Controller for Wi-Fi access			
Sr. No.	**General**	**Specification**	**Compliance Requirement**
		Should be Rack Mountable appliance	
		Should include security features available within the controller or externally which shall operate both in “bridge mode” or "transparent mode” apart from the standard NAT mode.	Will not be compulsory for compliance
		Appliance provided must have dual redundant internal power supply	
		The controller should be web managable	
	Wireless Controller		
		Wireless controller shall controll 500 Access Points from day one but expandable upto 1000 Ap’s	
		The appliance should support IEEE 802.11a/b/g/n standards-based wireless Access Points	
		Supports strong Authentication and Encryption Standards Include Open/ WEP64/ WEP128/ Shared, Guest Captive Portal, WPA /WPA2 802.11i Preshared key,WPA / WPA2 802.11i with Radius support	
		The wireless controller support the following types of client load balancing:	
		a)Access Point Hand-off - the wireless controller signals a client to switch to another access point.	
		b)Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency automatically	
		Support Fast Roaming (IEEE 802.11r) or equivalent. This includes Seamless rapid mobility across VLAN and subnets Includes 802.11i pre-auth and fast roaming	
		Support fast roaming across L2, and L3 for video, audio and voice over wireless client	
		Allow IP connectivity between the Controller and the APs for external VLAN routing where the Controller and the APs are on different VLANs	
		The wireless controller should include the following features.	
		1. Wireless guest management	
		2. Captive portal with capability to capture login credentials or identity	
		3. Wireless Mesh, **Bridging Features**	Wireless Mesh
		4. BYOD (Bring Your Own Device) Support	
		5. User and application control	
		6. Encrypted Remote Access point support	
		8. Traffic Rate shaping	
		BYOD should be having below features (separate appliance must be quote if wireless controller doesn't have this feature)	
		Detect client device Mac address, device type(such as windows device, Android device, Iphone, Ipad, blackberry, etc) and host name	
		controller should be able to allow or deny traffic based on device type (such as windows device, Android device, Iphone, Ipad, blackberry, etc)	

		Controller should be able controll the bandwidith based on device type(such as windows device, Android device, Iphone, Ipad, blackberry, etc)	
		The wireless Controller should support the following RF Management features	
		a) Having Automatic Channel Allocation	
		b) Having Automatic Power Control	
		c) Supporting Neighbourhood scanning of RF environment to minimise neighbouring AP interference and leakage across floors.	
		d) Having Coverage Hole Detection	
		e) Providing alerts when APs are down or compromised RF environment is detected	
		f) Having Self healing - Automatic neighbouring AP power increase to fill in for coverage losses	
		Support 802.11i/WPA/WPA2 Enterprise with standard interface to external AAA/RADIUS Server	
		Support Different AAA Server per SSID	
		Support IEEE 802.11e Media Access Control (MAC) Protocol, Wi-Fi Multimedia (WMM) and Traffic Specification (TSPEC).	
		Restrict ingress traffic to the wired network - should also allow restriction of bandwidth per user, device, SSID	
		Prioritise all traffic by a minimum of four categories (highest to low voice, video, best effort and background	
		The wireless Controller should support Rogue AP detection and Blocking	
		It should be able to detect the 3rd party wireless enabled Mobile devices with Hot spot programs and able to prevent the users from connecting those mobile devices	
		Wireless Controller should able to Block Intra SSID traffic	
		It should Include Wireless Guest Access Provisioning for Allowing non-IT staff to create Guest account,Assign Time quota, generate temp password, print, email or SMS the information to the Guest user	
		The wireless Controller should able to detect the following Wireless Intrusion Attacks such as Unauthorized Device Detection, Rogue/Interfering AP Detection, Ad-hoc Network Detection and Containment, Wireless Bridge Detection, Misconfigured AP Detection, Weak WEP Detection	
Additional Security & Features			
		The OS on the wireless controller or the external security device should be “IPv6 Phase II Ready” certified	
		Basic Firewall feature to prevent and block unneccsary traffic between various SSID's	
Interface and Connectivity			
		The Wireless controller should support two or more gigabit copper interfaces with auto sensing 10/100/1000 capability. **If external security device having firewall, Gateway Anti-Virus, DLP, etc., with storage for logs is provided, then it shall have minimum 6 x 10/100/1000BaseT network interfaces.**	The Wireless controller should support two or more gigabit copper interfaces with auto sensing 10/100/1000 capability.
		Should have 1 console port	
		Should support VLAN tagging (IEEE 802.1q)	
	Authentication		
		Should have authentication for Users/Admins (Local and Remote – RADIUS, LDAP & TACACS+)	
		Support for RSA SecureID or other Token based Products	
		Support for Native Windows Active Directory and Novell eDirectory Integration	

		Should support PKI / Digital Certificate based two-factor Authentication for all type of users	
	Reporting		
		The Contrroller should be able to provide all reports.	

Access Points	Number of external antennas will not be critical factor for compliance.

Manpower Rates per annum should be quoted. May be extended for three years.

University reserve the right to increase or decrease quantity of any item or drop completely.

Minor deviations may be waved off on availablility of proper justification