ANNEXURE – 1

TECHINICAL SPECIFICATION FOR OUTDOOR WIRELESS SOLUTION

Sl. No.	Features	Specifications	Compliance (Yes/No)
A. Solution requirement			
1	Architecture	Centralized WLAN architecture where Controller (Virtual / Hardware) should support management of up to 100 access points. In case of virtual and if required, it should be quoted with required server/hardware for the controller.	
2		Single virtual controller or hardware controller should support up to 2000 concurrent devices and up to 500 guests. Required licenses must be supplied if applicable.	
3		Offered system must be highly available and must have no single point of failure. Controller must be deployed in 1+1 redundancy.	
4		Support Point to Point / Point to Multipoint solution	
5		Offered solution should support a single anchor for RADIUS requests from all wireless users, regardless of which access point they connect through.	
6		Support 802.11a/b/g/n/ac wireless standards	
7	Authentication & Encryption	MAC, 802.1x, web based authentication. Offered solution must have the ability to utilize RADIUS attributes to assign users or devices to specific roles/VLANs.	
8	Security	An integrated wireless intrusion detection system shall safeguard the network from unauthorized or rogue access points, clients, and other devices that could potentially harm network operations.	
9		WLAN solution should detect and protect Ad-hoc connections (i.e. clients forming a network amongst themselves without an AP).	
10		System should detect and prevent windows bridge (i.e. client that is associated to AP is also connected to wired network and enabled bridging	

		between two interfaces)	
11	**RF Scanning**	WLAN solution shall be capable enough to scan the 2.4 or 5GHz radio bands to identify sources of Wi-Fi and Non Wi-Fi interference sources, and make the results available locally and to a remote management solution.	
12	**High Availability**	In the event of a failure of the master controller, a standby controller or AP shall automatically take over the master role. Clients shall not disconnect from other AP's during failover and if master AP or controller is not available, other AP's shall not reboot even after any time limit.	
13	**RF MANAGEMENT**	Automatically assigns channel and power settings for all AP's in the network according to the change in the RF environment	
14		Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.	
15		Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software	
16		Solution must have the ability to intelligently and dynamically load-balance devices without receiving a new association request from the device	
17		For advance forensic should perform spectrum analysis to detect and classify sources of interferences. System should provide chart displays and spectrograms for real-time troubleshooting and visualization.	
18	**Access Point Management**	Automatic and secure updates of firmware and software on all APs without user intervention	
19		All AP configuration and service delivery	

		information centrally managed and maintained	
20	**Access Control**	Rules for access rights based on any combination of time, location, user identity, device identity, and extended attributes from the authentication database	
21		Solution should provide the capability to support dynamic role updates of users based on messages received through external APIs	
22	**Quality of Service**	Solution must Provide application, user, and policy based QoS	
23		Battery-saving features such as proxy ARP for clients, multicast/broadcast filtering, large DTIM configurations, multicast/broadcast to unicast conversion integrated into the AP and controllers without requiring client side software components	
24	**Management**	Command line interface to control and manage all aspects of the WLAN system from controller	
25		SNMP v3	
26		Browser-based system for total solution management including: configuration, monitoring, troubleshooting.	
27		Single dashboard view of overall network, user, and security status	
28		Administrative rights partitioning - different admins have different rights.	
B. SPECIFICATION FOR OUTDOOR ACCESS POINT			
1	External Protection	Must be IP67 rated for dust and water protection. No third party casing will be accepted.	
2	Ports	AP should have two Auto-sensing 10/100/1000 port	
3	Connectivity	Support 802.3 standard Power-over-Ethernet (PoE+) with full capacity operation at full power of the radios	
4	Power	Must support Direct 100- 240 VAC /DC and PoE+ to power up access point	
5	Mobility	Minimum of 8 SSIDs available on each AP simultaneously without negatively impacting system performance	
6		Access Point radio should be minimum 3X3 MIMO with minimum 3 spatial streams or	

		more. Dual Radio capable	
7	Security	Capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical "touch" and no additional cost.	
8	Management	Real-time, fully integrated spectrum analyzer capabilities on the APs, that does not require dedicated sensors or separate operating system running on the AP radios	
9		The Access Point should have the technology to improve downlink performance to all mobile devices	
10	High throughput	802.11ac ready from day one. Supported data rates: 1.3 Gbps on 5GHz & 600Mbps on 2.4GHz	
11	Diagnostics	Real time packet capture on the APs, without disconnecting clients	
12	Mounting	Access point should be supplied with OEM mounting kit and shall support pole, wall, and roof mounting options	
13	Operating Temperature	The Access point shall be rated for operation over an ambient temperature range of 0° to 60°C	
14	Antenna	Integrated/external antenna, minimum 6 nos per access point, 5dBi gain for both 2.4GHz and 5GHz	