemented by SI/Bidder. Successful bidder/SI should engage the OEM Professional Services for above scope.
7	OEM Criteria for Wireless (Pg. No. 4, S.No. 7), and corresponding item in Tech. Compliance.	OEM should participate via only one authorised partner in this bid. MAF to be provided to the authorised partner and OEM should submit an undertaking that they will support IIT directly if the partner fails to fulfil their contractual obligations with respect to support during warranty or AMC period.	OEM should participate via authorised partners in this bid. MAF to be provided to the authorised partners and OEM should submit an undertaking that they will support IIT directly/via another authorized partner, if the partner fails to fulfil their contractual obligations with respect to support during warranty or AMC period.
8	OEM Criteria of wireless (Pg. No. 4, S.No. 13, stage 3, col. 3 'Delivery period (from PO)'), and corresponding item in Tech. Compliance	16 Weeks	24 Weeks
9	WLC (Pg. No. 5, S.No. 2), and corresponding item in Tech. Compliance	Proposed WLC should be on premise solution	WLC should be an on premise physical or virtual appliance. In case of virtual appliance, the supporting hardware and related accessories is under the scope of the bidder
10	WLC (Pg. No. 6, S.No. 30), and corresponding item in Tech. Compliance	The solution should support location tracking of all wireless devices (APs and Clients) on floor maps loaded on the Management controller from Day 1. No internet based location services should be utilised (Google and other online maps )	The solution should support location tracking of all wireless devices (APs and Clients) on floor maps loaded on the Management controller/NMS from Day 1. No internet based location services should be utilised (Google and other online maps )
11	WLC (Pg. No. 6, S.No. 31), and corresponding item in Tech. Compliance	The solution must support Automatic packet capture in event of a client failure	The solution must support Automatic packet capture in event of a client failure or anomalous events
12	WLC (Pg. No. 6, S.No. 32), and corresponding item in Tech. Compliance	The WLAN management plane should support a visual hierarchical location tree, where the nodes of the location tree inherit settings and configuration from the global level into subsequent levels in the hierarchy. The solution must also provide hierarchical alerts wherein sub-events are correlated under parent incident alert thereby enabling event correlation.	The WLAN management plane should support a visual hierarchical location tree, where the nodes of the location tree inherit settings and configuration from the global level into subsequent levels in the hierarchy. The solution must also provide hierarchical alerts either via a multi zone concept for event correlation or via an option wherein subevents are correlated under parent incident alert thereby enabling event correlation

13	WLC (Pg. No. 6, S.No. 33) , and corresponding item in Tech. Compliance	The solution should support automated root cause analysis of Wi-Fi issues such as low RSSI, low data rate, Authentication related issues on per client basis.	The solution should support automated /manual root cause analysis of Wi-Fi issues such as authentication related issues on per client basis, DHCP and DNS related issues. The solution to support automated root cause analysis for low RSSI and low data rate issues.
14	WLC (Pg. No. 6, S.No. 36), and corresponding item in Tech. Compliance	The solution must be able to detect and automatically prevent all wifi enabled devices such as smartphones bridging/ICS when connected to the network	The solution must be able to detect and automatically prevent any adhoc network / all wifi enabled devices such as smartphones bridging/ICS when connected to the network
15	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 6, S.No. 2), and corresponding item in Tech. Compliance	Access Point shall be able to powered up using PoE (.af)	Access Point shall be able to powered up using PoE/PoE+/UPOE (.af/.at/.bt)
16	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 6, S.No. 7), and corresponding item in Tech. Compliance	Access Point shall ship with metal-based mounting bracket for durability and reliability	Access Point shall ship with metal/fiber-based mounting bracket for durability and reliability
17	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 34, S.No. 8), and corresponding item in Tech. Compliance	Access Point shall be able to leverage current Access Point mount kit and cable conduit	Access Point shall be able to leverage current Access Point mount kit/cable conduit
18	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 6, S.No. 9), and corresponding item in Tech. Compliance	Access Point shall support Console port that uses Standard Port (RJ-45) type connection	Access Point shall support Console port that uses Standard Port (RJ-45)/serial USB connection/special SSID for initial config and during disconnected network situations
19	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 7, S.No. 10), and corresponding item in Tech. Compliance	Access Point should have 1x 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz	Access Point should have 1x 1Gbps, 2.5Gbps, 5Gbps Multigigabit Ethernet (RJ-45)
20	WiFi AP with 4x4 on 2.4GHz and 8x8 on 5GHz (Pg. No. 7, S.No. 22), and corresponding item in Tech. Compliance	Access Point must continue serving clients when the link to the controller is down. It should also have the option to authenticate users through the Radius server directly from Access Point during link unavailability to the controller.	Access Point must continue serving clients when the internet link to the controller is down. It should also have the option to authenticate users through the Radius server directly from Access Point during link unavailability to the controller with in the same LAN segment
21	WiFi AP with 4x4 on both radios (Pg. No. 7, S.No. 2),	Access Point shall be able to powered up using PoE (.af)	Access Point shall be able to powered up using PoE/PoE+/UPOE (.af/.at/.bt)

	and corresponding item in Tech. Compliance		
21	WiFi AP with 4x4 on both radios (Pg. No. 8, S.No. 7), and corresponding item in Tech. Compliance	Access Point shall be able to leverage current Access Point mount kit and cable conduit	Access Point shall be able to leverage current Access Point mount kit/cable conduit
22	WiFi AP with 4x4 on both radios (Pg. No. 8, S.No. 8), and corresponding item in Tech. Compliance	Access Point shall support Console port that uses Standard Port (RJ-45) type connection	Access Point shall support Console port that uses Standard Port (RJ-45)/serial USB connection/special SSID for initial config and during disconnected network situations
23	WiFi AP with 4x4 on both radios (Pg. No. 8, S.No. 9), and corresponding item in Tech. Compliance	Access Point should have 1x 1000, 2500 Multigigabit Ethernet (RJ-45) – IEEE 802.3bz	Access Point should have 1x 1Gbps, 2.5Gbps, 5Gbps Multigigabit Ethernet (RJ-45)
24	WiFi AP with 4x4 on both radios (Pg. No. 8, S.No. 15), and corresponding item in Tech. Compliance	Must have -97dB or better receiver sensitivity	Must have -96dB or better receiver sensitivity
25	WiFi AP with 4x4 on both radios (Pg. No. 8, S.No. 21), and corresponding item in Tech. Compliance	Access Point must continue serving clients when the link to the controller is down. It should also have the option to authenticate users through the Radius server directly from Access Point during link unavailability to the controller.	Access Point must continue serving clients when the internet link to the controller is down. It should also have the option to authenticate users through the Radius server directly from Access Point during link unavailability to the controller with in the same LAN segment
26	Clause 13 (Warranty of quality and quantity), and corresponding item in Tech Compliance	2 years AMC after completion of OEM standard warranty may be quoted as an optional.	2 years AMC after completion of OEM standard warranty need to be quoted as an optional item, and this item shall not be part of tender evaluation. This 2-year AMC is for future purposes only.
27	Clause 14 (Liquidated Damages, Pg. No. 18) New line added, at the end of the section.		Liquidated damages shall not be applicable provided the standby stagewise release of temporary items are supplied and made operational.
28	Clause 15 (Delivery Schedule, Pg. No. 18)	“supply, installation of ordered items within 16 weeks.....”	“supply, installation of ordered items within 24 weeks ....”

Sd/-  
Deputy Registrar