Corrigendum (Version -1 Dated March 10, 2015)

Following are the amendments / changes / insertions / deletions as per Corrigendum (Version -1 Dated March 10, 2015) to the Tender Document No. ULWF/CCC/12015 for Upgrdation of LAN & Wi-Fi dated February 12, 2015.

SN.	Item Clause No. / Page No.	Original clause in Tender	Revised Clause (To be read as)
1.	Core Switch SN. 2 / Page No. 21	Switch should have internal redundant Power supplies and fans.	Switch should have internal redundant Power supplies.
2.	Core Switch SN. 9 / Page No. 21	Should have Static Routing, RIP, OSPF, VRRP, ISIS and PIM from day one.	Should have Static Routing, RIP, OSPF, VRRP and PIM from day one.
3.	Core Switch SN. 18 / Page No. 21	Should support MPLS and ISIS.	This clause stands deleted.
4.	Distribution Switch SN. 3 / Page No. 22	Should support stacking up to 6 units or more in a single stack managed by a single IP address and necessary stacking ports should be available from day	Should support stacking up to 4 units or more in a single stack managed by a single IP address and necessary stacking ports should be available from day one.
5.	Distribution Switch SN. 17 / Page No. 22	Should support MPLS and ISIS.	This clause stands deleted.
6.	Access Switch (Type 1) SN. 15 / Page No. 23	Should support MPLS and ISIS.	This clause stands deleted.
7.	Access Switch (Type 2) POE SN. 15 / Page No. 24	Should support MPLS and ISIS.	This clause stands deleted.
8.	Access Switch (Type 3) SN. 15 / Page No. 25	Should support MPLS and ISIS.	This clause stands deleted.
9.	Wireless Controller SN. 4 / Page No. 26	Controller should support minimum 256 WLAN's.	Controller should support minimum 64 WLAN's.
10.	Wireless Controller SN. 13 / Page No. 27	System should provide DOS attacks and Intrusion Detection and Prevention and Control for any Rough Access Points.	Controller / System should provide DOS attacks and Intrusion Detection and Prevention and Control for any Rogue Access Points.
11.	Wireless Controller SN. 14 / Page No. 27	The access point should be able to scan for rogue access points and the controller should be able to locate them on a floor map. The controller / system should be able to send a notification to the administrator when a rogue access point has been detected.	The access point should be able to scan for rogue access points and the controller / system should be able to locate them on a floor map. The controller / system should be able to send a notification to the administrator when a rogue access point has been detected.

12.	Wireless Controller SN. 22 / Page No. 27	When Mesh is enabled the controller should be able to show the mesh topology on floor plans.	This clause stands deleted.
13.	Wireless Controller SN. 25 / Page No. 28	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.	Controller / System 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.	Wireless Controller SN. 31 / Page No. 28	System should be able to send password direct through Email and SMS to the user.	Controller / System should be able to send password through Email and SMS to the user.
15.	Wireless Controller SN. 32 / Page No. 28	System should be able to generate one click password for single user, multiple users or single user multiple devices.	Controller / System should be able to generate one click password for single user, multiple users or single user multiple devices.
16.	Wireless Controller SN. 33 / Page No. 28	System should support user management features like Rate limiting based on time based WLAN Access and User Profile for WLAN etc.	Controller / System should support user management features like Rate limiting based on time based WLAN Access and User Profile for WLAN etc.
17.	Indoor Access Point (AP) – A SN. 2 / Page No. 29	802.11n Access Point should be able to power up using standards 802.3af POE input, and at the same time Operate in full MIMO mode. It must have option to power through 12V DC power Adapter also.	802.11n Access Point should be able to power up using standards 802.3af POE input, and at the same time operate in full MIMO mode. It must have option to power through external AC power source also.
18.	Indoor Access Point (AP) – A SN. 6 / Page No. 29	AP should have -99dB or better receiver sensitivity.	AP should have -98dB or better receiver sensitivity.
19.	Indoor Access Point (AP) – A SN. 14 / Page No. 29	AP should have technique to provide better reception for hard to hear clients and consistent performance while clients change their orientation i.e. beam forming / polarization.	AP should have technique to provide better reception for hard to hear clients and consistent performance while clients change their orientation i.e. beam forming / polarization / any similar technology.
20.	Indoor Access Point (AP) – A SN. 15 / Page No. 29	AP should support the operating temperature 0° to 45° C and Humidity : 15 to 95% non – condensing.	AP should support the operating temperature 0° to 40° C and Humidity : 15 to 90% non – condensing.
21.	Indoor Access Point (AP) – B SN. 2 / Page No. 31	The AP shall have at least one Gigabit Ethernet port supporting 10/100/1000BaseT with 802.3af/at PoE support, 3 port 10/100 including 1 port PoE out to power VOIP phone and one Digital PBX Pass through port support.	The AP shall have at least one Gigabit Ethernet port supporting 10/100/1000BaseT with 802.3af/at PoE support and 3 numbers of 10/100BaseT ports.
22.	Indoor Access Point (AP) – B SN. 8 / Page No. 31	The AP shall support indoor wireless mesh configuration.	The AP shall support indoor wireless mesh configuration in synchronization with controller /

			system.
23.	Indoor Access Point (AP) – B SN. 14 / Page No. 32	AP should provide L2TP/ PPoE or equivalent tunneling support.	This clause stands deleted.
24.	Indoor Access Point (AP) – B SN. 20 / Page No. 32	AP shall have WISPr support for walled garden deployments as well as provisioning Wi-Fi hotspots with time based user access/ session control.	This clause stands deleted.
25.	Indoor Access Point (AP) – B SN. 23 / Page No. 32	AP shall support Captive portal for guest user authentication.	AP shall support Captive portal for guest user authentication in synchronization with controller / system.
26.	Indoor Access Point (AP) – B SN. 25 / Page No. 32	Operating Temperature: 0 to 50 degree Centigrade.	Operating Temperature: 0 to 40 degree Centigrade.
27.	Indoor Access Point (AP) – B SN. 26 / Page No. 32	Operating Humidity: 15% - 95% non – condensing.	Operating Humidity: 15% - 90% non – condensing.
28.	Outdoor Access Point (AP) SN. 11 / Page No. 33	AP should support the operating temperature -10° to 55° C and Humidity: 15 to 95% non – condensing.	AP should support the operating temperature 0° to 55° C and Humidity: 15 to 90% non – condensing.
29.	Specification for passive and other miscellaneous items SN. J / Page No. 37	CAT 6 Outside Plant UTP Cable.	Here bidders can quote the cable with same specifications or better cable which can be used for outdoor installations in all weather conditions such as Rain, Moisture, Humidity, Heat etc. without any failure.

Note: In case of Indoor Access Point (AP) – B (For Director's Office / HODs offices) on Page number 31-32, Bidders / Vendors can meet this requirement by providing controller based indoor access point using Managed Switch with the desired ports and other requirements in relevant clauses laid in tender.