

Annexure-1 (Scope of Work)

1. Introduction

Chaudhary Devi Lal University, Sirsa is planning to replace its old Wi-Fi setup with a new Wi-Fi set up along with Optical Fibre Ring network all around the University and to install the new Wi-Fi setup with the sophisticated equipments of latest specifications at the following sites/buildings in order to facilitate its students, research scholars, and faculty members, non-teaching staff and to facilitate administrative offices.

Chaudhary Devi Lal University (CDLU), Sirsa invites **technical and financial proposal** for Supply, Installation, Testing and Commissioning of WI-FI setup at CDLU, Sirsa as per details given in this document. CDLU has strength of approx. **5000** students, **1000** teaching & administrative staff. It also has hostels for boys and girls students with capacity of **1500** students approx.

- 1. CV Raman Bhawan Teaching Block**
- 2. Tagore Bhawan Teaching Block +Media Centre**
- 3. Vivekananda Library Building**
- 4. Faculty House**
- 5. Construction Branch**
- 6. VC Camp Office + VC Residence**

The entire university campus, encompassing all the previously mentioned locations, will be interlinked via an Optical Fiber Cable (OFC) backbone with 10Gbps/100Gbps capacity, utilizing a Ring Mechanism configuration. In this Ring Mechanism, a star network will be established for each building. Additionally, Route Markers will be strategically placed approximately every 50 or 100 meters (as per the requirement) along the underground Optical Fiber Network nearby roads of the University. For a visual representation of the university layout, please refer to the attached map in Annexure -I.

रेलटेल
RAILTEL

2. Scope of Work

This is a **turnkey project** for replacing and expanding existing centrally controlled wireless network setup and installation of new Wi-Fi network setup in Chaudhary Devi Lal University, Sirsa.

1. The University invites **technical and financial proposal** who have the capability to provide a **TOTAL TURNKEY** solution which includes
 - (a) Planning and Pre-Documentation
 - (b) Supply, Installation, configuration, testing, commissioning
 - (c) Integration with the existing environment
 - (d) On-site training to the concerned staff members
 - (e) Final Documentation of whole Project
 - (f) Five years of comprehensive warranty, and three years of post-warranty AMC(if required, Please quote rate per year).
2. The Vendor/Firm shall be responsible for providing all required materials, equipments and services for which general specification specified herein or otherwise which are required to fulfil the intent of ensuring operability, maintainability, and reliability of the complete equipments covered under this project within Vendor/Firm's quoted price. **We are not mentioning any quantity that is the work of Vendor/Firm they have to plan and build network layout structure by visiting and understanding the actual requirements at the sites in the University.**
3. The Vendor/Firm may quote and include in their bill of quantities any components, which they deem necessary for successful implementation of the project.
4. All products being quoted should be compatible and seamlessly integrated with the existing networking infrastructure in Chaudhary Devi Lal University, Sirsa.
5. Each product should come with a comprehensive on-site warranty including labour and spares for **Five years** starting from the date of installation/inspection.
6. **The existing OFC/Switches must be used wherever possible. All the Connectivity to various departments/labs and other areas where existing switches and network are working has to be connected with the Wi-Fi network.**
7. The Vendor/Firm must ensure that the resources (personnel) allocated for each of the above tasks are competent and capable of meeting all the technical requirements to ensure that the broad objective of delivery of services as per expectations is fully met.
8. **The firm shall be responsible to draw complete site plan and network layout in the form of diagram or chart work plan layout and the equipments to be installed at the site accordingly.**

3 General Technical Specifications & Requirements

- 1 The technical & financial proposal should be valid for minimum period of 90 days.
- 2 **Complete technical specifications with complete network layout structure with model number of each component (Switches/WAP/Passive) and detailed specifications should be sent along with the proposal. Proposal not matching the minimum technical specifications will be rejected.**
- 3 A site survey is required to find out Radio Frequency (RF) occurring already in CDLU environment and its overall effect.
- 4 The proposed system should support RF Coverage Map to allow troubleshooting of any issue.
- 5 The Vendor/Firm shall provide OEM's authorization letter confirming that the OEM supports the Vendor/Firm.
- 6 The Vendor/Firm shall submit the following documents along with the technical proposal:
 - a. WPC approval for APs
 - b. Type approval from TEC for the switches
 - c. Relevant UL/IEC certification
 - d. Technical compliance report, Installation plan
 - e. Cabling layout plan
 - f. Deployment architecture
- 7 The Vendor/Firm should specify the detailed requirements for active components, passive components, civil works, and Installation & Servicing.
- 8 **The Vendor/Firm should specify all technical specifications of the distribution L3 switches, L2 switches, Passive components, Civil works and Installation & Services in the prescribed format.**

रेलटेल
RAILTEL

4 Technical Requirements

The Vendor/Firm should specify the following requirements in details with network layout structure and different positioning of all active and passive components with the model number and detailed specifications of all active components. Also specify the number of users catered by each Wireless Access Point.

The topology must involve redundant fibre-optic connections between the core (Layer-3) switches (CS1 & CS2), Distribution Switches for each Building (Wherever is required – with Detailed Plan) and the access (Layer-2) switches in the racks.

- There are different racks in different locations.
- Core switches within a single rack are required to be inter-stackable via stacking cables.
- All requisite licenses for achieving all the features mentioned in this document must be **perpetual** and must be included from the day of commissioning.
- The distribution switches must be configurable to create groups for each VLAN to act as a virtual logical gateway (default gateway) for all the hosts within the VLAN for redundancy.
- Switches must be rack mountable in a standard network rack. All accessories required for mounting must be included in the quote.
- All quoted core switches must contain at least two hot-swappable redundant power supplies and include IEC type D/M (3 round pin) power cords for all power supplies.
- The Core Switch should be high-performance switches that feature high port density, routing, and ultra-low latency, designed to be deployed as TOR switch
- Non-blocking architecture. The switch should have essential requisite certifications.

Switches must support the following

- o 48x1G/10G/25G/+ 8x40G/100G network support (48 Port - Core Switches all Fiber Ports)
- o 1G/10G network support (24 Port Distribution Switches + 10Gx 8SFP+)
- o 1G/10G network support (24/16/12/8 Port Access Switches + 10G x 2 or 4 SFP+)
- o IEEE 802.1Q VLAN tagging
- o 802.1Q VLAN on all ports with support for a minimum of 4000 VLANs.
- o Spanning Tree Protocol as per IEEE 802.1d
- o Multiple Spanning-Tree Protocol as per IEEE 802.1s
- o Rapid Spanning-Tree Protocol as per IEEE 802.1w
- o Support for Self-learning of unicast & multicast MAC addresses and associated VLANs
- o Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
- o “Port Mirroring” functionality for measurements using a network analyser

- o Minimum 64 multiple Spanning-tree instances.
- o RoHS Compliance
- o IEEE 802.1x support
- o IPV6 and IPV6 & IPV4 dual stack

Wireless access points must support the following

- o WAP should be Wi-Fi CERTIFIED 6™.

Indoor/Outdoor WAP:

- i. Must have at least 3.5 Gbps aggregate data rate.
- ii. Must have at least 4x4:4 on 5 GHz and 2.4 GHz radio
- iii. Must support DL-MU-MIMO and UL-MU-MIMO
- iv. Must support DL-MU-OFDMA and UL-MU-OFDMA
- v. Must support security at client and enterprises level WPA3 with all standard/enterprises level security

Wireless controller must support the following:

- o The controller shall support deployment flexibility without compromising any features.
- o The controller should be from same OEM of active network devices which are being quoted by Vendor/Firm for compatibility. It should also cover existing network devices with new/upgraded network devices installed in the campus of University.
- o The controller shall support **minimum 5 Gbps tunnelling capacity and shall be upgradable to 10 Gbps.**
- o The controller shall support 2 x 10 G/Multigigabit copper uplink.
- o Wireless Controller shall support link aggregation and load sharing between Access Point to WLC links.
- o Controller should have scalability to **support 1000 Access Points (APs)** from day one without any change and controller **should support 256 AP** from day one without licensing charges.
- o Run OVA format file by virtual software or system
- o Centralized Management
- o Local data forwarding, no user traffic sent to the controller
- o Bank-grade TLS encryption from end-to-end with X.509
- o certificate based authentication
- o User and privilege management, support multi-factor safety
- o authentication
- o Mobile app for iOS and Android
- o Network-based management and unified device configuration
- o Network/device/client/guest monitoring
- o Network topology to display the visual information of device and client
- o Layer2 and Layer3 based AP discovery

- Access Security and Control
- Supports access policy configuration (blacklist, whitelist, time policy schedule)
- Multiple WLAN security type including open, personal, enterprise, ppsk, etc
- Bandwidth rules for client access
- Supports firewall to control both wired and wireless client
- Rogue AP detection and alert
- Reporting and Monitoring
- Real-time devices and client monitoring
- Detailed reports by network, device, client, etc
- Retrieval of historical data for statistical observations
- Customize monitoring panel (add and remove chart, adjust the display order)

Network Management System (NMS) should support the following:

- Single NMS should be able to manage Wired and Wireless devices. It should be from same OEM of active network devices or open source which are being quoted by Vendor/Firm for compatibility. It should also cover existing network devices with new/upgraded network devices installed in the campus of University.
- Should have Powerful monitoring engine which can scale and manage 500s of hosts and servers.
- Should have Comprehensive web dashboard giving the visibility of complete network components and monitoring data.
- Should have multi-tenant capabilities where multiple users have access to NMS dashboard.
- Should have extendable architecture which can easily integrate with third-party applications with multiple APIs.
- Should have features like fast alerting system, sends alerts to admins immediately after any issue is identified.
- Should have multiple plugins, custom coded plugins can also be used with NMS
- Should have good log and database system storing everything happening on the network with ease.
- Should provide proactive planning feature helps to know when it's time to upgrade the infrastructure.

रेलटेल
RAILTEL

5. Acceptance Parameters for the Proposed Solution

Coverage and Capacity Planning

- i. On-site site survey by the Vendor/Firm is mandatory to plan Wi-Fi deployment in each floor of each building.
- ii. The Vendor/Firm should provide the location of Access Points on the floor plan for all buildings
- iii. The Vendor/Firm should provide OEM-certified coverage heat map for 2.4 GHz and 5 GHz separately with -65 dBm RSSI threshold for 2.4 GHz and 5 GHz. All coverage holes in the premises should be indicated clearly.
- iv. The Vendor/Firm should provide OEM-certified AP coverage redundancy map and how many number of users will be served by each AP.

Physical Installation

- i. Inspect installation of Network racks, OFC, UPS, Power Cables, UTP cables and Network Switches.
- ii. Configuration check on controller including the policies.
- iii. Test the physical mounting of each Access Point.
- iv. Test each Access Point connectivity to the central controller.

Wired Network Test:

- i. Perform OTDR/RFC 2544 tests for all OFC links and submit reports.
- ii. Perform end-to-end connectivity test of all UTP links and submit reports.
- iii. Check reachability and latency test on all Network Switches and submit reports.

Wi-Fi Controller Configuration Test:

- i. Check authorized Wi-Fi set up for each Subnet / VLAN / Location as the case may be.
- ii. Check both Authorized user and Guest user policies.
- iii. Test each Access Point if they have the right authorized and guest policy.
- iv. Check Wi-Fi prevention policy for each subnet, VLAN and location.
- v. Check the configured alerts and alert delivery methods.
- vi. Check the administrative users and their access rights.
- vii. Check the configured reports (content, delivery frequency, recipient list).
- viii. Check the automatic backup and archival parameters.

- ix. Check archival of logs.

Commissioning Test

- i. Test for all Access Points connectivity to the controller.
 - ii. Test and verify authorized Access Points inventory and authorized client inventory.
 - iii. Verify external Access Points list and verify uncategorized / unauthorized client list.
 - iv. Verify if all authorized wireless devices are tagged to the right location.
 - v. Test for authorized client connection to authorized Access Point and respective SSID as per the set authentication policy.
 - vi. Test for Guest client connection to authorized Access Points and respective SSID as per the set authentication policy.
 - vii. Test if the Access Points are operational after shutting down the controller.
 - viii. Test if automatic Rogue Access Points prevention is working on all types of rogue APs.
 - ix. Test if unauthorized client association to authorized Access points is automatically prevented.
 - x. Test if automatic client Mis-association prevention is working.
 - xi. Test if Ad-Hoc Networks are detected and automatically prevented.
 - xii. Test if Mac-Spoofing is detected.
 - xiii. Test if the automatic prevention of Honeypot (with Multipot) is functional.
 - xiv. Test is Denial of Service (DoS) Attack is detected.
- 3 Testing of deployment of policies, firmware updating remotely through the controller.
 - 4 Testing WIPS functionality across the subnet.
 - 5 The entire testing exercise should complete in all respects.

6 Documentation and Reports

- i. Documentation of the entire project along with testing reports must be submitted to CDLU, Sirsa.
- ii. Documentation must include RF Coverage Heat Maps clearing showing that the -65 dBm RSSI requirement within the **whole campus of the University** is met.
- iii. Documentation must include a complete network diagram that clearly depicts the Switch Management IP Address, Switch Location, AP Location, and Switch Port to each AP.
- iv. Documentation must include complete configuration in a step-by-step manner.

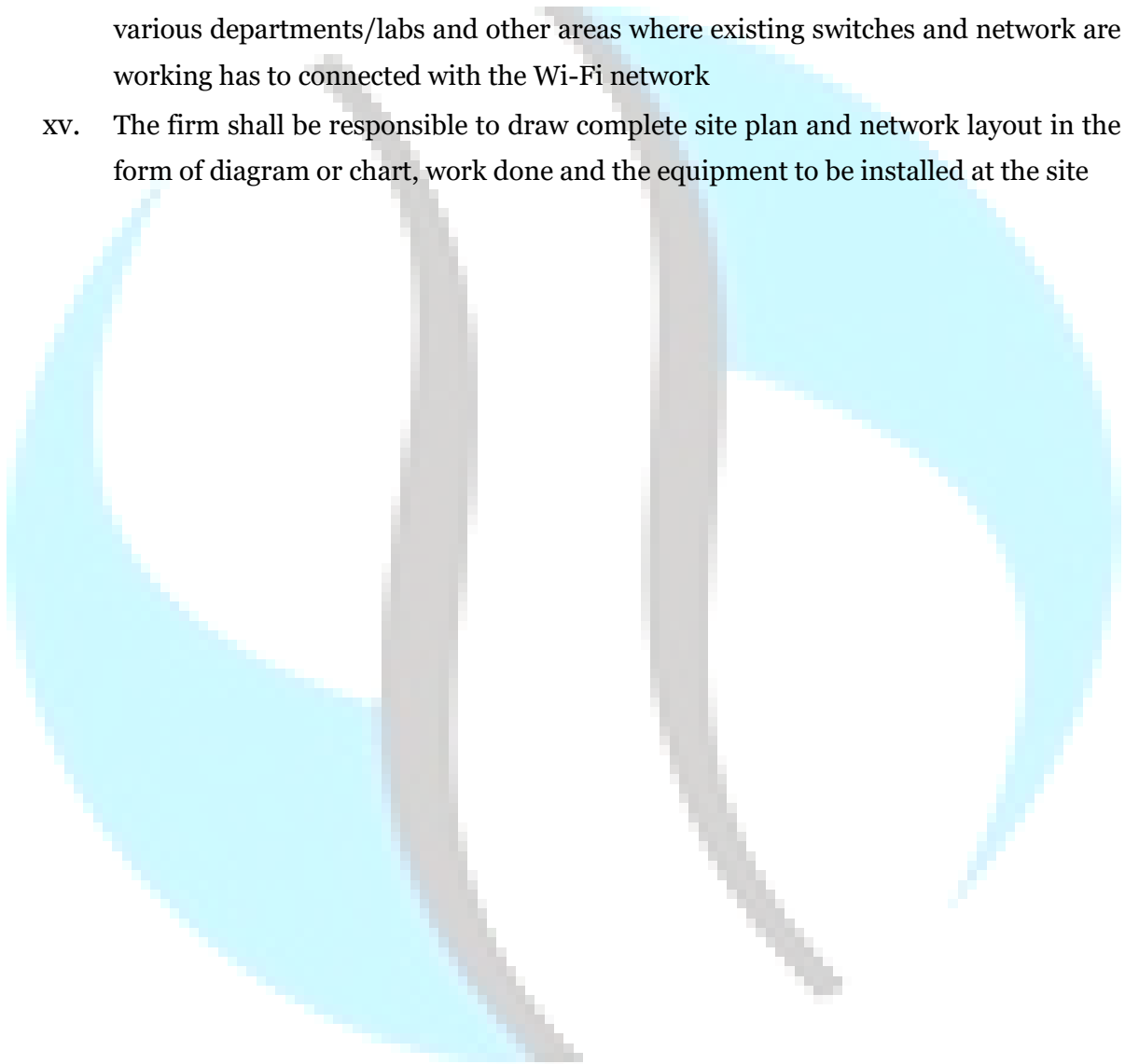
Solution Fine Tuning and Handover to operations team of CDLU

- 3 Fine tune Wi-Fi Access policies and security policies.
- 4 Rebuild authorized device inventory and remediate mis-configured APs.

7 License, Warranty and Support Requirements

- i. The total solution should include licenses for all necessary features from the first day of the installation.
- ii. **All the licenses quoted should be perpetual.**
- iii. All the features and signatures including WIPS available at the time of expiration of license should continue to work. Renewal of licenses should be required only for new features and updates/releases announced by the OEM after the contract expires.
- iv. The total solution should have **5-year on-site warranty** for Access Points, Switches, UPS & batteries, cabling & accessories, and controller.
- v. The total solution should include technical support for software/firmware and software upgrades for a controller, Access Points, and Switches **for 5 years.**
- vi. The total solution against the supply order shall be the latest version and should be under support for a minimum of the **next 5 years.**
- vii. The total solution should be upgradable to the latest stable version, as and when available, at no extra cost.
- viii. The items features of active and passive components mentioned in this requirement are the general features. The Vendor/Firm may quote and include in their bill of quantities of any components, which they necessary for successful implementation of the project.
- ix. The proposal should also include **additional 3 years' AMC** specified as a separate line item.
- x. Warranty support should **include 4 hrs. response time** and provision of replacement along with appropriate configuration and installation in next business day for Hardware.
- xi. The vendor should have enough spare parts and backup of configurations and setup etc., to provide standby in case of any repair in the equipment's, cables, software etc., and the repair/replacement of the original equipment should be done within 24hours.
- xii. Design of the Wireless Network in its deployment should adhere to the Governments norms defined and should comply with all its security measures.
- xiii. Should provide single point of contact and should provide call logging and escalation matrix.

- xiv. The existing OFC/Switches must be used wherever possible. All the Connectivity to various departments/labs and other areas where existing switches and network are working has to connected with the Wi-Fi network
- xv. The firm shall be responsible to draw complete site plan and network layout in the form of diagram or chart, work done and the equipment to be installed at the site



रेलटेल
RAILTEL