SECTION-III:
TECHNICAL SPECIFICATIONS

Table – 1: Wireless Access Point for Indoor with following specifications **– 2 Nos**

S. No	Specification / Requirement
1	**Wireless Access Point**
1.1	Indoor Use
2	**Radio Specifications**
2.1	Access Point should be dual-band, dual-radio indoor access point
2.2	The Access Point should support 4x4:4 + 2x2:2 streams SU/MU MIMO on 5GHz and 2.4GHz
2.3	AP should support IEEE 802.11 a/b/g/n/ac/ax amendments.
2.4	Antenna should direct the radio signals per-device on a packet-by-packet in real-time to support high device density environments. Should have 3 dBi gain. Antenna operates without the need for device feedback to support devices using legacy standards.
2.5	AP should provide 23 dBm EIRP on 2.4GHz and 5 GHz, -93 dBm on 2.4GHZ and -98 dBm on 5GHZ receive sensitivity.
3	**Interface and Power Requirements**
3.1	AP should have 2 Ethernet ports including one 2.5 Gig port
3.2	It should have less than 21.95Watts power consumption for full functionality including USB port on PoE
3.3	Should have on-board IoT radio. Should have option to add modular IoT radio using USB port. Both onboard and modular IoT radios should support BLE and Zigbee protocols.
4	**Networking Requirements**
4.1	AP should have capacity to handle minimum 300 Concurrent devices.
4.2	AP should be flexible hardware to be deployed as Standalone, Controller-less (Cluster), Controller-based, Cloud-based.
4.3	Should have IPv6 support, IEEE 802.1Q, Band balancing, airtime fairness, QoS, L2/L3/L4 ACL
4.4	AP should be able to act as sensor for WIPS, Location analytics engine and Network analytics engine.
4.5	APs should be site-survivable automatically. Configuration should be possible to configure as such if controller goes down, still APs should be able to handle client traffic without manual intervention.
5	**Security & Monitoring**
5.1	AP should support AES256 encrypted GRE-based tunnel for data forwarding.
5.2	AP Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, iPSK/DPSK/MPSK or equivalent, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256. It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w MFP and 802.11r Fast roaming.
6	**Management Features**
6.1	AP should be having administration access through HTTPS GUI, SSH CLI. It should provide WLAN configuration for standalone operation and provisioning tools for controller/cloud operations. If controller config disallows GUI/CLI access it should follow same.
6.2	AP should have recovery SSID for easy access to CLI console when AP is unreachable

	through network or console port
7	**Mandatory Compliance:**
7.1	AP should be quoted with metal based hard-ceiling, wall mounting kits.
7.2	Should have hidden latching mechanism and Plenum rating.
7.3	Should have operating temperature of 0-40 ºC
7.4	AP hardware should have been approved by Wireless Planning Commission (TRAI, Govt of India). ETA certificate should be submitted. Wi-Fi alliance certification also mandatory.
8	**Warranty**
8.1	AP should have a minimum of 5 year Warranty for hardware and support.
9	**Product brochure**
9.1	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications, features along with cross reference. Should also provide Manufacturer's Authorization.

Table – 2: Wireless Access Point for Indoor with following specifications **– 5 Nos**

S. No	Specification / Requirement
1	**Wireless Access Point**
1.1	Indoor Use
2	**Radio Specifications**
2.1	Access Point should be dual-band, dual-radio indoor access point
2.2	The Access Point should support 2x2:2 + 2x2:2 streams SU/MU MIMO on 5GHz and 2.4GHz
2.3	AP should support IEEE 802.11 a/b/g/n/ac/ax amendments.
2.4	Antenna should direct the radio signals per-device on a packet-by-packet in real-time to support high device density environments. Should have 3 dBi gain. Antenna operates without the need for device feedback to support devices using legacy standards.
2.5	AP should provide 23 dBm EIRP on 2.4GHz and 5 GHz, -93 dBm on 2.4GHZ and -98 dBm on 5GHZ receive sensitivity.
3	**Interface and Power Requirements**
3.1	AP should have 2 Ethernet ports including one PoEt
3.2	It should have less than 21.95Watts power consumption for full functionality including USB port on PoE
3.3	Should have onboard IoT radio. Should have option to add modular IoT radio using USB port. Both onboard and modular IoT radios should support BLE and Zigbee protocols.
4	**Networking Requirements**
4.1	AP should have capacity to handle minimum 300 Concurrent devices.
4.2	AP should be flexible hardware to be deployed as Standalone, Controller-less (Cluster), Controller-based, Cloud-based.
4.3	Should have IPv6 support, IEEE 802.1Q, Band balancing, airtime fairness, QoS, L2/L3/L4 ACL
4.4	AP should be able to act as sensor for WIPS, Location analytics engine and Network analytics engine.
4.5	APs should be site-survivable. Configuration should be possible to configure as such if controller goes down, still APs should be able to handle client traffic.

5	**Security & Monitoring**
5.1	AP should support AES256 encrypted GRE-based tunnel for data forwarding.
5.2	AP Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, iPSK/DPSK/MPSK or equivalent, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256. It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w MFP and 802.11r Fast roaming.
6	**Management Features**
6.1	AP should be having administration access through HTTPS GUI, SSH CLI. It should provide WLAN configuration for standalone operation and provisioning tools for controller/cloud operations. If controller config disallows GUI/CLI access it should follow same.
6.2	AP should have recovery SSID for easy access to CLI console when AP is unreachable through network or console port
7	**Mandatory Compliance:**
7.1	AP should be quoted with metal based hard-ceiling, wall mounting kits.
7.2	Should have hidden latching mechanism and Plenum rating.
7.3	Should have operating temperature of 0-40 ºC
7.4	AP hardware should have been approved by Wireless Planning Commission (TRAI, Govt of India). ETA certificate should be submitted. Wi-Fi alliance certification also mandatory.
8	**Warranty**
8.1	AP should have a minimum of 5 year Warranty for hardware and support.
9	**Product brochure**
9.1	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications, features along with cross reference. Should also provide Manufacturer's Authorization.

Table – 3: Wireless Access Point for Outdoor with following specifications – **2 Nos**

S. No	Specification / Requirement
1	**Wireless Access Point**
1.1	Outdoor Use
2	**Radio Specifications**
2.1	Access Point should be dual-band, dual-radio, IP67 rated 120 degrees sectorial outdoor access point
2.2	The Access Point should support 2x2:2 + 2x2:2 streams SU/MU MIMO on 5GHz and 2.4GHz
2.3	AP should support IEEE 802.11 a/b/g/n/ac/ax amendments.
2.4	AP should provide 22dBm peak transmit power on both radios, -93 dBm receive sensitivity.
2.5	It should have adaptive antenna technology for performance optimization and interference mitigation features. Antenna should provide Extended coverage utilizing multi-directional antenna patterns. Polarization Diversity with Maximal Ratio Combining (PDMRC).
2.6	Antenna should dynamically choose antenna patterns in real-time environment to establish the best possible connection with every device. Should support at least 50 antenna patterns combinations.

2.7	Antenna should direct the radio signals per-device on a packet-by-packet in real-time to support high device density environments. Should have 6-8 dBi gain. Antenna operates without the need for device feedback to support devices using legacy standards.
3	**Interface and Power Requirements**
3.1	AP should have one RJ-45 based Ethernet PoE port.
3.2	It should have less than 21.95Watts power consumption for full functionality including USB port on PoE
4	**Networking Requirements**
4.1	AP should have capacity to handle minimum 100 Concurrent devices.
4.2	AP should be flexible hardware to be deployed as Standalone, Controller-less (Cluster), Controller-based, Cloud-based.
4.3	Should have IPv6 support, IEEE 802.1Q, Band balancing, airtime fairness, QoS, L2/L3/L4 ACL
4.6	APs should be site-survivable. Configuration should be possible to configure as such if controller goes down, still APs should be able to handle client traffic.
5	**Security & Monitoring**
5.1	AP should support AES256 encrypted GRE-based tunnel for data forwarding.
5.2	AP Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, iPSK/DPSK/MPSK or equivalent, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256. It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w MFP and 802.11r Fast roaming.
6	**Management Features**
7.1	AP should be having administration access through HTTPS GUI, SSH CLI. It should provide WLAN configuration for standalone operation and provisioning tools for controller/cloud operations. If controller config disallows GUI/CLI access it should follow same.
7.2	AP should support network speed testing tool. Bidder should provide software for both computers and mobile during installation.
7.3	AP should have recovery SSID for easy access to CLI console when AP is unreachable through network.
8	**Mandatory Compliance:**
8.1	AP should be quoted with metal based hard-ceiling, wall mounting kits.
8.2	Should have Plenum rating.
8.3	Should have operating temperature of -10-60 ºC
8.4	AP hardware should have been approved by Wireless Planning Commission (TRAI, Govt of India). ETA certificate should be submitted. Wi-Fi alliance certification also mandatory.
9	**Warranty**
9.1	AP should have a minimum of 5 year Warranty for hardware and support.
10	**Product brochure**
10.1	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications, features along with cross reference.. Should also provide Manufacturer's Authorization.

Table – 4: Wireless Access Point for Outdoor with following specifications – **4 Nos**

S. No	Specification / Requirement
1	**Wireless Access Point**
1.1	Outdoor use
2	**Radio Specifications**

2.1	Access Point should be dual-band, dual-radio, IP67 rated outdoor access point
2.2	The Access Point should support 2x2:2 + 2x2:2 streams SU/MU MIMO on 5GHz and 2.4GHz
2.3	AP should support IEEE 802.11 a/b/g/n/ac/ax amendments.
2.4	AP should provide 22dBm peak transmit power on both radios, -93 dBm receive sensitivity.
2.5	It should have adaptive antenna technology for performance optimization and interference mitigation features. Antenna should provide Extended coverage utilizing multi-directional antenna patterns. Polarization Diversity with Maximal Ratio Combining (PDMRC).
2.6	Antenna should dynamically choose antenna patterns in real-time environment to establish the best possible connection with every device. Should support at least 50 antenna patterns combinations or equivalent.
2.7	Antenna should direct the radio signals per-device on a packet-by-packet in real-time to support high device density environments. Should have 3 dBi gain. Antenna operates without the need for device feedback to support devices using legacy standards.
3	**Interface and Power Requirements**
3.1	AP should have one RJ-45 based Ethernet PoE port.
3.2	It should have less than 21.95Watts power consumption for full functionality including USB port on PoE
4	**Networking Requirements**
4.1	AP should have capacity to handle minimum 100 Concurrent devices.
4.2	AP should be flexible hardware to be deployed as Standalone, Controller-less (Cluster), Controller-based, Cloud-based.
4.3	Should have IPv6 support, IEEE 802.1Q, Band balancing, airtime fairness, QoS, L2/L3/L4 ACL
4.6	APs should be site-survivable. Configuration should be possible to configure as such if controller goes down, still APs should be able to handle client traffic.
5	**Security & Monitoring**
5.1	AP should support AES256 encrypted GRE-based tunnel for data forwarding.
5.2	AP Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, iPSK/DPSK/MPSK or equivalent, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256. It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w MFP and 802.11r Fast roaming.
6	**Management Features**
7.1	AP should be having administration access through HTTPS GUI, SSH CLI. It should provide WLAN configuration for standalone operation and provisioning tools for controller/cloud operations. If controller config disallows GUI/CLI access it should follow same.
7.2	AP should support network speed testing tool. Bidder should provide software for both computers and mobile during installation.
7.3	AP should have recovery SSID for easy access to CLI console when AP is unreachable through network.
8	**Mandatory Compliance:**
8.1	AP should be quoted with metal based hard-ceiling, wall mounting kits.
8.2	Should have Plenum rating.
8.3	Should have operating temperature of -10-60 ºC
8.4	AP hardware should have been approved by Wireless Planning Commission (TRAI, Govt of India). ETA certificate should be submitted. Wi-Fi alliance certification also mandatory.
9	**Warranty**
9.1	AP should have a minimum of 5 year Warranty for hardware and support.
10	**Product brochure**
10.1	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications, features along with cross reference. Should also provide Manufacturer's Authorization.

Table – 5: Wireless Controller with following specifications (with one time license) – 1 No.

S. No	Specification / Requirement
1	**Wireless Controller with Perpetual License**
1.1	Software Controller
2	**Essential Features**
2.1	The WLAN solution should have on prem controller. It can be appliance or server based with required hardware; software and respective licenses from day-1
2.2	Controller should have Easy Setup through UPnP Network Discovery and Installation Wizard.
2.3	Controller should support 50 AP from day one and should be scalable up to 100 APs or more with support of seamless roaming access over L2/L3 network.
2.4	Controller should have capacity to handle minimum 1000 or more Concurrent devices.
2.5	Controller should support integrated user authentication capability of minimum 1,000 users without the need for any external database servers (AD/LDAP).
2.6	Redundancy Features: Controller Must support Active:Standby, Active:Active with N+1 redundancy options. When HA is enabled in future, AP licenses should be shared among Active:Standby Controllers.
3	**Wireless management Features**
3.1	Controller should monitor and maintain Access points related information such as IP/MAC, Model, Firmware, Radio and traffic statistics, RF/LLDP neighbours, GPS location etc., It should also manage Configuration of APs group-wise, zone-wise. Should have option to override group config specific to AP.
3.2	Controller should provide air-time fairness, Band Steering, Spectrum analysis.
3.3	Controller should support Automatic Channel Interference System (having an in-built algorithm with right intelligence that scouts all available channels that promises improved wireless capacity in congested environments based on related statistics), Smart mesh system.
3.4	Controller should support Visual Client Connection Diagnostics.
3.5	Controller should be able to support Bonjour Fencing to Chromecast, QoS Features like 802.11e, WMM, U-APSD.
3.6	Should have capabilities such as Filtering of Alarms and event Log based on APs, SSID or Zones
3.7	Controller should support Wireless heat maps to show coverage areas and holes. Controller also should support Google maps integration.
3.8	Controller should support IoT controller integration to support BLE, Zigbee implementation over single ethernet network.
3.9	APs should be site-survivable. Configuration should be possible to configure as such if controller goes down, still APs should be able to handle client traffic.
4	**Guest Access Management**
4.1	Controller should provide a Guest Login portal in order to authenticate users that are not part of the organization.
4.2	Controller should be able to provide a web-based application that allows non-technical staff to create Guest accounts with validity for fixed duration like hours or days.
4.3	As part of WLAN solution should be able provide Self Service Guest access which will provide access to guests without IT intervention
5	**Security & Monitoring**
5.1	Controller should support AES256 encrypted GRE-based tunnel for data forwarding.
5.2	Controller Should support auth/encryption methods for WLAN configuration: Open, WEP, WPA2-AES, iPSK//DPSK/MPSK or equivalent, WPA3-SAE, WPA3-OWE, IEEE 802.1X/EAP, AAA, AES-GCMP-256. It should also support Role-Based Access Control, rate-limiting, device fingerprinting, 802.11w

	MFP and 802.11r Fast roaming.
5.3	Controller should also support WISPr and Hotspot2.0.
5.4	Controller should support Firewall Features including L2/L3/L4 Access Control profiles, Application Control profiles, Deep packet inspection, Device based policies etc., Should support URL filtering when required.
5.5	As part of WLAN solution should support minimum 500 Identity based Pre-Shared Keys from day-1.
5.6	Controller should Isolate unicast/multicast/broadcast wireless client traffic from all hosts on the same VLAN/subnet. Client isolation should also have Whitelisting options. Controller should have the capability to limit/prevent clients from using static IP addresses thereby enhancing network efficiency and preventing network conflicts.
5.7	Support for Walled garden "Walled Garden" functionality to allow restricted access to select destinations by unauthorized wireless users.
5.8	Controller should support WIDS/WIPS for security including Rogue AP detection and prevention, Evil-twin/AP spoofing detection and Ad-Hoc detection.
6	**Management Features**
6.1	Controller should be having administration access through HTTPS GUI, SSH CLI. HTTPS GUI should be able to present a customizable dashboard with information on the status of the network.
6.2	Administrative users should have account security features such as session idle timer, account lockout, password expiration/recovery, password reuse policy, two factor authentications. Should have option to enable captcha to make sure a human is logging into the system.
6.3	Controller should have library of well-documented REST-APIs and full set of MQTT/GPB to allow integration with 3rd party apps.
6.4	Access points can discover Controllers across Layer-3 network through DHCP or DNS option. Controller should have Mobile App for Smartphone to provision APs.
6.5	The Controller should support the ability to create different areas/zones in which AP can be grouped logically or physically based on location e.g. different buildings in a campus can be configured as different area/zones so that each area/zone will have different configuration and policies.
6.6	Controller should be able to raise critical alarms by sending an email. The email client on the Controller should support SMTP outbound authentication and TLS encryption.
6.7	Should support centralized & flexible licensing. Customer should be able to assign AP licenses to required controller as per requirement flexibly.
7	**Mandatory Compliance:**
7.1	If any of the features above require separate license, it should be quoted along with Controller, and the license should be perpetual.
8	**Warranty**
8.1	Controller should be quoted with TAC Support and Warranty for 5 years.
9	**Product brochure**
9.1	Vendor should provide printed technical catalogues/brochures for the quoted model containing technical specifications, features along with cross reference. Should also provide Manufacturer's Authorization.

Table – 6: User Authentication and On-boarding Solution with following specifications (with Perpetual License) **– 1 No**

S. No	Specification / Requirement
1	**Software application for User Management, Authentication and on boarding**
1.1	Solution to cover users from LAN and Wifi.
2	**Essential Features**
2.1	This solution should support Authorisation, Authentication & Accounting (AAA), network access

	control, BYOD and Guest Access by incorporating identity, physical/device information and conditional elements on a single platform.
2.2	Should support variety of authentication methods (802.1 X, MAC auth and web auth) for Wired and wireless networking equipment.
2.3	It should support up to 600 devices (300 Users) with 5 years support from day 1
2.4	It should provide facility for phased implementation approach by starting with role based access management and later incorporating end point health of security measurement.
2.5	It should support RADIUS server for client device authentication and TACACS+ for network device authentication with logging.
2.6	The solution should have integrated support for Microsoft windows end points for health and posture checks.
2.7	Authentication or authorization support for LDAP, AD, and Kerberos and SQL compliance
3	**The solution should have the following features**
	• Built-in guest management and device/user on boarding. • Web based management interface with dashboard. • Reporting and analysis with custom data filters. • Data repository for user, device, transaction information. • Rich polices using identity, device, and health of conditional elements. • Integrated network-based device profiler utilizing collection via SNMP, AD, and HTTP. • Support for smart devices and traditional computing platforms. • Ability to support iOS, Windows and Android • Correlation of user, device and authentication information for trouble shooting and tracking. It should provide high level of visibility into what devices are on the network and associated with what users. • Support for automated on boarding of devices to enable secure access via self-serve portal • Ability to integrate with active directory so users that are approved for BYOD may be authenticated via identity and device attributes. • Should be able to accept MS Excel/ .csv file with user details and should be able to return the same file with assigned passwords/tokens to all users mentioned in the file for login authentication credentials.
4	**Solution must be capable of providing**
	• Self-provisioned guest access license for 1000 users should be available. • Ability to provide free or billable guest access with payment solution. • Ability to send automated SMS or email credentials to the guest users. • Ability to set account details including time frame, and Band width, contract. • Once account time frame expiries the user account becomes inactive automatically. • Solution must be capable of providing advertising services. • Guest solution should manage the individual guest credentials in database. • Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit. • Auto login for self-registration work flow no need for the guest to retrieve account credentials from SMS or email for initial login (as required). • Bulk import of guest accounts with ability to trigger notification of credentials via email, MS Excel file/ .csv file. • Post login session statistics page displayed to users so they can monitor usage of quota assigned (as required) • Location based captive portal-display different landing page based on where guest is connecting to the network. • Fully customizable self-registration of guest creation pages. • Able to generate the user log for a minimum period of 6 months in correlation to the firewall of the network.

Table – 7: Other Items

S. No.	Description	Qty.
1.	24 Port POE Gigabit Switch with 2 SFP Modules	02 Nos.
2.	64 GB Server RAM (Existing - HP Proliant 370 Server, Serial No. SGH130X80K) (Product No. 588857-B21)	02 Nos.
3.	6F Armoured Fibre Optic Cable (mtrs. as required)	As req.
4.	Fiber Patch cords (mtrs. as required)	As req.
5.	CAT 6 Cable, RJ45 jacks (mtrs. and nos. as required)	As req.
6.	6U Rack with cable manager and power manager	01 Nos
7.	Power manager	01 Nos

- **The bidder is completely responsible for**
  - i. Ensuring that all categories of Controller, Access Points and "User Authentication and On-boarding Solution" will be from same OEM.
  - ii. All existing Access Points and Wired connections should be integrated in the proposed "User Authentication and On-boarding solution" along with the new Access Points. Also, the solution should support, further wired and wireless device inclusions in its ambit.
  - iii. Including all such items which are not mentioned in this BoQ but required to be met keeping in view of the NIPHM technical and functional requirements as required by the solution in its totality, need to be included and listed in the offer without fail.
  - iv. Laying of Fiber with Splicing, Installation of access points with required accessories. (Where ever, underground laying of cables is considered, the same shall be laid at a minimum depth of 03 (three) feet with markers enroute. Wherever overhead cables are laid, it should be ensured that they shall be at a minimum height with vehicle clearance and all required support structures like, it is encased with HDPE pipe and supported by a strong GI wire and poles (as required)).
  - v. Installation and Configuration of Server, Virtual Controller, User Management Solution, VLAN with Guest login and Log maintenance etc.
  - vi. Configuring existing firewall to align with the solution and generate required reports related to user access, uploads and downloads, traffic, security breaches, content access etc.
  - vii. And all other such activities which need to be completed for the successful installation, configuration, integration with the existing network and roll-out of the required solution as desired by NIPHM.
  - viii. Any disturbance in existing services and issues / damage to the existing equipment / infrastructure of NIPHM shall be restored within a minimum time of two working days and any equipment damaged shall be replaced by the equipment of same or higher configuration by the bidder in the stipulated time of order completion. The replacement (if any) should be done if accepted by NIPHM officials.

- **Site visit Certificate**: Mandatory, without which the bid shall be rejected. (Format enclosed as **Annexure - VI**)

ANNEXURE – VI

Format for Self-Declaration of Site-Visit of NIPHM, Hyderabad

I_____(Name of the authorized person) hereby certify that we M/s. _____ (bidder name) have visited the campus of NIPHM Hyderabad to familiarize/ understand and assess requirements of the solution as required by NIPHM and expected quality level of services that are required to be rendered. I/we have understood the required solution in its totality.

Signature and
Seal of the Bidder
with Date:

Name in Block
Letters:

Designation:

Full Address:

Contact no.:

Countersign by
NIPHM Hyderabad
Official(s) with
Date:

Name of the
Official:

Designation: